

Governança e boas práticas na Lei Geral de Proteção de Dados por meio da conformidade, da gestão de riscos e da *accountability*

Governance and best practices at LGPD trough compliance, risk management and accountability

Grace Ladeira Garbaccio¹

Flávia Lubieska N. Kischelewski²

Resumo: Este trabalho tratou do tema da governança e das boas práticas à luz da Lei Geral de Proteção de

-
- 1 Doutora em Direito com Pós-doutorado em Administração pela Université Paris 1 - Panthéon Sorbonne/França e em Direito pela Université Côte d'Azur - Nice/França. Professora dos Mestrados e Doutorados em Administração Pública e em Direito Constitucional do IDP - Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa. Professora convidada da Université Paris 1 - Panthéon Sorbonne; da Universidade Sapienza di Roma e da Universidade de Mendoza/Argentina. Profissional da área de Sustentabilidade, Governança Corporativa & Compliance, formada em Direito pela Universidade Federal de Minas Gerais (2002) e em Administração pela Fundação João Pinheiro (2000), com Mestrado em Direito pela Université de Limoges (2005) e Doutorado em Direito - Université de Limoges (2009) - reconhecido pela UFSC (2010).
 - 2 Mestre em Direito pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa de Brasília (2022). Mestranda pela Universidade de Mendoza/Argentina. Advogada em Curitiba/PR, atuante em direito societário, contratual e digital.

Dados Pessoais (LGPD), com foco nos procedimentos de conformidade, levantamento e gerenciamento de riscos, além do princípio da *accountability* (prestação de contas). O objetivo central foi responder: quais elementos de governança e boas práticas devem ser utilizados para efetiva conformidade à LGPD? Adotou-se como metodologia de pesquisa o método de abordagem dedutivo, com análise exploratória-bibliográfica. Os objetivos específicos foram: estudar o *compliance*, o princípio da *accountability* e os mecanismos de gerenciamentos de riscos como meios de estabelecimento de governança da privacidade e da proteção de dados nas organizações; analisar o relatório de impacto de dados como forma de mitigar riscos e preservar os direitos dos e liberdades dos titulares; examinar experiências estrangeiras, especialmente oriundas da União Europeia como modelos para governança e boas práticas para o Brasil. Conclui-se que o *compliance* é uma forma do Estado transferir parte da atividade de fiscalização ao ente privado. Ainda assim, um programa estruturado de gestão de riscos e a governança construída com atenção ao princípio da *accountability* são vantagens para as instituições, fomentando a estabilidade financeira, a integridade empresarial e a preservação da reputação.

Palavras-chave: Governança. *Compliance*. Gerenciamento de riscos. Prestação de contas. LGPD.

Abstract: This paper dealt with the theme of governance and best practices in the light of the Brazilian Lei Geral de Proteção de Dados Pessoais (LGPD), focusing on compliance procedures, survey and risk management, in addition to the accountability principle. The main goal of this paper was to answer: which elements of governance and best practices should be used to effectively be compliant to LGPD? The deductive approach method was adopted as the

research methodology, with exploratory-bibliographic analysis. The specific goals of the paper were: to study compliance, the accountability principle and the mechanisms of risk management in order to establish data governance in organizations; analyze the data impact report as a way to mitigate risks and preserve the rights and freedoms of the data subjects; to examine foreign experiences, especially from the European Union as models for privacy and data protection governance and best practices for Brazil. It is concluded that compliance in the area of privacy and data protection is a way for the State transfer part of its powers to the private entity. Even so, a structured risk management program and governance built with attention to the accountability principle are advantages for institutions, promoting financial stability, business integrity and the preservation of reputation.

Keywords: Governance. Compliance. Risk Management. Accountability. LGPD.

1. Introdução

Expressões como governança, mitigação de riscos, *compliance*, boas práticas, *accountability*, entre outras vêm, há alguns anos, permeando o cenário nacional das organizações públicas e privadas com maior constância. O advento da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais ou LGPD) impulsiona um incremento dessa utilização por juristas, agentes do setor públicos e entes privados, mas, mais importante, incentiva a implementação dessas técnicas. No lugar de apenas serem expressões de modismo³, o legislador estimula uma efetiva mudança de

3 O tratamento ético dos dados pessoais não é uma moda, representando na atualidade um direito fundamental das pessoas. (Rodriguez, 2020, p. 411)

postura que se estende às atividades de tratamento de dados pessoais.

Em realidade, esses verbetes e as técnicas não são novos; havendo, apenas uma expansão desses mecanismos para novos setores da economia, incluindo, como referido, o tratamento de dados pessoais. A partir da LGPD, tem-se um marco legal para impor uma correspondência prática às suas disposições. O que antes poderia ocorrer apenas eventual e espontaneamente (sob a forma de autorregulação para governança e gerenciamento de riscos relativos ao uso de dados pessoais), deve agora ser realizado por força de lei e com base na LGPD, por controladores e operadores⁴.

Assim sendo, segundo artigo 50, *caput*, da LGPD, há um impulsionamento para a adoção de regras de boas práticas e de governança. Cabe, em decorrência, estabelecer um programa de governança da privacidade e da proteção de dados eficaz, passível de ser avaliado, inclusive por terceiros, seja a Autoridade Nacional de Proteção de Dados – ANPD, sejam auditores externos, seja o Poder Judiciário. A materialização desse programa ocorre por meio da produção de políticas, códigos, termos, treinamentos, registros de evidências e outros documentos, com sistemática adequada e proporcional ao porte da empresa ou ao órgão público⁵.

4 Nos termos dos incisos VI e VII, do artigo 5º, da LGPD, controlador e operador são, respectivamente, a pessoa natural ou jurídica, de direito público ou privado, (i) a quem competem as decisões referentes ao tratamento de dados pessoais; e (ii) que realiza o tratamento de dados pessoais em nome do controlador.

5 O regulamento europeu de proteção de dados pessoais traz uma especificação sobre porte de organizações que não encontra parâmetro na LGPD. Os registros das atividades de tratamento não se aplicam às empresas ou organizações com menos de 250 trabalhadores, salvo se o tratamento puder implicar risco para os direitos e liberdades do titular dos dados, não seja ocasional e não abranja dados sensíveis (categorias especiais), ou dados pessoais relativos a condenações penais e infrações. (Kischelewski, 2021).

Para se estar em conformidade com a legislação, convém se espelhar, inicialmente, em programas de *compliance*⁶ composto por técnicas de abordagem e gestão de riscos. Isso é imprescindível porque as possibilidades de erro ou de não conformidade com as centenas de dispositivos da lei serão enormes, o que poderá ocasionar o surgimento de uma nova indústria de indenizações⁷ e a imposição de sanções administrativas pela ANPD⁸. O uso de *frameworks*⁹ de gerenciamento de riscos em privacidade e de segurança da informação, como as normas específicas da Associação Brasileira de Normas Técnicas (ABNT), também são úteis nessa atividade porque trazem, entre outros aspectos, mecanismos que estimulam a mudança cultural das organizações.

Essas ferramentas são também especialmente benéficas quando houver necessidade de avaliar se é indicado ou não produzir um relatório de impacto de dados pessoais (RIPD) ou, por exemplo, uma avaliação de legítimo interesse (LIA do acrônimo, em inglês, *legitimate interest assessment*). Adicionalmente, o foco na abordagem de possíveis riscos na operação relacionada ao tratamento de dados pessoais favorece a construção de meios para perpetrar o *privacy by design*, isto é, internalizar a proteção de dados desde a

6 Por semântica do termo, sua derivação se dá a partir da locução inglesa *to comply*, que traz consigo as ideias de cumprir, obedecer, satisfazer ou atender a uma imposição. Assim as ditas práticas de *compliance* são aquelas destinadas garantir que o particular esteja em conformidade com as normas que regem sua atividade. (Thamay; Tamer, 2020, p. 105-106).

7 No terreno fértil que a Justiça Brasileira oferece para o *demandismo*, a nova lei é um rastilho para um paiol de pólvora, pronto para explodir em inúmeros litígios. (Becker; Bruzzi; Wolkart, 2019).

8 Negrão, 2020, p. 31.

9 *Framework* pode ser compreendido como um sistema que reúne regras, ideias ou crenças empregadas para planejar ou decidir algo. São usados, em muitos casos, na consecução de projetos por conterem técnicas ou ferramentas que podem ser usadas em situações similares.

concepção do produto ou serviços e mantê-la como padrão.

Dessa maneira, ao longo do presente artigo, pretende-se examinar os referenciais estrangeiros que nortearam a inserção, na LGPD, da recomendação para que os agentes de tratamento formulem regras de boas práticas e de governança. Objetiva-se, igualmente, estudar o *compliance*, o princípio da *accountability* e os mecanismos de gerenciamentos de riscos como meios de estabelecimento de governança da privacidade e da proteção de dados nas organizações.

Esse exame passará, ainda, pela breve análise de modelos de sistemas de governança, sugestões de organismos estrangeiros, uso de políticas de segurança da informação e técnicas de gerenciamento de riscos, além de *frameworks* ou modelos com maior referência, como bases para cumprimento da LGPD e para a diminuição dos riscos de sanções administrativas e litígios no Poder Judiciário. Com base no método de abordagem dedutivo, a partir de uma análise exploratória-bibliográfica, bem como de experiências internacionais e da LGPD, que, segundo consta na sua própria nomenclatura, é uma legislação de cunho generalista, que carece de pormenorização. Esses institutos abrangentes são confrontados com modelos de gestão, gerenciamento e conformidade também considerado gerais, isto é, que servirão para várias circunstâncias similares. Apesar disso, a efetiva adequação aos ditames da LGPD, como se vislumbrou, somente será alcançado quando as especificidades de cada organização e de cultura corporativa ou órgão público forem igualmente abrangidas na construção do programa de governança de proteção de dados pessoais.

2. A importância dos dados para organizações e a necessidade de regras de governança

Na sociedade da informação, dados pessoais podem ser encontrados em qualquer organização, sendo mantidos e usados com diversas finalidades, como na gestão do relacionamento com o cliente, gestão de recursos humanos, prestação de serviços públicos, tratamentos médicos etc.¹⁰ Os desenvolvimentos tecnológicos das últimas décadas têm propiciado um intercâmbio e um acúmulo de dados gigantesco, demandando novas técnicas que favoreçam sua utilização para atuais e novos atores que ingressam nesse meio. O compartilhamento de dados se tornou um fenômeno global, pois a nova web gira em torno de comunidades, de participação e de fácil manipulação¹¹. Não é necessária uma formação precisa para entender que neste contexto específico do mundo digital, facilita-se o acúmulo indiscriminado de todo tipo de informação e dados em servidores e eles podem ser conhecidos e utilizados pelos usuários sendo encontrados acidentalmente através de pesquisas aleatórias¹².

A troca de informações sempre existiu e sempre foi considerada como algo importante para o ser humano, equiparando-se, em certa medida, informação a poder ou dinheiro. Há alguns anos, dados vêm sendo equiparados ao petróleo¹³ na era digital ou, até mesmo, ao urânio¹⁴. Esse

10 Alsenoy, 2012, p. 25.

11 Barreto Junior; Leite, 2017, p. 408.

12 Andresani; Stamile, 2018, p. 463.

13 Veja mais na revista *The Economist*, de março de 2017: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em 10 abr. 2024.

14 DADOS não são o “novo PETRÓLEO”. Comparando com fontes de energia, DADOS seriam o novo URÂNIO. Têm que ser REFINADOS para separar o que se quer do que não serve, têm que atingir MASSA CRÍTICA para gerar energia [VALOR!] e o DESCARTE é um perigo, para o negócio e o ecossistema. (Meira, 2020).

entendimento parece ter se tornado mais palpável nas últimas décadas, diante da ascensão das *big techs*, empresas que se desenvolveram a partir de plataformas tecnológicas baseadas em dados pessoais (como Google, Airbnb, Uber, Facebook e WhatsApp).

Os ativos da informação¹⁵ são preciosos para as organizações, ainda que sua atividade principal não esteja diretamente relacionada à prestação de serviços ou fornecimento de produtos que dependam da exploração de bancos de dados. Em certa medida, grande parte das atividades econômicas e da oferta de serviços públicos depende de informações pessoais e, independentemente de haver retorno financeiro ou não, é responsabilidade do controlador e do operador de dados pessoais o uso adequado e a proteção dos dados. Se essa responsabilização já existia anteriormente, com base na legislação civil e consumerista, essa possibilidade foi significativamente reforçada pela promulgação da LGPD.

Perante a importância dos dados e os riscos inerentes às atividades de tratamentos e seus impactos sobre as pessoas físicas, além da possibilidade de concentração de mercados, demanda-se e justifica-se a tutela estatal. A função regulatória deve ser ampla para disciplinar a informação gerada a partir do processamento e do tratamento dos dados pessoais, em um devido contexto. São as informações extraídas a partir desses dados, e não eles próprios, que formarão a representação virtual do indivíduo na sociedade¹⁶.

É preciso considerar que os dados se tornaram a matéria-prima como base da revolução digital, da inteligência

15 Pelo Glossário de Segurança da Informação do Gabinete da Segurança Institucional da Presidência da República, objeto da Portaria SGI nº 93, de 26 de setembro de 2019, ativos de informação significam os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

16 Mendes; Fonseca, 2020, p. 517.

artificial, da internet das coisas (IOT), da análise de costumes e preferências, das estratégias digitais de vendas e de consumo das famílias e das pessoas. A informação já é um dos maiores ativos da maioria das empresas¹⁷. Tecnicamente, dados e informações não são iguais; sendo o segundo algo que se pode derivar do primeiro. O dado é o estado primitivo da informação, pois não é algo *per se* que acresce o conhecimento. Dados são simplesmente *atos brutos* que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação¹⁸.

De tal modo, o verdadeiro valor dos dados está nos potenciais tratamentos e, diferentemente do óleo bruto, os dados são bens imateriais e não rivais, ou seja, podem ser copiados, processados e reutilizados potencialmente *ad infinitum*¹⁹. A despeito do valor dos dados e do fato de legislações de diversos países disporem sobre proteção à privacidade ou aos dados pessoais, não se pode olvidar que, em realidade, o cerne da proteção é o titular. Ao mesmo tempo que há maior empoderamento, há maiores riscos que podem afetar a pessoa física.

Ainda que haja a autodeterminação informativa, o titular de dados não tem meios ou ingerência para acompanhar todos os tratamentos que podem ser realizados com suas informações particulares. Muito lhe é desconhecido. As organizações devem, por conseguinte, estabelecer a chamada governança da privacidade e da proteção de dados, contemplando meios de controle e de segurança da informação, de forma a preservar os direitos dos titulares, sendo transparente²⁰ para eles e para autoridades regulatórias. O

17 Negrão, 2020, p. 30.

18 Bioni, 2019, p. 36.

19 Belli, 2021, p. 389.

20 Transparência é uma característica daquilo que vemos, como vemos ou como nos mostramos através de um filtro (Andresani e Stamile, 2018, p. 459).

benefício, em contrapartida, é uma utilização mais flexível dos dados pessoais por essas organizações²¹.

É nesse ambiente que a LGPD, em seu artigo 50, impulsiona a adoção de regras de boas práticas e de governança por controladores e operadores de dados como meio de proteção ao titular de dados pessoais. Reconhece-se que o incremento das atividades de tratamentos de dados é acompanhado respectivamente do aumento dos riscos, podendo ser atingidos os direitos fundamentais dos titulares ou suas liberdades civis, além de prejudicar a reputação e as operações do agente de tratamento, acarretando perdas financeiras²² e de mercado.

2.1 Antecedentes estrangeiros da governança e das boas práticas como referências à LGPD

Com maior frequência, vem-se presenciando casos de vazamentos de dados²³, fraudes diversas como as bancárias em meios virtuais, acusações de manipulações de redes com fins eleitoreiros, questionamentos sobre as responsabilidades sobre os gestores de redes sociais²⁴, ataques a portais

21 CIPL, 2011.

22 Não demorou a concessão de indenizações em razão do início da vigência da LGPD (<https://www.migalhas.com.br/depeso/334657/decisao-do-tj-sp-inaugura-aplicacao-da-lgpd>); entre outras ações com repercussão relevante (<https://www.migalhas.com.br/quentes/345285/linha-de-metro-e-condenada-por-instalar-cameras-com-captura-facial>). Acesso em 10 abr. 2024.

23 Ilustrativamente, podem-se recordar algumas notícias: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-apura-caso-de-vazamento-de-dados-de-operadoras-de-telefonias>; <https://tecnologia.ig.com.br/2021-03-28/ao-menos-oito-vazamentos-de-dados-ocorreram-no-brasil-em-2021-quem-e-punido.html>; <https://canaltech.com.br/seguranca/vazamento-de-dados-do-zoom-compromete-mais-de-500-mil-usuarios-163316/>. Acesso em 10 abr. 2024.

24 Para um estudo mais aprofundado sobre a responsabilidade civil dos

de instituições públicas acarretando a indisponibilidade dos serviços²⁵ e tantos outros desvios de conduta. Esse lado negativo da balança ocasionou

(...) uma corrida pela preservação da integridade e reputação da empresa, bem como a utilização de ferramentas para garantir que as boas práticas estabelecidas pela governança sejam seguidas, assegurar que a organização esteja em conformidade com as diversas legalidades atreladas ao negócio, além de identificar os diversos riscos que possam comprometer os objetivos organizacionais²⁶.

Costuma-se entender risco como possibilidade de algo não dar certo. Mas seu conceito atual no mundo corporativo vai além: envolver a quantificação e a qualificação da incerteza, tanto no que diz respeito às perdas quanto aos ganhos por indivíduos ou organizações²⁷, inclusive em termos de perda de reputação e financeiras. Ademais, em razão da falibilidade em evitar ilegalidades, o Estado partilha com o particular a tarefa de evitá-las. O *compliance*, nessa perspectiva, representa um novo passo na relação entre Estado e capital, marcado agora por uma nova forma de controle que conta diretamente com a participação do particular²⁸.

Para melhor compreendermos a evolução, no Brasil, das recomendações sobre governança e boas práticas no campo da proteção de dados ao abrigo na LGPD e também

provedores de aplicações por ato de terceiro na Lei nº 12.965/2015 (Marco Civil da Internet), vide artigo específico sobre o tema de autoria de Irineu Francisco Barreto Junior e Beatriz Salles Ferreira Leite, na Revista Brasileira de Estudos Políticos (RBEP), nº 115.

25 Inúmeros são os exemplos como os recentemente ocorridos em relação ao Poder Judiciário, como o ataque a sistemas do Conselho Nacional de Justiça, do Tribunal de Justiça do Estado do Rio Grande do Sul e do Tribunal de Justiça do Estado de São Paulo.

26 Trivelato; Mendes e Dias, 2018, p. 2.

27 IBGC, 2017, p. 11.

28 Thamay; Tamer, 2020, p. 105.

entender a participação das organizações na busca da conformidade, cabe recordar as experiências internacionais que norteiam essas questões. Em 1980, a Organização para Cooperação e Desenvolvimento Econômico (OCDE) publicou, sob a forma de Recomendação, as *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*²⁹, que refletem um consenso sobre os princípios básicos que deveriam ser observados na criação de legislações nacionais. Entre seus objetivos, pugnava-se pela remoção ou pela não criação, em nome da privacidade, de barreiras injustificadas ao fluxo transfronteiriço de dados pessoais.

O principal destaque para essas diretrizes foi o surgimento do princípio da *accountability*³⁰, estatuinto que o controlador de dados deve ser responsável pelo cumprimento das medidas que dão efeito aos princípios que apresenta. A *accountability* está expressamente contida na LGPD, no inciso X, do artigo 6º, sendo aqui traduzida como responsabilização e prestação de contas, embora, na origem, sua verdadeira compreensão demande o cumprimento de mais ações. De qualquer modo, cabe, resumidamente, ao agente de dados demonstrar a adoção de medidas eficazes para a gestão de riscos e comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas.

Com grande similaridade, encontramos os Princípios de Governo das Sociedades do G20 e da OCDE³¹, pelos

29 Disponível em: <https://www.oecd.org/digital/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm>. Acesso em 10 abr. 2024.

30 Para melhor compreensão do princípio da *accountability* na proteção de dados pessoais, recomenda-se a leitura do *CIPL Accountability Q&A*, disponível em https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_q_a__3_july_2019_.pdf. Acesso em 10 abr. 2024.

31 OCDE (2016), Princípios de Governo das Sociedades do G20 e

quais a governança propõe ajudar a construir um ambiente de confiança, transparência³² e responsabilidade, necessário para fomentar o investimento a longo prazo, a estabilidade financeira e a integridade empresarial, apoiando, assim, um crescimento mais forte e sociedades mais inclusivas (como se vê a definição de governança está ligada aos fins que se pretende alcançar).

No âmbito europeu, o estímulo à governança da privacidade e da proteção de dados pessoais foi formalizado a partir de 1995, ainda que isso não conste diretamente no texto regulatório. A Diretiva 95/46/CE³³ era a referência europeia em matéria de proteção dos dados pessoais até maio de 2018. De forma congruente com as disposições preconizadas nas diretrizes da OCDE, a Diretiva previa, em seus artigos 18 a 20, a obrigação de notificação das autoridades nacionais anteriormente ao processamento de determinadas atividades de tratamento de dados pessoais³⁴, criando uma interação e diálogo entre os agentes de tratamento com as autoridades, num ambiente transparente e com preservação dos direitos das pessoas físicas.

da OCDE, Editions OCDE, Paris. Disponível em: <http://dx.doi.org/10.1787/9789264259195-pt>. Acesso em 10 abr. 2024.

- 32 Para uma análise crítica e específica sobre a transparência na regulação e governança da internet, sugere-se a leitura do artigo *Transparency in internet regulation and governance: arguments and counter-arguments with some methodological reflections*, de Gianluca Andresani e Natalina Stamile, publicado na Revista Brasileira de Estudos Políticos (RBEP), nº 117. Os autores fazem uma relação interessante entre transparência, veracidade, confiabilidade, privacidade e controle na internet.
- 33 Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, que permaneceu vigente até 24/05/2018. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046>. Acesso em 10 abr. 2024.
- 34 CARVALHO; MATTIUZO; PONCE, 2021, pp. 362-363.

Em substituição à citada Diretiva, foi promulgado o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, em 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados³⁵ ou Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* ou, conforme acrônimo em inglês, GDPR). Essa nova regulamentação, com efeitos desde 25 de maio de 2018, juntamente com a Diretiva substituída, são as principais inspirações para a elaboração parlamentar da LGPD e, em consequência, das referências nacionais para boas práticas e governança da privacidade e da proteção de dados a serem aplicadas pelos agentes de tratamento.

O GDPR também trouxe expressamente o princípio da *accountability*, em seu artigo 24º, atribuindo aos controladores o dever de implementar medidas técnicas e organizativas adequadas para assegurar e comprovar que o tratamento é realizado em conformidade com regulamento. Deve, igualmente, haver revisão e atualização frequente de tais medidas, que podem ser implementadas por meio de políticas e códigos de conduta, além de serem demonstráveis. A responsabilidade do agente é variável de acordo com a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, sem prejuízo dos riscos para os direitos e liberdades das pessoas naturais, o que deve ser aferido com base em elementos diversos.

Cumprir destacar que essa responsabilidade tem por fundamento, como se depreende do Considerando 75 do GDPR, os já referidos riscos para os direitos e liberdades das pessoas. Uma vantagem do GDPR em relação à LGPD nesse contexto é que o primeiro traz uma série de situações que

35 Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em 10 abril 2024.

podem figurar como violação aos direitos e liberdades das pessoas: (i) tratamento que possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza econômica ou social; (ii) avaliação de aspectos de natureza pessoal, em particular análises ou previsões de aspectos que digam respeito ao desempenho no trabalho, à situação econômica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou aos deslocamentos das pessoas, a fim de definir ou fazer uso de perfis; (iii) tratamento de dados relativos a pessoas singulares vulneráveis, em particular crianças; etc.

Para Pessin e Lilla,

da mesma forma que o GDPR, a LGPD pode ser vislumbrada como um diploma normativo que estabelece instrumentos para a gestão de riscos à privacidade, possibilitando que os agentes de tratamento avaliem os impactos das operações envolvendo dados pessoais dos titulares de tais informações, isto é, compreender em que medida novos modelos de negócios, tecnologias, produtos e serviço podem impactar os direitos e as liberdades fundamentais dessas pessoas durante todo o ciclo de vida do dado, desde a coleta até o descarte (2020, pp. 106-107).

Desse modo, é preciso que os riscos sejam medidos com base numa avaliação objetiva, que seja determinado se as operações de tratamento de dados implicam risco e em que medida pode haver danos ou prejuízos aos titulares. Esses levantamentos devem ser efetuados desde a elaboração de um produto ou serviço, passando a ser um pressuposto indispensável e permanente no tratamento de dados pessoais. É nesse contexto que se compreende a relevância do artigo 25º, do GDPR, ao prever um novo comportamento, isto é, a

proteção de dados *by design* (desde a concepção) e *by default* (por padrão). Trata-se da orientação de que a implementação de tais medidas passa pelo desenvolvimento de produtos e serviços, que devem ser concebidos desde o princípio de forma a permitir o mais completo atendimento às regras³⁶ e ditames legais.

A governança pode ser aplicada a qualquer ente público ou privado, não importando o porte da organização, desde que se façam os necessários ajustes. É em meio a esse contexto que se pode compreender disposto no §1º, do artigo 50, da LGPD, que prevê que o controlador e o operador levarão em consideração, ao estabelecer regras de boas práticas, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular. É uma redação muito próxima do Considerando 74, do GDPR.

Não há, no entanto, na LGPD o dever de consulta prévia à ANPD. Isso ocorre nos países que adotam o GDPR, quando certos tipos de operações de tratamento envolverem a utilização de novas tecnologias ou pertencerem a um novo tipo sem que tenham sido antecedidas por uma avaliação de impacto sobre a proteção de dados por parte do responsável pelo tratamento, ou serem ainda vistas como necessárias em razão do período decorrido desde o tratamento inicial responsável pelo tratamento. O GDPR confere um “voto de confiança” aos agentes de tratamento e fixa o risco como crivo para essas notificações: elas são necessárias somente quando o tratamento puder gerar “alto risco para os direitos e liberdades fundamentais” (Considerando nº 89, do RGPD)³⁷, segundo estabelecido no artigo 34º.

36 Carvalho; Mattiuzo; Ponce, 2021, p. 363.

37 Mendes; Fonseca, 2020, p. 522.

2.2 Governança da proteção de dados e boas práticas no Brasil – além da Igpd

No setor privado, para o Instituto Brasileiro de Governança Corporativa (IBGC), governança significa o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas³⁸. Por sua vez, na esfera pública, o Decreto nº 9.203, de 22 de novembro de 2017, considera governança pública como um conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade³⁹.

Como se vê, governança pode ser aplicada a qualquer ente público ou privado, não importando o porte da organização, desde que se façam as adaptações cabíveis. É preciso que sejam seguidos os princípios de integridade, confiabilidade, transparência e *accountability*, com procedimentos estruturados e compromisso da alta administração (*tone at the top*⁴⁰), devendo, ainda, haver gestão de riscos, revisão e monitoramento de tempos em tempos para as melhorias oportunas. É importante que sejam realizadas auditorias internas periódicas para avaliar o cumprimento de regras por parte de funcionários e colaboradores de todos os níveis hierárquico⁴¹.

38 IBGC, 2015, p. 20.

39 Recomenda-se a leitura adicional do Guia da política de governança pública / Casa Civil da Presidência da República – Brasília: Casa Civil da Presidência da República, 2018. Disponível em: <https://www.gov.br/casacivil/pt-br/centrais-de-conteudo/downloads/guia-da-politica-de-governanca-publica>. Acesso em 10 abr. 2024.

40 O exemplo de ética deve vir de cima.

41 Carvalho; Mattiuzo; Ponce, 2021, p. 372.

A governança da privacidade e da proteção de dados, por sua vez, é espécie do gênero governança⁴². Pelo art. 2º, inciso VI da Portaria nº 58/2016⁴³, que dispõe sobre procedimentos complementares para o compartilhamento de bases de dados oficiais entre órgãos e entidades da administração pública federal direta e indireta e as demais entidades controladas direta ou indiretamente pela União⁴⁴, governança

42 Para SILVA, que designa um arranjo institucional orientado a propósitos associados, em última instância, ao alcance de padrões de desempenho econômico (retorno sobre investimentos) de empresas privadas constituídas sob a forma de um modelo específico de propriedade: a sociedade anônima, cujo capital é dividido em ações (títulos financeiros) comercializados em bolsa de valores, ou seja, em mercado público. Disponível em: <http://repositorio.ipea.gov.br/handle/11058/8970>. Acesso em 10 abr. 2024.

43 Portaria nº 58/2016 da Secretaria de Tecnologia da Informação do Ministério do Planejamento, Desenvolvimento e Gestão, disponível em <https://www.gov.br/conarq/pt-br/legislacao-arquivistica/portarias-federais/portaria-no-58-de-23-de-dezembro-de-2016#:~:text=Disp%C3%B5e%20sobre%20os%20procedimentos%20complementares,direta%20ou%20indiretamente%20pela%20Uni%C3%A3o>. Acesso em 10 abr. 2024.

44 Essa Portaria regulamenta as disposições do Decreto nº 8.777, de 11 de maio de 2016, que institui a Política de Dados Abertos do Poder Executivo Federal. Tal Decreto, em razão da data de sua promulgação, deve ser contextualizada com a LGPD que foi publicada em 14 de agosto de 2018, entrando em vigência (em quase todas suas disposições) em setembro de 2020 apenas. Mesmo que o Decreto não disponha, obviamente, sobre dados pessoais, trata-se de uma inovação legislativa que permanece atual, pois, por exemplo, entre os meios para implantação da Política de Dados Abertos estabeleceu a criação e manutenção de inventários e catálogos corporativos de dados, assim como a criação de processos para o engajamento de cidadãos, com o objetivo de facilitar e priorizar a abertura da dados, esclarecer dúvidas de interpretação na utilização e corrigir problemas nos dados já disponibilizados. Esses aspectos são muito próximos ao que se recomenda na LGPD em termos de mapeamento dos dados pessoais e procedimentos para cumprimento dos direitos dos titulares de dados. Para maiores detalhamentos, vide o Portal Brasileiro de Dados Abertos (<https://dados.gov.br/dados/conteudo/politica-de-dados-abertos>) e o estudo disponível em https://www.gov.br/governodigital/pt-br/governanca-de-dados/ap_degdi_fabiana_v_final.pdf. Acesso em 10 abr. 2024.

da privacidade e da proteção de dados

é o conjunto de políticas, processos, pessoas e tecnologias que visam a estruturar e administrar os ativos de informação, com o objetivo de aprimorar a eficiência dos processos de gestão e da qualidade dos dados, a fim de promover eficiência operacional, bem como garantir a confiabilidade das informações que suportam a tomada de decisão.

De forma mais sintética, o Decreto nº 10.406, de 9 de outubro de 2016, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados⁴⁵, conceitua, em seu artigo 2º, XV, a governança da privacidade e da proteção de dados como sendo o exercício de autoridade e controle que permite o gerenciamento de dados sob as perspectivas do compartilhamento, da arquitetura, da segurança, da qualidade, da operação e de outros aspectos tecnológicos.

Como dito, a governança da privacidade e da proteção de dados é um desdobramento da governança geral e

envolve o cruzamento de diversas disciplinas, com foco em qualidade de dados, passando por avaliação, gerência, melhoria, monitoração de seu uso, além de aspectos de segurança e privacidade associados a eles. Para tal, as empresas deverão definir objetivos organizacionais e processos institucionalizados, que deverão ser implementados dentro do equilíbrio fundamental entre TI e áreas de negócios⁴⁶.

45 No uso de suas atribuições, o Comitê Central de Governança de Dados, por meio da Resolução nº 4, de 14 de abril de 2020, disponibilizou o Guia de Boas Práticas para Implementação da Lei Geral de Proteção de Dados na Administração Pública Federal em <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd>. Acesso em 10 abr. 2024.

46 Barbieri; Farinelli, 2013, p. 7.

Como suscitado previamente, essa temática vem adquirindo contornos de relevância, especialmente nos meios corporativos. Cibersegurança e conformidade regulatória foram considerados pela consultoria Gartner, em 2024, como umas das maiores preocupações pelos Diretores Presidentes (CEOs) de empresas, o que se reflete no mercado de trabalho, que requer especialistas, embora escassos, para auxiliar na avaliação de riscos e segurança⁴⁷. A consultoria KPMG, na mesma linha, destacou a necessidade de criação de planos de planos de segurança cibernética como um dos temas prioritários para debate pelos Conselhos de Administração de companhias em 2024, em função da digitalização acelerada. Nesse contexto,

outro grande desafio é a governança de dados, abrangendo *compliance* com leis e regulamentos da indústria onde a empresa atua, bem como as regras de privacidade de dados, que determinam como informações pessoais de clientes, funcionários ou fornecedores são processadas, armazenadas, coletadas e utilizadas. Também é preciso atentar para as políticas e protocolos em relação à ética no uso dos dados — em particular, como gerenciar o uso legal das informações do cliente, atendendo às expectativas de uso desses próprios clientes. Gerenciar essas expectativas tem como objetivo mitigar possíveis riscos significativos para a reputação e a credibilidade da companhia, além de representar um desafio crítico para a liderança⁴⁸.

O incentivo pelo Estado à adoção de mecanismos de boas práticas, governança ou *compliance* representa uma forma de compartilhar atividade própria do Poder Público (isto é, a garantia do cumprimento da legislação) com agentes privados⁴⁹. Com a LGPD entrando em vigor, vislumbra-se

47 Disponível em: <https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends>. Acesso em 10 abr. 2024.

48 Disponível em: <https://kpmg.com/br/pt/home/insights/2024/02/conselho-de-administracao-2024.html>. Acesso em 10 de abril 2024.

49 Carvalho; Mattiuzo; Ponce, 2021, p. 364.

o início de uma mudança com uma quebra de paradigma ético-econômico-social vivenciado pelas empresas e pela sociedade hoje⁵⁰.

Então, ao entender a ética como o conjunto de princípios orientadores do comportamento humano em uma sociedade, a privacidade como o controle sobre informações e dados pessoais e o *compliance* como a observância das normas existentes para adequação do tratamento de dados pessoais no ciberespaço, constrói-se um caminho sólido para o tratamento dos dados pessoais. Ou seja, para um tratamento de dados pessoais correto, a atividade deve ir além das boas práticas e das questões de privacidade, mas também atentar para o lado ético da sociedade em que está inserida⁵¹.

As organizações públicas e privadas devem desenvolver um modelo de governança da privacidade e da proteção de dados que considere os riscos operacionais e implemente controles para gerenciá-los ou eliminá-los. É exatamente o Sistema de Gerenciamento da Segurança da Informação que dispõe as Normas Técnica ABNT NBR ISO/IEC 27001, 27002 e 27701⁵². A atenção à segurança da informação⁵³ é elemento chave para a mitigação de riscos que tenham sido

50 Saldanha; Pinheiro, 2020, p. 230.

51 Saldanha; Pinheiro, 2020, p. 233.

52 Jimene; Sicuto, 2020, p. 57.

53 A segurança da informação é uma “ciência voltada à gestão da informação, pautada nos seguintes pilares: a) confidencialidade da informação, que consiste na premissa de que a informação precisa ser conhecida somente por quem precise conhecê-la para exercer suas atividades profissionais, baseada no princípio *need to know*; b) disponibilidade da informação, com fulcro na premissa de que a informação deve estar disponível quando necessária para a execução dos trabalhos; c) integridade da informação, baseada na ideia de que a informação deve ser confiável, pois não sofreu alterações. Adicionalmente, outros atributos também podem ser associados à Segurança da Informação, como a autenticidade (veracidade da autoria da informação), o não repúdio (o autor não tem meios para negar ser o verdadeiro autor da informação) e a conformidade (o uso da tecnologia deve estar em conformidade com as leis vigentes do país)” (Jimene; Sicuto, 2020, p. 43).

apurados nas organizações e para a continuidade do negócio.

Não obstante a importância da governança e das boas práticas para o tratamento de dados pessoais, no sistema brasileiro, o perigo está justamente em que estes “Códigos de Boas Práticas” não é preventivamente avalizado pela ANPD. No entanto eles podem ser reconhecidos e divulgados pela ANPD, conforme dispõe o §3º do artigo 50⁵⁴.

De mais a mais, a ANPD previu para a Fase 1 de sua agenda de trabalhos para o biênio 2023-2024⁵⁵, o início da etapa de edição de regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais. Esse será um trabalho normativo que substituirá o guia inicial, de perguntas e respostas sobre o RIPD divulgado no portal da ANPD em abril de 2023⁵⁶.

Enquanto isso, na ausência de documentos regulatórios de orientação definitiva, reforça-se o peso das iniciativas de governança pelas organizações⁵⁷. Isso poderá até mesmo servir de subsídio para reduzir a aplicação de uma sanção pela ANPD, na forma do artigo 52, §1º, VIII da LGPD.

54 §3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional. (Lima, 2020, p. 229).

55 Resolução CD/ANPD nº 11, de 27 de dezembro de 2023, disponível em <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-11-de-27-de-dezembro-de-2023-534947737>. Acesso em 10 abr. 2024.

56 Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd/relatorio-de-impacto-a-protecao-de-dados-pessoais#p3. Acesso em 10 abr. 2024.

57 O governo federal divulga seu modelo de RIPD em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias-e-modelos>. Acesso em 10 abr. 2024.

3. Implementação da governança da privacidade e proteção de dados a partir do gerenciamento de riscos, do *compliance* e da *accountability*

Ainda que muito se fale em governança, esse termo não comporta um conceito único⁵⁸, tendo alguns pilares como a *accountability*, o *compliance* e o gerenciamento de riscos. É relevante compreender o alcance e o sentido da governança para entender o conteúdo e o espírito da LGPD, de forma a materializar o que se entende por governança, em especial, no contexto aqui proposto, qual seja, a governança da privacidade e da proteção de dados e as respectivas boas práticas.

A palavra risco aparece 11 (onze) vezes ao longo da LGPD, de modo que gestão de riscos é uma maneira de abordar um programa de conformidade e adequação à essa legislação. Disso derivam vários *frameworks* ou modelos de sistemas de implementação de governança da privacidade e da proteção de dados, os quais se pautam, em grande medida, numa abordagem baseada em risco (*risk based approach*).

Nesse sentido, antes mesmo do GDPR e da LGPD, em janeiro de 2014, o *Centre for Information Policy Leadership* (CIPL)⁵⁹ lançou um projeto relativo à privacidade de dados com abordagem baseada em risco: *The Privacy Risk Framework Project*. Como fruto desse projeto, em junho daquele ano, foi divulgado um artigo, sob o título *A Risk-based Approach to*

58 Vide ainda “Afiml, o que é governança?”. Disponível em: <https://www.migalhas.com.br/depeso/340109/afiml-o-que-e-governanca>. Acesso em 10 abr. 2024.

59 O CIPL é um *think tank* global de privacidade e política de dados, com sede em Washington, DC, Bruxelas e Londres, visando desenvolver soluções globais e melhores práticas para privacidade e uso responsável de dados para permitir a era da informação moderna. Sobre o CIPL: <https://www.informationpolicycentre.com/about.html>.

*Privacy: Improving Effectiveness in Practice*⁶⁰, que contempla uma matriz modelo de riscos. Considerando que as leis de proteção de dados e privacidade são destinadas a proteger pessoas e não dados, o ponto focal do mapeamento de riscos deve considerar riscos de privacidade significativos aos indivíduos. Isso deve ser avaliado diante de uma situação concreta ou passível de acontecer, de modo a se estimar a probabilidade da ocorrência de um ano.

Esse documento demonstra que a abordagem baseada em risco perpassa a mera conformidade às exigências regulatórias. Deve-se ir ao âmago das organizações para buscar o que se pretende atingir, verificar como são implementados os requisitos para atendimento à proteção de dados e como isso pode ser validado. Paralelamente à conformidade pelas organizações, a participação do ente regulador nesse contexto é igualmente destacada, cabendo-lhe avaliar a eficácia do processamento dos riscos.

Partindo do princípio de que riscos são geralmente mitigados, mas raramente eliminados, pode haver situações em que o regulador conclua que o processo de avaliação de riscos era razoável e completo, discordando, mesmo assim, da decisão final⁶¹. É imprescindível, dessa forma, que as au-

60 Disponível em https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf. Acesso em 10 abr. 2024.

61 The approach implies that regulators will need to assess the efficacy of risk processes. In keeping with the principle that risks are usually mitigated but seldom eliminated, there may be situations where a regulator concludes the risk assessment process was reasonable and complete but simply disagrees with the end decision. In that situation, the company may be especially exposed if the harm in fact materialises. In other situations, as the FTC has shown with imaginative use of consent decrees which impact on privacy programs, a regulator that finds fault with risk assessments is well placed to ensure constructively that its rulings have positive effects in the future (CIPL, 2014).

toridades regulatórias participem do processo de orientação para avaliação de riscos. Em certos casos, pode-se, por exemplo, emitir opiniões ou resoluções que orientem os agentes de tratamento, isto é, informem, por exemplo, níveis de aceitação e tolerância a riscos que poderão ser considerados.

A abordagem, baseada em risco, também é encontrada no GDPR, em seu Considerando 74, que estabelece as medidas que os controlares deverão considerar diante do risco para os direitos e liberdades das pessoas físicas, levando-se em conta juntamente a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados. Outros dispositivos que contemplem riscos, elevado risco ou avaliação de riscos podem ser encontrados no GDPR, especialmente, ao longo do Capítulo IV – Responsável pelo tratamento e subcontratante. Desse modo, a abordagem baseada em risco deve ocorrer à luz das probabilidades de gravidade⁶².

O Considerando 75, por sua vez, é uma espécie de norte orientativo ao apresentar hipóteses em que o tratamento de dados pessoais poderá acarretar risco aos direitos e liberdades individuais, como mencionado previamente. Com base no GDPR, a avaliação de riscos deve, portanto, considerar as ameaças potenciais em quaisquer tratamentos, tais como coleta excessiva ou injustificada de dados; uso ou armazenamento impreciso ou desatualizado de dados; uso impróprio ou mal uso dos dados, incluindo (i) uso dos dados além das expectativas razoáveis do titular; (ii) uso incomum de dados além das normas sociais, em que qualquer titular razoável nesse contexto se oporia; (iii) inferência ou tomada de decisão injustificada, para a qual a organização não consegue se defender objetivamente.

62 Disponível em https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21-december_2016.pdf. Acesso em 10 abr. 2024.

São ainda ameaças potenciais aos direitos e liberdades do titular, conforme a publicação *Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR*⁶³, a perda, ou o furto ou destruição e alteração de dados, bem como o acesso, transferência, compartilhamento ou publicação de dados não justificadamente ou sem autorização⁶⁴. Sinteticamente, é por meio do levantamento e gerenciamento de riscos que se poderá buscar a conformidade (estar em *compliance*), estabelecer mecanismos de responsabilização e prestação de contas (*accountability*), atingindo-se assim uma governança em benefício da organização e dos titulares de dados.

3.1 Levantamento de riscos e relatórios de impacto à proteção de dados

A análise de riscos é formada em duas etapas, o levantamento de riscos e o gerenciamento de riscos. Avaliar o risco é medir o seu nível de probabilidade e gravidade, ao passo que gerenciá-lo implica decidir aceitá-lo ou não⁶⁵, assim como evitá-lo, reduzi-lo ou compartilhá-lo. Como riscos são eventos futuros e incertos, não há garantias quanto ao seu controle prévio por completo, sendo possível, dentro das atividades de gerenciamento, identificá-los e mitigá-los. De acordo com a obra *Gerenciamento de Riscos Corporativos – Estrutura Integrada*, emitida em 2007 pelo *Committee of Sponsoring Organizations of the Treadway Commission (COSO)*⁶⁶, o geren-

63 CIPL, 2016, p. 26.

64 Disponível em https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf. Acesso em 10 abr. 2024.

65 <https://www.sciencedirect.com/science/article/abs/pii/S0267364917302698> (Gellert, 2018).

66 Disponível em <https://www.coso.org/documents/coso-erm-executive->

ciamento de riscos corporativos tem por finalidade (i) alinhar o apetite a risco com a estratégia adotada; (ii) fortalecer as decisões em resposta aos riscos; (iii) reduzir as surpresas e prejuízos operacionais; (iv) identificar e administrar riscos múltiplos e entre empreendimentos; (v) aproveitar oportunidades e (vi) otimizar o capital.

Tal obra contempla ainda uma orientação metodológica de identificação de eventos de uma organização assentada nos seguintes eventos: (i) identificação de eventos; (ii) análise interna; (iii) alçadas e limites; (iv) seminários e entrevistas com facilitadores; (v) análise de fluxo de processos; (vi) indicadores preventivos de eventos; e (vii) metodologia de dados sobre eventos de perda. Além disso, é preciso ter atividades de controle que incluam políticas que disciplinem o que deverá ser feito e os procedimentos para fazê-las serem cumpridas.

Como forma de impor a avaliação de riscos, o artigo 35º do GDPR prevê o “*Data protection impact assessment and prior consultation*” (DPIA), quando um determinado tipo de tratamento em particular que utilize novas tecnologias, considerando sua natureza no âmbito, contexto e finalidades, implicar em elevado riscos⁶⁷. Em realidade, na prática, considerando todos os elementos que devem ser utilizados para elaborar o relatório de impacto, é preciso que as organizações conduzam uma avaliação preliminar para determinar se o DPIA ou, no acrônimo em português, RIPD, é necessário.

Vale ressaltar, ainda, o papel consultivo do Encarregado da Proteção de Dados ou *Data Protection Officer* (DPO), em relação ao DPIA disciplinado no GDPR. Isso não quer dizer que esse profissional seja responsável por proceder ao DPIA ou seja o único responsável por essa avaliação. É

summary-portuguese.pdf. Acesso em 10 abr. 2024.

67 Lima, 2020, p. 227.

mais provável que outros da organização selecionem ou levantem os riscos preliminarmente e então submetam as questões mais complexas ou de alto risco ao DPO (CIPL, 2016, p. 40). Na LGPD, não há nenhuma disposição referente à atuação do encarregado no RIPD⁶⁸, sendo razoável supor que a ANPD se ampare na experiência do GDPR para editar norma regulamentares que disponham sobre essa questão.

O chamado *Article 29 Working Party* (WP29), composto por representantes de cada uma das autoridades de proteção de dados na União Europeia, adotou diretrizes para a elaboração dos DPIAs em casos em que o tratamento de dados tivesse a probabilidade de resultar em elevados riscos, nos termos do GDPR. Essas diretrizes foram endossadas pelo seu substituto, o Comitê Europeu de Proteção de Dados (*European Data Protection Board* – EDPB)⁶⁹, e auxiliam na compreensão das disposições do GDPR sobre o tema⁷⁰. Existem, nessas diretrizes, nove critérios que podem indicar elevado risco no tratamento de dados. No sentido oposto, o WP29 também identificou exemplos em que não haveria motivo para condução de um DPIA.

Esse trabalho é altamente relevante porque levou à formação de precedentes, por meio de listas publicadas pelas autoridades regulatórias de cada Estado-Membro da UE dos tipos de operações de tratamento sujeitas ou não à obrigatoriedade de realização do DIPA (art. 35(4) (5), GDPR)⁷¹. Essas listas são comunicadas ao EDPB periodicamente e podem ser usadas comparativamente por encarregados de dados e agentes de tratamento no Brasil, para atendimento às normas da LGPD.

68 Pessin; Lilla, 2020, p. 115.

69 Disponível em <https://ec.europa.eu/newsroom/article29/items/611236>. Acesso em 10 abr. 2024.

70 Pessin; Lilla, 2020, p. 109.

71 Pessin; Lillia, 2020, p. 113.

Uma outra circunstância que pode levar à conclusão de que um relatório de impacto deve ser conduzido é o registro das operações de tratamento, conforme previsto no art. 37 da LGPD. Esse registro é passível de identificar eventuais riscos potenciais que possam justificar a realização de relatórios de impacto⁷². De qualquer modo, a elaboração de um DPIA ou RPID tem, entre outros objetivos, gerar evidências de que as obrigações legais estão sendo cumpridas e que os riscos estão sendo endereçados.

O desafio para as organizações e para a governança é criar uma lista mínima de requisitos de padronização e controle sem o risco de se perder nos milhares de indicadores (KPI) que podem ser criados em um ambiente que procura vasculhar tudo e todos⁷³. Não obstante, o RIPD é um dos documentos mais importantes na implementação de um programa de governança da privacidade e da proteção de dados e poderá ser de elaboração facultativa ou, até mesmo, obrigatória, consoante o *caput* do art. 38, da LGPD.

Vale mencionar que de nada adianta elaborar o melhor RIPD, com a adoção das melhores práticas e processos, se as recomendações que forem obtidas como resultado desse trabalho não forem de fato implementadas pela organização⁷⁴. É preciso superar um grande desafio que ainda está presente nas organizações e consiste na mudança do *mindset*, na forma como é concebido o tratamento de dados pessoais e a internalização da responsabilidade que cada uma das áreas tem quando fazem o tratamento⁷⁵.

Quanto à eventual publicidade do RIPD, a LGPD não traz essa previsão, embora essa transparência, ainda que

72 Martins; Guariento, 2019.

73 Amaral, 2020, p. 111.

74 Palhares, 2019, p. 282.

75 Rodriguez, 2020, p. 388.

parcial, possa vir a ser ponderada pelas organizações. Sem embargo, avaliações detalhadas de impacto e risco de privacidade devem ser realizadas e publicadas, documentando claramente os riscos de privacidade e todas as medidas tomadas para mitigação, considerando-se as alternativas presentes e métricas selecionadas⁷⁶. Somado ao fato de que, na prática, não há obrigatoriedade publicar o RIPD, tampouco é preciso o submeter previamente à ANPD. Eventual envio dependerá de requisição por parte da autoridade⁷⁷, sendo mandatória sua elaboração em situações que ainda dependerão de regulamentação⁷⁸.

Em todo caso, o relatório deve ser efetuado, seja por conta de sua importância e vantagens que podem ser obtidas pela entidade, seja porque a autoridade poderá o solicitar a qualquer momento. A privacidade deve fazer parte da construção e arquitetura dos sistemas de TI (tecnologia da informação) e das práticas empresariais. Não se trata de um adicional ao projeto, mas de uma atividade essencial desde o início, que possa inclusive ser objeto de análises e auditorias externas⁷⁹.

76 Cavoukian, 2009, p. 3.

77 O §3º, do artigo 10 da LGPD, estabelece que a autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial. O setor público também poderá ser instado a entregar o RIPD, tomando-se por base o §3º, do art. 4º da LGPD.

78 Nos termos do artigo 38 da LGPD, a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

79 Cavoukian, 2009, p. 3.

3.2 Relatórios de impacto à proteção de dados pessoais na prática

A LGPD traz apenas alguns indicativos para a produção de um RIPD, sendo certo que o relatório deverá conter (i) descrição dos processos de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais, (ii) descrição dos tipos de dados coletados; (iii) metodologia utilizada para a coleta e para a garantia da segurança das informações; e (iv) medidas, salvaguardas e mecanismos de mitigação de risco devidamente analisadas pelo controlador.

Nesse sentido, a ANPD divulgou, em abril de 2024, com base no artigo 38 da LGPD, que o RIPD deve conter, no mínimo, (i) a descrição dos tipos de dados pessoais coletados ou tratados de qualquer forma; (ii) a metodologia usada para o tratamento e para a garantia da segurança das informações; e (iii) a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados⁸⁰.

Existe, portanto, considerável espaço para posterior regulação por parte da ANPD acerca da exata operacionalização dos relatórios de impacto à proteção de dados pessoais⁸¹. Isso é inclusive esperado por meio da edição de regulamentos e procedimentos, configurando uma das competências da ANPD, conforme o inciso XIII, do artigo 55-J da LGPD. Ocorre, no entanto, que a LGPD já está vigente, de maneira que os controladores não podem deixar para conduzir uma avaliação de riscos e produzir um RIPD somente depois que houver a regulamentação.

80 Vide: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p6.

81 Carvalho; Mattiuzo; Ponce, 2021, p. 369.

Essa questão é tão importante que se espera para 2024 a edição de uma Resolução pela ANPD sobre os RIPDs, considerando que esse tema é objeto da Fase 1 da agenda regulatória bienal proposta pela autoridade para o biênio 2023-2024⁸². Enquanto isso, diante da ausência de maiores subsídios fornecidos pela ANPD, é preciso se pautar em outras iniciativas ou modelos para a consecução de um RIPD. Os modelos de risco definem os fatores a serem avaliados e as relações entre tais elementos. Caso uma organização não esteja usando um modelo de risco pré-definido, ela deve especificar claramente quais os fatores de risco que serão avaliados e as relações entre esses fatores⁸³.

Em termos de modelos de relatórios de impacto, existem aqueles divulgados, por exemplo, pelas mais conhecidas autoridades europeias de proteção de dados, como o *Information Commissioner's Office* (ICO) do Reino Unido⁸⁴, pela *Commission Nationale de l'Informatique et des Libertés* francesa (CNIL)⁸⁵ e pela *Agencia Española de Protección de Datos* (AEPD)⁸⁶. Adicionalmente a esses modelos, existem outros, como o do *NIST Privacy Framework*, do *National Institute of Standards and Technology*, do Departamento de Comércio dos Estados Unidos⁸⁷.

82 Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-11-de-27-de-dezembro-de-2023-534947737>. Acesso em 10 abr. 2024.

83 NIST, 2020, p. 40.

84 Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/>. Acesso em 10 abr. 2024.

85 Disponível em: <https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd>. Acesso em 10 abr. 2024.

86 Disponível em: <https://www.aepd.es/es/documento/guia-evaluaciones-de-impacto-rgpd.pdf>. Acesso em 10 abr. 2024.

87 Disponível em: <https://doi.org/10.6028/NIST.CSWP.01162020>. Acesso em 10 abr. 2024.

Em solo pátrio, além de existirem as Normas ABNT ISO/IEC relativas à gestão de riscos e segurança da informação, especialmente a 27701:2019, que já se baseia na LGPD, encontramos exemplo proposto pelo governo federal. Visando auxiliar os órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) durante o processo de adequação à LGPD, a Secretaria de Governo Digital publicou diversos guias operacionais⁸⁸. Entre essas contribuições, encontra-se uma Ferramenta para Avaliação de Riscos de Segurança e Privacidade, além de um modelo de RIPD. Complementarmente, é possível assistir, gratuitamente, a vídeos de oficinas que foram conduzidas por representantes da administração pública e ler documentos de suporte⁸⁹.

Diante do exposto, verifica-se que há farto material de fácil acesso que serve como ponto de partida para a elaboração do RIPD; todavia, para a grande parte dos controladores que deverão cumprir essa obrigação legal, esse é um terreno muito desconhecido. Num ambiente de incertezas, uma alternativa é executar o RIPD e revisá-lo, posteriormente para aprimoramento. À medida que o grau de conformidade e de maturidade perante legislação aumentem, esse relatório tenderá a ser mais robusto, servindo como instrumento efetivo para embasar decisões pelas organizações.

Essa revisão deve ocorrer até mesmo para a atualização dos possíveis impactos estimados, vez que as condições inicialmente analisadas podem mudar com o passar de apenas alguns meses, por exemplo. As matrizes de risco

88 Disponíveis em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd>. Acesso em 10 abr. 2024.

89 Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias-e-modelos>.

não são necessariamente estáticas, pois devem acompanhar a evolução das operações dos entes públicos e privados. A retomada periódica do RIPDa é, aliás, uma boa prática a ser incorporada no desenho do programa de governança da privacidade e da proteção de dados e seus correspondentes *Data Compliance Measure Set* ou *Privacy & Data Protection Measure Set*⁹⁰.

4. Conclusão

A obrigação legal de adequação às normas de proteção dos dados pessoais é uma realidade. Não é mais possível que as organizações públicas e privadas adiem a absorção dos dispositivos da LGPD. Para que a conformidade legal possa se materializar, é preciso que empresas e órgãos da administração pública direta e indireta invistam no desenvolvimento e implementação de programas de governança e boas práticas, em cumprimento às disposições da LGPD. Isso deve ocorrer por meio do estabelecimento de mecanismos de *compliance*, gerenciamento de riscos e *accountability*.

As altas lideranças devem incluir essas atividades como mandatórias e rotineiras no direcionamento da gestão e no comando das operações, incentivando o desempenho de tarefas preventivas voltadas à identificação e mitigação de riscos, além do monitoramento de indicadores chave, relativos à proteção de dados pessoais e ao atingimento dos resultados esperados. É importante que haja proatividade nas ações por parte das organizações, agindo com transparência e respeito aos direitos dos usuários, estabelecendo processos bem descritos e monitoramento constantes.

A concretização de um sistema de governança da privacidade e da proteção de dados e a adoção das chamadas

90 Rodriguez, 2020, p. 410.

boas práticas contribui para o aprimoramento de operações das organizações, além da preservação da reputação e a sustentabilidade do negócio ou serviço. Mesmo que a ANPD ainda não tenha regulamentado o que se espera em termos de governança e boas práticas, as organizações não podem postergar essas condutas. É preciso que haja a incorporação de uma nova cultura voltada à proteção de dados, especialmente porque a LGPD já está vigente.

Embora, a ANPD permaneça adotando uma postura mais pedagógica do que propriamente punitiva, o mercado já vem exigindo a conformidade com a LGPD, seja porque já foram ajuizadas algumas ações perante o Poder Judiciário, seja porque a autorregulação faz com que essa necessidade se espalhe para outras organizações. Não se trata, assim, apenas de prevenir eventuais multas administrativas. É imperativo que se compreenda que a governança da privacidade e da proteção de dados e a implementação de boas práticas traz benefícios às organizações e, principalmente, aos titulares de dados pessoais.

Bibliografia bibliográficas

A RISK-BASED Approach to Privacy: Improving Effectiveness in Practice. 2014. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf. Acesso em: 10 abril 2024.

ACCOUNTABILITY: Data Governance for the Evolving Digital Marketplace1. 2011. Centre for Information Policy Leadership. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/accountability-data_governance_for_the_evolution_digital_marketpla

ce__april_2011_.pdf. Acesso em: 10 abril 2024.

ALSENOY, Brendan Val. Allocating responsibility among controllers, processors, and “everything in between”: the definition of actors and roles in Directive 95/46/EC. **Computer Law & Security Review**, [s. l], v. 28, n. 1, p. 25-43, fev. 2014. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0267364911001828>. Acesso em: 10 abril 2024.

AMARAL, Armando Lima. O desafio de cyber security em grandes e heterogêneas estruturas. In: MONTANARO, Domingo; GIOVA, Giuliano; BLUM, Renato Opice. **Cyber Risk: estratégias nacionais e corporativas sobre riscos e segurança cibernética**. São Paulo: Thomson Reuters, 2020. Cap. 5. p. 109-118.

ANDRESANI, Gianluca; STAMILE, Natalina. Transparency in internet regulation and governance: arguments and counter-arguments with some methodological reflections: Transparência na regulação e na governança da internet: Argumentos e contra-argumentos com algumas reflexões metodológicas. **Revista Brasileira de Estudos Políticos (RBEP)**, Belo Horizonte, ano 2018, n. 117, p. 443-476, 1 dez. 2018. DOI 10.9732/P.0034-7191.2018V117P443. Disponível em: <https://periodicos.ufmg.br/index.php/rbep/article/view/17598/14382>. Acesso em: 16 abr. 2024.

BARBIERI, Carlos; FARINELLI, Fernanda. Uma visão sintética e comentada do Data Management Body of Knowledge (DMBOK). FUMSOFT, 16 abr. 2024. DOI 10.13140/RG.2.1.1561.2561. Disponível em: https://www.researchgate.net/publication/297699158_Uma_visao_sintetica_e_comentada_do_Data_Management_Body_of_Knowledge_DMBOK. Acesso em: 10 abr. 2024.

BARRETO JUNIOR, Irineu Francisco; LEITE, Beatriz Salles Ferreira. Responsabilidade civil dos provedores de aplicações por ato de terceiro na lei 12.965/14 (marco civil da internet). **Revista Brasileira de Estudos Políticos (RBEP)**, Belo Horizonte, ano 391, n. 115, p. 438, 16 jul. 2017. DOI 10.9732/P.0034-7191.2017V115P391. Disponível em: <https://periodicos.ufmg.br/index.php/rbep/issue/view/956>. Acesso em: 16 abr. 2024.

BELLI, Luca. Como implementar a LGPD por meio da avaliação de impacto sobre privacidade e ética de dados (AIPED). In: DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otávio Luiz; MENDES, Laura Schertel (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. Cap. 20. p. 389-419.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

CAVOUKIAN, Ann. **Privacy by Design: the 7 foundational principles**. The 7 Foundational Principles. 2009. Disponível em: <https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>. Acesso em: 10 abril 2024.

CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. Boas práticas e governança na LGPD. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otávio Luiz; MENDES, Laura Schertel (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. Cap. 18. p. 361-374.

Código das melhores práticas de governança corporativa. 5.ed. Instituto Brasileiro de Governança Corporativa. São Paulo: IBGC, 2015.

Gerenciamento de riscos corporativos: evolução em governança e estratégia. Instituto Brasileiro de Governança

Corporativa. São Paulo: IBGC, 2017 (Sério Cadernos de Governança Corporativa, 19).

JIMENE, Camilla do Vale; SICUTO, Guilherme Hernandes. Segurança da informação sob a perspectiva da legislação brasileira: aspectos relevantes. In: MONTANARO, Domingo; GIOVA, Giuliano; BLUM, Renato Opice. **Cyber Risk: estratégias nacionais e corporativas sobre riscos e segurança cibernética**. São Paulo: Thomson Reuters, 2020. Cap. 2. p. 41-60.

KISCHELEWSKI, Flávia Lubieska das Neves. **Startups, pequenas empresas e LGPD: o desafio da regulamentação**. 2021. Disponível em: <https://www.conjur.com.br/2021-fev-11/kischelewski-startups-pequenas-empresas-lgpd>. Acesso em: 10 abril 2024.

LIMA, Cíntia Rosa Pereira de. **Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados: de acordo com a Lei Geral de Proteção de Dados (Lei n. 13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco Civil da Internet (Lei 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015)**. 1ª ed. São Paulo: Almedina, 2020.

MARTINS, Ricardo Maffeis; GUARIENTO, Daniel Bittencourt. Adequação à LGPD: uma oportunidade para empresas reverem seus modelos de negócio e desenvolverem novos produtos. **Migalhas**, [s. l], 27 set. 2019. Disponível em: <https://www.migalhas.com.br/coluna/impressoes-digitais/311707/adequacao-a-lgpd--uma-oportunidade-para-empresas-reverem-seus-modelos-de-negocio-e-desenvolverem-novos-produtos>. Acesso em: 10 abril 2024.

MEIRA, Silvio. **#DADOS não são o “novo PETRÓLEO”**. 08 jan. 2020. Twitter: @srlm. Disponível em: <https://twitter>.

com/srlm/status/1214986628336250880. Acesso em: 10 abril 2024.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO: tendências contemporâneas de materialização. **REI - REVISTA ESTUDOS INSTITUCIONAIS**, [S.l.], v. 6, n. 2, p. 507-533, set. 2020. ISSN 2447-5467. Disponível em: <https://www.estudosinstitucionais.com/REI/article/view/521/510>. Acesso em: 10 abril 2024.

NEGRÃO, Antônio Carlos. Economia digital, proteção de dados e competitividade. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas. **Lei Geral de Proteção de Dados (Lei 13.709/2018)**: a caminho da efetividade: contribuições para a implementação da lgpd. São Paulo: Revista dos Tribunais, 2020. p. 29-37.

PALHARES, Felipe. O relatório de impacto à proteção de dados pessoais. In: MALDONADO, Viviane Nóbrega; TAMER, Maurício. **LGPD: lei geral de proteção de dados pessoais: manual de implementação**. São Paulo: Thomson Reuters, 2019. Cap. 7. p. 247-287.

PESSIN, Marcos Vinícius Palomo; LILLA, Paulo. Relatório de impacto à proteção de dados e avaliação de legítimo interesse. In: BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti. **Data Protection Officer (Encarregado)**: teoria e prática de acordo com a lgpd e o gdpr. São Paulo: Thomson Reuters, 2020. p. 105-134.

RODRIGUEZ, Humberto de Jesús Ortiz. A prática do monitoramento dos programas de privacidade e proteção de dados pessoais e as auditorias legais e contratuais: transparência, responsabilidade e prestação de contas. In: BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabret-

ti. **Data Protection Officer (Encarregado)**: teoria e prática de acordo com a LGPD e o GDPR. São Paulo: Thomson Reuters, 2020. p. 387-411.

SALDANHA, Paloma Mendes; PINHEIRO, Bárbara Santi-ni. Data Protection Officer (Encarregado) - Teoria e Prática de acordo com a LGPD e o GDPR - Gestão de terceiros. In: BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti. **Data Protection Officer (Encarregado)**: teoria e prática de acordo com a lgpd e o gdpr. São Paulo: Thomson Reuters, 2020. p. 172-197.

TRIVELATO, Bianca Freire; MENDES, Daniel Pacheco; DIAS, Marco Antônio. A importância do gerenciamento de riscos nas organizações contemporâneas. **Refas**: Revista da FATEC Zona Sul, São Paulo, v. 4, n. 2, p. 1-20, 1 fev. 2018. Disponível em: <http://www.revistarefas.com.br/index.php/RevFATECZS/article/view/147/141#>. Acesso em: 10 abril 2024.

WOLKART, Erik Navarro; BECKER, Daniel; BRUZZI, Eduardo. **Estamos trancados num paiol de pólvora: LGPD, ANPD e demandismo**: nova lei pode fazer explodir inúmeros litígios pelo país. Nova lei pode fazer explodir inúmeros litígios pelo país. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/regulacao-e-novas-tecnologias/estamos-trancados-num-paiol-de-polvora-lgpd-anpd-e-demandismo-20072019>. Acesso em: 10 abril 2024.

Recebido em: 29/06/2021
Aprovado em: 16/04/2024

Grace Ladeira Garbaccio
E-mail: glgarbaccio@hotmail.com

Flávia Lubieska Neves Kischelewski
E-mail: flavialubieska@hotmail.com

