e³ – Revista de Economia, Empresas e Empreendedores na CPLP
Volume 08 Número 01 | 10.29073/e3.v8i1.618

A LGPD E A Risk-Based Approach Da Governança Corporativa: A Primeira Medida Para O Controlador Aplicar Os Princípios

GDPR And The Risk-Based Approach To Corporate Governance: The First Measure For The Controller To Apply The Principles

Júlia Zimmermann Ghisleni
Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS
juliazghisleni@gmail.com

Conflito de interesses: nada a declarar. Financiamento: nada a declarar.

Histórico:
Submissão | Received: 22/03/2022
Aprovação | Accepted: 29/03/2022
Publicação | Published: 31/03/2022

Volume 08 Número 01 | 10.29073/e3.v8i1.618

Resumo

A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados) instituiu diretrizes para o tratamento de dados de pessoas naturais brasileiras, que devem ser adotadas pelo controlador e equilibradas com os princípios e bases legais previstos na Lei. No presente artigo será realizada uma breve contextualização da GDPR e *Data protection governance* e aprofundadas as principais características da governança corporativa. Isto posto, terá como objetivo de embasar a correlação entre os princípios da LGPD e o pilar do *Accountability* (prestação de contas) da governança corporativa. Além disso, será verificado se o controlador, ao prestar contas sob o regime da LGPD, poderá se respaldar na abordagem baseada em riscos.

Palavras-chave: Lei Geral de Proteção de Dados, Governança corporativa, Prestação de contas, Gestão de riscos

Abstract

The law no. 13,709/2018 (General Data Protection Law or *Lei Geral de Proteção de Dados*) instituted directives for safe data processing of any native Brazilian, which must be adopted by controllers and balanced according to the principles and legal basis described by this law. In the present article, a brief contextualization of the connection between GDPR and data protection governance will be established, in addition to a conceptualization of the main features of corporate governance. After having these concepts clarified, a correlation between the principles of GDPR and the definition of corporate governance's accountability will be sought. Furthermore, it will be verified if controllers, when exercising accountability under the GDPR's regime, will be able to rely on the risk-based approach.

Keywords: General Data Protection Regulation, Corporate governance, Accountability, Risk management

Sumário

1. Introdução

O direito à privacidade não é um conceito recente para a ciência jurídica. Ele se origina da Declaração Universal dos Direitos Humanos e foi trazido para dentro do extenso rol de direitos fundamentais do art. 5º da Constituição Federal[3]. Como muitas outras normas constitucionais, é caracterizado por ser um conceito que propositalmente permite interpretação ampla e diversificada, para poder se adequar à realidade fática do estado no decorrer do tempo (Lages, Durães & Santos, 2015). No contexto da sociedade da informação, no qual os dados contam com alto valor para as empresas, o debate de como a privacidade deve ser abordada é amplificado, razão pela qual se fez necessária a Lei Geral de Proteção de Dados.

De um ponto de vista, a legislação de proteção de dados representa para o cidadão segurança e empoderamento para opinar sobre o compartilhamento de suas informações. Já para as organizações às quais essas informações serão fornecidas, a aludida lei representa um desafio ético, no qual novas diligências deverão ser tomadas para firmar os novos direitos trazidos. Isso posto, já é conhecido que a governança corporativa é um sistema pelo qual se assegura a ética empresarial, na qual um dos principais pilares é a prestação de contas. No entanto, pouco se sabe como a noção de prestação de contas será abordada em face dos valores da LGPD, principalmente para as organizações que tomarão as principais decisões envolvendo a gestão dos dados dos seus titulares.

Face às observações expostas, o presente trabalho tem como objetivo identificar de que forma o princípio da prestação de contas, incidente no controlador, relaciona-se com os outros princípios da LGPD sob a ótica da governança corporativa. Para esse fim, será destacada a definição de *Accountability* e a sua necessidade no ambiente corporativo, bem como serão conceituados, inicialmente, os princípios que promovem os valores centrais do decreto, os quais qualificam o consentimento dos titulares. Após, serão definidos os princípios que possuem função preventiva (por estabelecimento de sanções da LGPD) e como poderiam incentivar o controlador a agir na direção pretendida pelos valores da LGPD. Por fim, serão identificados o princípio da prestação de contas, a sua relação com os demais princípios da lei e como essa relação deverá ser interpretada pelo controlador.

De antemão, já se elucida que a pesquisa não irá adentrar nos conceitos de *data protection officer* e no relatório de impacto à proteção de dados, trazidos também pela LGPD - embora contem com grande relevância temática no âmbito da prestação de contas, cujo conceito será discutido mais adiante. Em vez disso, o trabalho pretende, via pesquisa teórica e bibliográfica, analisar os princípios da LGPD e proporcionar ao controlador a iniciativa mais adequada para interpretá-los e demonstrá-los. Tal iniciativa será restringida a um referencial adotado para colocar em prática os demais instrumentos da prestação de contas descritos em lei.

2. Conceitos Preliminares

2.1 A GDPR e a governança de dados: uma breve contextualização

Em 25 de janeiro de 2012, instaurou-se, pela Comissão da União Europeia, uma proposta legislativa com o intuito de amparar a coleta e o processamento de dados dos seus cidadãos. Após 3 anos de estudos e diálogos em tramitação na Comissão, aprovou-se um marco regulatório que impactaria subsequentemente não só a proteção de dados dos 28 países-membros da União Europeia, como também países que contratam com empresas sujeitas à tal regulamentação, como o Brasil. Sendo reflexo de um progressivo esforço de instituições e leis encaminhadas na direção da privacidade ao longo das últimas décadas, na União Europeia, a *General Data Protection Regulation* (GDPR) foi, assim, um passo relevante no direito à privacidade no meio ambiente digital[4].

A compreensão jurídica da proteção de dados pessoais, como uma extensão do direito fundamental à privacidade[5], para o direito europeu, foi um fator diferencial, tornando as suas políticas legislativas, ao longo dos anos, referenciais na tutela efetiva do direito fundamental supramencionado - em contraste com as demais jurisdições que foram complacentes com a comoditização do compartilhamento de dados. Tal fato possibilita que muitas empresas controladoras abusem da sua posição no mercado (Sharma, 2019).

No tocante à vantagem da qual gozam as empresas controladoras referentes ao acesso e ao compartilhamento de dados, tem-se uma percepção - superficial - de que a pessoa natural esteja, de fato, sob controle dos seus dados, principalmente, quando depende do fornecimento deles para obter emprego, informação, bens e outros serviços (Kiss & Szoke, 2015). Diante de tal pretexto, é perceptível que tal abordagem do Estado, ao considerar a proteção dos dados pessoais uma forma de manifestar direitos fundamentais, é benéfica para os titulares.

Isso, na prática, é assegurado de maneira que novos direitos são atribuídos aos titulares e novos deveres são atribuídos aos controladores e operadores[6] pelo regulamento de proteção de dados. Diante de novos deveres e sanções legalmente expressos e direcionados à proteção e ao tratamento de dados, impostos aos controladores, surge a necessidade de implementação de políticas de gestão voltadas para mitigar os potenciais riscos gerados pela coleta e compartilhamento de dados, direcionadas à prevenção e à minimização de danos em casos de violações aos novos dispositivos legais dessa categoria (Vainzof & Frabretti, 2020).

Para melhor elucidação do conceito de tratamento de dados, Russo (2019) os define como:

> *[...] toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento armazenamento, eliminação, avaliação ou controle de informação, modificação, comunicação, transparência, difusão ou extração.*

Ainda nesse cenário, encaixa-se a governança corporativa, visto que esse sistema é fundamental para a promoção de práticas que garantam maior segurança às informações atinentes aos seus titulares, bem como para preservar a reputação dos controladores frente

ao seu público (Blok, 2020). Apoiando-se nessa noção, será demonstrado que a legislação de proteção de dados brasileira privilegia as organizações que adotam programas de governança e privacidade.

2.1.1 A governança corporativa

Naquilo que se insere no conceito de governança corporativa, convém defini-lo conforme o Código de Melhores Práticas do Instituto Brasileiro de Governança Corporativa (2015, p. 20):

> *Governança corporativa é o sistema pelo qual as empresas e demais organizações[7] são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum.*

Partindo do pressuposto de que essa é uma estrutura de relações, práticas e regras que garante a sustentabilidade da empresa em longo prazo (Rossetti, 2004), é possível afirmar que pode ser usada para a prevenção de conflitos entre *stakeholders*[8], estruturas de poder desproporcionalmente concentradas, degeneração da imagem frente aos investidores e consumidores, tomada de decisões de forma arbitrária e prejudicial, bem como a corrupção no meio empresarial.

Levando em consideração a conciliação de interesses e proteção dos grupos mais vulneráveis das organizações, a governança exerce o seu alcance tendo como suporte quatro princípios: transparência da organização (no que diz respeito às suas informações prestadas perante os interessados); equidade (de tratamento entre sócios e demais interessados); responsabilidade corporativa (perante os interessados, de forma que aja em conformidade com a lei) e *accountability* (Grupo de Trabalho Interagentes, 2016).

Consequentemente, observa-se igualmente, com isso, que os riscos que podem ser gerados no âmbito da proteção de dados podem ser eficientemente gerenciados pela abordagem da governança corporativa.

2.1.2 O princípio do Accountability (prestação de contas)

Dentro do amplo rol de diretrizes de gestão englobadas pela governança corporativa, o princípio da prestação de contas se insere como um dos seus quatro principais pilares. Trata-se de dever imposto aos agentes da governança corporativa, classificados pelo IBGC (2015, p. 91) da seguinte forma:

> *[...] indivíduos e órgãos envolvidos no sistema de governança, tais como sócios, conselheiros de administração, diretores, conselheiros fiscais, auditores, entre outros [...] responsáveis por assegurar que toda a organização esteja em conformidade com os seus princípios e valores, refletidos em políticas, procedimentos de controle e normas internas, e com as leis e os dispositivos regulatórios a que esteja submetida.*

Não obstante, o dever acima referenciado se tratar da premissa de que o ato de prestar contas deve ser realizado com expressas diretrizes. Além disso, pressupõe-se que os agentes da governança corporativa tenham responsabilidade jurídica e todas as suas condutas precisam ser expressas, registradas, organizadas, frequentes e padronizadas (Giacomelli, 2017). Esse sistema permite maior transparência e comunicação entre os grupos de interesse existentes dentro e fora de uma

companhia. Por conseguinte, é inevitável que as atribuições impostas à gestão das organizações e asseguradas pelo *Accountability* sejam amplificadas frente a uma nova legislação de proteção de dados.

Na alçada dos reflexos da GDPR, algumas mudanças foram instituídas aos controladores, de forma que se criou uma *Corrente de Accountability*. Em outras palavras, as empresas controladoras terão mais obstáculos se tentarem evadir a sua responsabilidade jurídica, quando adentrar na coleta e no tratamento de dados, pois tanto o controlador quanto o operador têm o dever de prestar contas, bem como entre cocontroladores e cocoperadores, isto é, em todo o escopo da sua relação de compartilhamento e coleta de dados. Percebeu-se, assim, que dificilmente um controlador irá desviar-se da sua responsabilidade, alegando desconhecimento das práticas de um operador com quem está relacionado, por exemplo (Sharma, 2019)[9]. Trata-se de uma cadeia de gestão e responsabilidade pelo tratamento de dados (Falcão & Keller, 2021).

2.2 A governança dos dados no cenário brasileiro

Inicialmente, é pertinente delimitar que o conceito de proteção de dados se constitui como uma parte do direito fundamental à privacidade, o qual está assegurado no art. 11 do Código Civil[10], presente no rol de direitos da personalidade, sendo assim, intransmissível, irrenunciável e não voluntariamente limitável (Lima, 2020). Anteriormente a 2020, já havia diligências do ordenamento jurídico brasileiro na direção de amparar a privacidade de dados, sendo uma amostra disso o Código de Defesa do Consumidor, no seu art. 43[11] e o Marco Civil da Internet, legislação basilar para a LGPD.

Não obstante, no Brasil, o conceito de governança de dados recebe maior relevância com a chegada da Lei Geral de Proteção de Dados (LGPD). Isso se deve, sobretudo, ao fato de que a lei possui grande amplitude de aplicação, propondo-se a tutelar toda operação de tratamento de dados de pessoas naturais, no meio ambiente digital ou não, em território nacional, realizada pelos seus agentes. As categorias e competências desses últimos se subdividem, essencialmente, no que diz respeito ao tratamento de dados, entre a tomada de decisões nesse meio (controladores) e a sua execução (operadores).

No que intercede à LGPD com as demandas do mercado de investidores, nota-se que as exigências tendem a promover valores que reforcem a transparência, a sustentabilidade, bem como a defesa dos interesses de todos *stakeholders*. Isso vem sendo reafirmado por entidades internacionais como a *Business RoundTable*[12] e o Fórum Econômico Mundial de 2020[13] – nesse último, traçaram-se parâmetros para a cultura organizacional para as empresas nos próximos anos. Mais especificamente, os próximos objetivos que entidades internacionais traçaram para internalizar nas organizações serão direcionados aos temas Ambientais, Sociais e de Governança Corporativa[14].

Condiz afirmar que a adequação à LGPD se encaixa nesses parâmetros[15], dado que os conceitos de integridade e transparência sendo usados como meios de materializar um direito fundamental também são valores propostos pela nova legislação, estando inseridos, sobretudo, no tema da governança corporativa. Para as organizações, estar nos termos da LGPD será não só requisito mínimo para bons negócios no Brasil, como também para evitar os riscos presentes nas penalidades da lei (Redecker, 2020).

3. *ACCOUNTABILITY* e os princípios da LGPD: uma relação de interdependência

Ao se analisar os princípios da LGPD, é pertinente reiterar que boa parte dos dispositivos do decreto nº 13.709[16] se volta para tutelar os interesses do titular, de maneira que sejam preservados, simultaneamente, o desenvolvimento e a inovação[17]. Por conseguinte, os seus princípios estão centrados no ser humano, caso em que o legislador optou por priorizar a participação do indivíduo no fluxo de suas informações (Teffé & Viola, 2020). Adicionalmente, destaca-se também a tendência do legislador em regulamentar o tratamento de dados com base em princípios, em detrimento da imposição de deveres aos agentes de tratamento de forma específica e taxativa, em decorrência da sua aplicabilidade abrangente (Pestana, 2020).

Nesse sentido, importa ser aprofundados os conceitos relativos ao consentimento do titular e como esses princípios – expressos no art. 6º da legislação – se chocarão com os deveres do *Accountability*, a serem assumidos pelo controlador. Posteriormente, a principiologia da LGPD será também contemplada pelo ângulo do seu caráter sancionatório imposto ao controlador para, finalmente, incorporá-la com o dever de prestar contas, tanto expresso pela LGPD, quanto pela governança corporativa.

3.1 Dos princípios derivados do consentimento livre, informado e inequívoco[18]

Para atingir essa finalidade, o titular dos dados precisa estar dotado de autonomia informativa. Trata-se, de outro modo, de possibilitar que ele participe ativamente no ciclo de vida dos seus dados, tendo informações acessíveis a respeito do tratamento deles, quem o detém, bem como a finalidade para o qual serão destinados (Canto et al., 2019). Ainda, a concepção de liberdade do titular é efetivada ao ter-se a garantia de que não haja vícios de consentimento, possibilitando a faculdade de aceitar ou recusar os termos do controlador (Tefé & Viola, 2020). Para tanto, o indivíduo precisa estar guarnecido das informações necessárias para compreender a extensão do tratamento dos seus dados.

Por consequência, mostra-se imperativo o livre acesso do titular aos seus dados, podendo consultar informações referentes ao seu tratamento, devendo estar os dados devidamente atualizados, conforme o art. 6º IV e V da LGPD[19], respectivamente (Flumignan, 2020). Isso deve ser assegurado pelo controlador de maneira que estejam em consonância com a transparência, finalidade, necessidade e adequação.

Na LGPD, descreve-se o seu art. 6º como transparente à atividade de tratamento de dados, que é realizada com o fornecimento de "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial". À vista disso, é necessário que o controlador se atente ao momento do fornecimento de tais informações e da sua qualidade, uma vez que o titular pode requerer informações antes, durante e após o tratamento de dados. Em outras palavras, leva-se em consideração que na sua relação jurídica com o titular incide o princípio da boa-fé contratual objetiva[20]. A respeito dessa última, ela se define como um dever de lealdade e

honestidade entre os contratantes, o qual recai em todas as fases do contrato. Nessa mesma linha de raciocínio, esclarece Soares e Câmara (2012, p. 9-30): "A boa-fé objetiva é típica das relações contratuais e pré-contratuais, exige das partes um comportamento standard, avaliando-se as atitudes de cooperação e confiança das partes e o respeito por seus interesses respectivos".

No que se compreende como finalidade, o art. 6º, I, da aludida legislação, estabelece que o "tratamento dos dados pessoais deverá ser realizado com propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades". Como reflexo desse princípio, concebe-se uma limitação imposta à atuação do controlador, permitindo o tratamento de dados em proporção limitada àquele propósito que foi informado. A partir dessa definição, deduz-se que a comunicação do controlador com o titular a respeito do propósito da coleta de dados – ou da modificação do referido propósito – estará vinculada ao consentimento informado.

Outrossim, é necessário que o tratamento dos dados seja realizado, considerando-se a "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados", haja vista o inciso III do art. 6º da LGPD. Destarte, desse conceito decorre a noção de uma coleta de dados restrita ao imprescindível. Adicionalmente, pressupõe-se uma preocupação maior imposta ao controlador em categorizar quais serão os dados necessários, diante do aumento de responsabilidade jurídica atribuída ao agente ser proporcional à quantidade de dados extraídos pelo titular[21].

Por fim, do princípio da adequação, com previsão no art. 6º, II da lei, depreende-se "a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento". Do princípio resulta, para o controlador, a necessidade de firmar coerência entre os dados coletados com os objetivos estabelecidos em contrato.

Uma investigação aprofundada dos principais princípios que circundam o consentimento pode sugerir que a extensa quantidade de exigências para adquiri-lo representa uma exigência excessiva para os agentes de tratamento, circunstância que pode incentivar os controladores à busca pelo uso de outras bases legais para o tratamento. Diante disso, além de atribuir importância e proteção jurídica consideráveis ao consentimento, a LGPD precisa, em mesma proporção, encontrar outras ferramentas para assegurar a privacidade. Um exemplo disso seria a criação de incentivos ao controlador pela redução de sanções previstas na lei, vinculadas nas hipóteses em que, se incorrer em ilicitude, ficar demonstrado que houve maior preocupação em reduzir os danos aos titulares (Sombra, 2019).

3.2 Dos princípios com funções preventivas e sancionatórias ante os seus riscos

Na Lei Geral de Proteção de dados, os agentes do tratamento de dados estão sujeitos às sanções decorrentes do seu descumprimento. Isso ocorre, em especial, com o controlador, o qual será responsável[22], em face de qualquer dano causado por infringência ao decreto nº 13.709. Assim, ele assumirá esse dever de forma padronizada, salvo prova em contrário, que consiga o eximir absolutamente da sua responsabilidade por danos eventualmente causados – situação que demanda carga probatória extensiva de estar em *Compliance*[23] com a legislação (Sharma, 2019). Isso é o que

dispõe o parágrafo único do art. 44, conjuntamente ao art. 46 da LGPD:

> *Art. 44. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano. [...]*
>
> *Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.*

Ao se especificar a extensão dos deveres de responsabilidade e diligência, aludidos acima para cada agente, pressupõe-se que, para o controlador, esses serão mais abrangentes. Inclusive, levando-se em consideração que o controlador é responsável solidariamente com o operador[24] pela reparação de danos causados aos titulares quando envolvido diretamente com eles.

À vista disso, o critério adotado para delimitar o alcance da responsabilidade para cada agente são as obrigações expressas na lei. Nessa perspectiva, a Autoridade Nacional de Proteção de Dados (ANPD) determina, com diretrizes mais particulares ao caso concreto (ANPD, 2021, p. 17) que:

> *[...] As obrigações e responsabilidades do controlador e do operador são distintas, pois são determinadas de acordo com o papel exercido por cada um no âmbito do tratamento dos dados pessoais. Assim, a responsabilidade solidária [...] prevista para os casos de danos causados em razão do tratamento irregular realizado por operador (por descumprir as obrigações da legislação ou por não observar as instruções do controlador), pode ser considerada como uma excepcionalidade, já que em regra a responsabilidade é do controlador. A princípio, essa é a única hipótese em que o operador é equiparado ao controlador.*

Para tal fim, os aludidos deveres, de uma maneira geral dentro da lei, são inicialmente manifestados por vedação expressa à discriminação dos dados, descrita pelo art. 6º, IX, como a "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos". Interpreta-se como discriminatório o compartilhamento ou uso indevido de dados sensíveis, isto é, informações concernentes à origem racial ou étnica, religião, opinião política, filiação ao sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou vida sexual, dado genético ou biométrico quando vinculado a uma pessoa natural.

Em sequência, o legislador não só se absteve ao vedar o uso ilícito de dados aos agentes de tratamento, como também vedou a conduta abusiva – conceito que, até o presente momento, carece de especificidade na sua interpretação (Pestana, 2020), deixando em aberto a dimensão de atribuições do controlador dentro desse tópico.

Seguidamente, os princípios se direcionam, inclusive, a salvaguardar os danos à privacidade de dados sob a ótica de sua potencialidade. Destarte, evidenciam-se a segurança e a prevenção. A primeira é assegurada reforçando os princípios e sanções impostas pelos sobreditos dispositivos, no inciso VII do art. 6º, determinando a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão". Dessa definição se extrai que o compromisso do controlador com a proteção de dados pessoais ultrapassa a mera proibição

de abusar de sua posição de vantagem em convenção com o titular e se estende, dentro do possível, para proteger a sua privacidade perante os danos causados por terceiros (Flumignan & Flumignan, 2020).

Já a prevenção se elucida no inciso VIII do art. 6º e consiste na "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais".

Nos dispositivos acima referenciados, está evidente que é de interesse do controlador a adoção de mecanismos e condutas de *cybersecurity* antecedentes ao dano. Essas, além de proporcionarem maior proteção ao titular na esfera da tutela inibitória[25] dos danos à privacidade de dados (Flumignan & Flumignan, 2020) – os quais, em incidentes de vazamento de dados, muitas vezes são irreparáveis – propiciam, conjuntamente, uma oportunidade ao controlador de mitigar a sua responsabilidade por danos decorrentes da violação da segurança dos dados.

De fato, considera-se que as penalidades da lei serão aplicadas consoante procedimento administrativo com contraditório e ampla defesa e estão categorizadas no art. 52 I-XII, no qual será oportunizado ao agente de tratamento, mediante advertência, a adoção de melhores práticas antes de sofrer sanções de caráter pecuniário. Nesse sentido, o §1º do art. 52 indica, de forma transparente, condutas recomendadas ao controlador[26] e, se o último demonstrar que cumpriu em parte ou integralmente esses requisitos na sua gestão interna perante a autoridade competente[27], poderá beneficiar-se da redução das sanções do decreto nº 13.709. Dentro desse rol de condutas se situam os mecanismos de governança de dados (Pinheiro, 2021).

Assim, persevera-se a necessidade da governança de dados, uma vez que, com a LGPD em vigor, novos riscos legais serão gerados para as organizações, seja considerando-os sob uma ótica sancionatória, como também atinente à sua reputação. Será imperativo ao controlador ponderar sobre as políticas, procedimentos e controles referentes às práticas que irá adotar e verificar se, realmente – adotar ou permanecer com – práticas contrárias aos valores da lei compensarão os riscos das sanções regulatórias (Gonzales, Rhee & Herzog, 2020).

3.3 O princípio da responsabilização e prestação de contas em contraste ao papel da ANPD

Inicialmente, é fundamental tecer algumas considerações para distinguir que existe, além do princípio da prestação de contas na LGPD, um princípio geral sobre a prestação de contas ou *Accountability,* visto pelo prisma dos pilares da governança corporativa[28], cujo propósito é o monitoramento efetivo dos recursos das organizações, gestão econômica e social – considerando seu papel na coletividade, seja no âmbito empregatício, ambiental ou tributário – além de correção de falhas de mercado. Considera-se como uma das falhas de mercado abarcada pelo seu conteúdo a relação contratual, na qual uma das partes tem mais informações concernentes ao produto ou serviço que é objeto desse negócio – fato que constitui relação de assimetria informacional – estando essa parte em posição privilegiada (Silva & Murcia, 2016).

Para atingir essas finalidades, destaca-se a necessidade de que não basta que a gestão das organizações esteja sujeita à provisão de informações, mas também à disposição de explicações e justificativas acerca daquilo que foi informado e das suas condutas para serem avaliadas por um terceiro - cujos critérios de avaliação sejam estabelecidos externamente – além de submeter-se a questionamento,

julgamento e, posteriormente, possuir vulnerabilidade para enfrentar potenciais consequências. Isso demanda, em adição à mera divulgação de informações e os seus respectivos fundamentos, um diálogo que possibilite objeções e eventuais sanções (Keay & Loughrey, 2014).

A LGPD levou em consideração os sobreditos fatores e, por conseguinte, estabeleceu no art. 6º, X, o princípio da prestação de contas, nos moldes das demandas particulares à proteção de dados: "X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

Desse conceito se depreende que, além de ser imprescindível agir em termos com os dispositivos da LGPD, há a indispensabilidade de providenciar evidências que demonstrem que o controlador seguiu os deveres apresentados pela lei, portando-se com boa-fé e diligência no tratamento dos dados. Enfatiza-se, em somatória, a vinculação do tratamento dos dados para além da adoção das medidas da LGPD, incluindo também os resultados dessas medidas (Pestana, 2020). Nessa mesma perspectiva, defende Teixeira e Armelin (2020):

> *[...] não basta o agente ter cumprido todas as regras e determinações legais, é preciso que ele a todo tempo registre que cumpriu a lei, utilizando-se das mais diversas formas para que consiga comprovar o atendimento aos preceitos da lei caso algum incidente ocorra. É de se mencionar a obrigatoriedade da prestação de contas por parte do agente até mesmo quando não houver qualquer descumprimento ou irregularidade.*

Atendendo a essas demandas, as evidências requeridas pela prestação de contas serão demonstradas perante a Autoridade Nacional de Proteção de Dados, cuja função, delimitada pelo art. 5º XIX da LGPD[29], será de fiscalizar, sancionar e aplicar a legislação concernente à proteção de dados (Flumignan & Flumignan, 2020). Diante de tal função, qualifica-se como órgão componente da Presidência da República o associado à administração pública direta, dotado de independência funcional e autonomia financeira – condição necessária para fins de efetividade e imparcialidade na sua atuação. A fiscalização da proteção de dados também pode ser incumbida ao judiciário, mas com função subsidiária, considerando-se a utilidade de homogeneizar, por um órgão público específico, as regras e padrões que se enquadram dentro da disciplina do seu alcance (Lucca, Lima. 2020).

Tendo sido a função do princípio da prestação de contas no âmbito do tratamento de dados elucidada, bem como seu órgão competente para assegurá-lo caracterizado, importa indagar acerca dos meios de como atingir a sua eficácia. Primordialmente, merece considerar-se que, para haver *Accountability*, ou seja, a devida demonstração do cumprimento da LGPD e submissão a julgamento da ANPD, o controlador deverá interpretar e colocar em prática todos os princípios. Isso é o que sustenta Flumignan (2020): "A análise de cada um dos princípios autoriza a afirmação de que nenhum deles, de maneira isolada, é suficiente para a efetiva proteção de dados. Apenas uma análise sistemática e complementar alcançará o objetivo pretendido com a lei geral".

Ainda, no que diz respeito ao conteúdo que merece ser demonstrado, isto é, o objeto da prestação de contas, denota-se que, sob a perspectiva da ANPD, o emprego dos princípios da lei será uma das principais métricas adotadas para editar normas e regulamentos (Lucca, Lima. 2020), consequentemente, dentro dos seus critérios, irá aferir o

desempenho do controlador no seu programa de governança de dados.

O controlador possui papel significativo para assegurar o *Accountability*, de modo que esteja em *Compliance* com as medidas relativas aos demais princípios da lei. Todavia, mesmo se entendendo que a prestação de contas demanda demonstração pelo controlador da execução dos princípios, considera-se que os deveres impostos na LGPD se encontram em condição de generalidade com relação ao caso concreto, porquanto o *Accountability* carece de maior regulamentação por parte da ANPD para ainda ser demandado (KPMG Board Leadership Center, 2021).

Conforme exposto, há uma lacuna no que tange à prestação de contas. Dessa forma, é possível analisar a sua incidência no controlador, adotando-se a GDPR como referencial, sendo necessário, anteriormente, qualificar o controlador.

4. O Controlador

Já é conhecido que o art. 5º, VI, da LGPD, descreve o controlador como a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais". Contudo, a ANPD aprofunda as suas competências ao delimitar que as sobreditas decisões são atreladas aos elementos principais do tratamento de dados, podendo o controlador delegar elementos decisórios secundários e o tratamento de dados propriamente dito ao operador.

A Lei comunica, inclusive, que os elementos principais que integram as decisões do controlador são concernentes à finalidade do tratamento[30], à natureza dos dados tratados, à duração do tratamento, entre outros mais específicos para cada caso. À vista disso, afere a ANPD que a caracterização do controlador será funcional. Isso posto, é possível a estipulação em contrato de seu *status* legal de controlador, porém, a referência usada pela autoridade serão as ações do agente de tratamento[31]. Assim, ao serem identificados os agentes de tratamento, poderão ser requisitados ao controlador o dever de transparência e a prestação de contas (Sharma, 2019).

Acerca dos litígios que serão possibilitados entre o controlador e o interessado diante da ANPD, deve-se levar em consideração que, em conflitos com o titular, o ônus da prova recairá perante o agente de tratamento; logo, o controlador deve buscar ao máximo minimizar divergências dessa categoria. Isso pode ser evitado de forma que o controlador tome decisões se atentando aos direitos do titular, fazendo-o de forma constante, visto que a ANPD está revestida de prerrogativas para fiscalização, consequentemente, para demandar demonstrações do tratamento de dados por parte do controlador (Lima, 2020)[32].

4.1 A abordagem baseada em riscos da GDPR (risk-based approach) a ser adotada pelo controlador e a sua repercussão para a prestação de contas

À primeira vista, o Brasil possui uma cultura de governança corporativa pouco difusa em seu ambiente empresarial (Redecker, 2020) – e, no

caso, poucos são os temas abordados que derivam desse sistema nas organizações, como as premissas das ESG's e da proteção de dados, por exemplo. Diante disso, viu-se em 2020 uma demanda dos investidores externos crescente no sentido de que seja repensada a ética empresarial dentro do país (O'kelley, Goodman & Sanderson, 2021). Atentando-se a esse aspecto, bem como à estruturação das diretrizes da ANPD ainda pouco definidas, espera-se que a implementação da governança de dados nas organizações no contexto brasileiro seja um processo lento e gradual (KPMG Board Leadership Center , 2021).

No entanto, nada impede os controladores, no presente momento, de começar a executar os princípios – até porque a prestação do controlador será um processo contínuo e corriqueiro, o qual não se restringe apenas à implementação inicial de um programa de governança de dados[33]. Apesar da generalidade na qual os princípios da LGPD se encontram, já é decisivo que o controlador deverá balancear a quantidade de esforços direcionados para proteger os dados dos titulares, de forma que observe a probabilidade e a gravidade que o tratamento de dados terá nos direitos e liberdades dos titulares caso, hipoteticamente, os seus dados sejam comprometidos (Sharma, 2019).

Com relação ao "balanço" anteriormente referido, o qual deve ser feito nos moldes dos princípios da LGPD, impõe-se que a relevância e a qualidade do dado coletado e tratado irão determinar a proporção e a gravidade das consequências impostas ao controlador em face de imprevistos ou incidentes de vazamentos de dados. A título de exemplificação, as diligências para proteger apenas o nome do titular serão significativamente menores do que aquelas feitas para proteger uma informação acerca da condição de saúde do titular[34]. Da mesma forma, pressupõe Gomes (2019):

> *[...] é necessário primeiro verificar, através de uma avaliação, conduzida e estruturada mediante uma metodologia, sendo, neste caso, uma metodologia avaliativa de riscos, o impacto de operações de tratamento em liberdades civis e direitos fundamentais do ser humano, aqui compreendido como titular dos dados.*

A referida lógica, anteriormente à legislação de proteção de dados, já era denominava pela governança corporativa como uma "tomada de decisões baseada em riscos", procedimento cuja sucessão de atos parte da análise e do planejamento até a ação e o seu monitoramento e, posteriormente, à revisão dos possíveis impactos de objetivos pretendidos pela gestão (IIA, 2020). Similarmente, a GDPR instituiu a *risk-based approach* para lidar com as incertezas dos objetivos do tratamento de dados, pela qual a lei optou como meio de sustentar o *Accountability* (Kloza, Van Dijk & Gellert 2017), em especial, no art. 24º (1) do Capítulo IV, denominado "Responsabilidade do responsável pelo tratamento":

> *Artigo 24º. 1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.*

Em comparação, a LGPD faz menção similar à *risk-based approach* na Seção II, a qual dispõe

sobre as "boas práticas e governança", no art. 50, §1º e §2º, II:

> *Art. 50. § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, 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. § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável [...].*

O que o legislador do regulamento europeu pretendeu endossar com o dispositivo foi o uso da gestão de riscos como ponto de referência para fins de prestação de contas, de tal forma que seja possível aferir se as medidas técnicas e administrativas adotadas pelo controlador fornecem a proteção necessária e suficiente. Não se restringe, aliás, à mera exigência de medidas de *Compliance*, uma vez que infere que tais medidas estejam também em equivalência aos riscos e ao grau de proteção que o dado fornecido pelo titular demanda (Quelle, 2018).

Outra interpretação retirada do artigo 24º, supratranscrito, diz respeito à indagação de qual organização controladora deverá tomar maiores precauções na sua gestão no âmbito da proteção de dados. Em outras palavras, quanto maiores forem os impactos negativos estimados para o tratamento de dados, maior a probabilidade de que esse tratamento seja incompatível com a atividade do controlador. Em contrapartida, se for constatado que o tratamento de dados representa pouco risco à privacidade e discriminação dos dados do titular, em pouca intensidade o controlador deverá ser transparente com o titular ou prestar contas perante a autoridade competente[35].

No que concerne às possíveis desvantagens da *risk-based approach*, constata-se que os aludidos "riscos", a "probabilidade e gravidade" do tratamento de dados são conceitos dotados de indeterminação semântica, a qual demanda interpretação a cada caso por parte da autoridade competente. Inclusive, o termo "riscos", trazido pelo artigo 24º, aliado ao termo "direitos", origina o questionamento sobre em qual dos dois termos deve preponderar no método da prestação de contas em termos interpretativos: afinal, enquanto o primeiro termo emana da área do conhecimento de administração de empresas – cuja prática envolve a tomada de decisões por cálculo de probabilidade – o segundo remete à área jurídica e, consequentemente, é praticado com base no procedimento expresso pela lei (Kloza et al., 2017).

Quando abordada a relação com a *risk-based approach* com os princípios expressos na lei – similarmente estruturados como os da LGPD – distinguem-se duas interpretações de como os dois elementos irão interagir. Por um lado, é possível que a *risk-based approach* possa substituir os princípios, dado que as medidas de *Compliance* estariam estritamente vinculadas ao risco, retirando o foco do controlador em priorizar os direitos e liberdades do titular, perspectiva descrita por Gellert (2018) como:

> *O direito à proteção de dados deve ser aplicado de forma independente do nível de risco e, logo, providenciar um nível uniforme de Compliance [...] o Grupo de trabalho do artigo 29º da GDPR[36] já adotou postura clara em favor da natureza baseada em direitos da União Europeia ao se tratar da*

> *proteção de dados. Já defendeu que a risk-based approach está sendo cada vez mais e erroneamente empregada como uma alternativa à direitos e princípios da proteção de dados bem estabelecidos. [...] Essa exigência de providenciar um nível uniforme de Compliance [...] já foi usada como argumento a favor de separação rigorosa entre questões de Compliance e risco [...] que completo Compliance legal com a GDPR deveria sempre existir e a aferição de riscos apenas vem após isso.*

Já sob outra ótica, acredita-se que o risco e o *Compliance* deverão ser empregados conjuntamente para impulsionar a tomada de decisões das organizações, de forma que se leve em consideração os princípios da GDPR e, portanto, os direitos e as liberdades dos titulares. Inclusive, essa tomada de decisões baseada em riscos só poderá ser feita se os princípios da GDPR forem empregados. Essa abordagem parece, aliás, mais realista para ser colocada em prática no contexto brasileiro, dado que os programas de *Compliance* no país são pouco utilizados, bem como permitiria a fiscalização da ANPD mais efetiva e direcionada aos controladores, cujas atividades representam maior risco aos direitos fundamentais dos titulares. Essa tese é sustentada e favorecida por Quelle (2018):

> *A abordagem baseada em riscos não substitui os princípios e regras de proteção de dados. Em vez disso, exige que os controladores calibrem o que significa, de acordo com a lei, proteger os direitos e liberdades dos titulares dos dados. [...] Em outras palavras, a abordagem baseada no risco, como a conhecemos, não reduz a legislação de proteção de dados à análise de risco. Em vez disso, usa a noção de risco para regular como os controladores devem implementar a lei na prática. [...] torna o GDPR mais proibitivo com relação às operações de processamento arriscadas e exige mais dos controladores quando isso é apropriado à luz dos direitos, mas também pode dar origem a outras limitações dos direitos do titular dos dados. [...] É impossível exigir que os controladores implementem o GDPR de forma que os riscos aos direitos e liberdades dos titulares dos dados sejam levados em consideração, mantendo, ao mesmo tempo, a validade das normas jurídicas em mesma intensidade. [...] Muitas das normas do GDPR se submetem à calibração da risk-based approach e podem ser facilmente aprimoradas dessa maneira.*

Enfim, permanece a noção de que a *risk-based approach* materializará o princípio do *Accountability* para o controlador, tendo em mente que serão implementados requisitos ainda abstratos da GDPR, o que proporcionará, na prática, um norte ao determinar as principais medidas a serem adotadas (Quelle, 2017). É evidente que foi dado elevado poder de decisão ao controlador, amparado pela lei, inclusive. Esse poder, porém, deverá ser exercido mediante consulta à autoridade competente (no Brasil, seria a ANPD), quando apropriado, toda a vez que o curso de ação no tratamento de dados for escolhido (Quelle, 2018).

Os referidos poderes do controlador estão, inevitavelmente, limitados ao tratamento de dados em conformidade aos princípios da LGPD e sustentados pelo *accountability*, o qual será proporcional aos riscos assumidos.

5. Considerações Finais

A importância da adesão e da implementação de um programa de governança de dados dentro das organizações é evidenciada diante de demandas de investidores e *stakeholders* vindos do Brasil e do contexto internacional, bem como da demanda por maior segurança jurídica na tutela do direito à privacidade e à proteção de dados dos titulares. Esses últimos se encontram em condições vulneráveis e em condição de dependência dos serviços prestados pelos agentes do tratamento de dados, sobretudo no meio ambiente digital. Culminada a essas circunstâncias, está manifesta na LGPD a menção do princípio da prestação de contas, conceito inescapavelmente associado à governança corporativa.

À vista disso, o presente estudo teve como intuito aprofundar-se no *Accountability*, na sua função de princípio basilar da governança corporativa, que será materializado em face dos princípios que irão incidir na atuação das empresas controladoras, trazidos pela Lei Geral de Proteção de Dados. Foram aprofundados os seus princípios e, partindo disso, averiguadas as omissões que precisam ser supridas pela ANPD para descrever de que forma o controlador deverá prestar contas. Por enquanto, é convicto afirmar que o controlador terá que demonstrar aderência aos princípios, ponderando-os de forma correlacionada e por uma abordagem baseada em riscos.

O programa de governança precisa ser assegurado por mecanismos de *Accountability*, estando em consonância com os princípios da LGPD. Pretendia-se, inicialmente, verificar se os princípios fundados no consentimento se faziam suficientes para assegurar a privacidade, principal objetivo da lei. Entretanto, esses, apesar de direcionarem o tratamento de dados, não serão suficientemente materializados apenas pelo consentimento do titular, mesmo ele estando protegido juridicamente, fazendo-se necessários os mecanismos de *accountability*. Para tanto, além da imposição de sanções na LGPD – que informam os valores contrários à lei e auxiliam o controlador a ponderar os riscos do tratamento de dados – exige-se uma interpretação dos princípios de forma interdependente por parte do controlador.

Considerou-se que o *accountability* se trata da demonstração dos procedimentos que estão sendo adotados pela organização e a submissão deles a julgamento, e, juntamente, a LGPD optou por deixar expresso no seu texto o princípio da prestação de contas e a preferência da adoção, por parte do controlador, de uma abordagem baseada em riscos, tal como o texto da GDPR. Desse pressuposto, foi possível extrair a *risk-based approach* como métrica a ser adotada pelo controlador ao ponderar os princípios da lei nas operações de tratamento de dados que realiza e, posteriormente, demonstrar isso perante a ANPD. Todavia, os meios pelo qual a *risk-based approach* serão demonstrados ainda são vagos e carecem de especificação pela ANPD, além disso, os efeitos dessa preferência adotada pela lei permanecem incertos.

Finalmente, merece aprofundamento os impactos que a opção legislativa da *risk-based approach* está produzindo para os casos específicos na aplicação da GDPR, a qual já entrou em vigor em 2018, e como as autoridades supervisoras estão suprindo a vagueza interpretativa dessa abordagem em contexto europeu. Em uma pesquisa própria, inclusive, é válido estudar o instrumento pelo qual serão descritos os possíveis riscos do

tratamento de dados (no caso da LGPD, o relatório de impacto à proteção de dados pessoais) e a sua respectiva demonstração à autoridade competente, e quem, na gestão das organizações, mediará essa interação entre o controlador e ANPD no ato de prestar contas - dado que a *risk-based approach* será apenas um ponto de partida para garantir a prestação de contas.

Dessa feita, os estudos não cessam aqui, é necessária a participação de instâncias acadêmicas e, principalmente, da sociedade para criar mecanismos de *accountability e,* assim, proporcionar maior segurança aos que agentes que lidam com dados

.

6. Notas

2 Art. 5º, X. São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

3 “Resolução nº 73/22 e 74/29, em 1973–1974, do Conselho Europeu, que formalizou a vinculação dos estados comprometidos; Diretrizes nº 95/46/EC, direcionadas para a proteção dos indivíduos no âmbito do processamento de seus dados, bem como sua movimentação (Data Protection Directive), em 1995; Regulamento nº 45/2001 da UE da proteção dos indivíduos, no âmbito do processamento de dados por instituições ou organismos dentro de sua Comunidade e na livre circulação desses dados” (Ziegler, Evequoz & Huamani, 2019).

4 Art. 7º da Carta de direitos fundamentais da União Europeia “Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.”

5 Entende-se como o controlador o disposto no art. 5.º, VI da lei nº 13.708/18 (LGPD): “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”. No conceito de operador, descreve-se o disposto no 5.º, VII, da referida lei, como a “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”.

6 Para fins de compreensão de estudo define-se organização como a “pessoa ou grupo de pessoas com suas próprias funções com responsabilidades, autoridades e relações para alcançar seus objetivos. O conceito de organização inclui, mas não é limitado a: organizações sem fins lucrativos (associações e fundações); companhia, sociedade limitada, cooperativa, sociedade de propósito específico, organização individual de responsabilidade limitada. Pública, privada ou de economia mista” (Redecker, 2020).

7 “Stakeholder, ou interessado, é toda a figura que se relaciona com a organização e sofre seus impactos. À exemplo disso têm-se os empregados, clientes, fornecedores, acionistas, comunidades, entre outros” (Giacomelli, 2017).

8 Esse fenômeno não é exclusivo da responsabilidade jurídica referente à proteção e tratamento de dados. Trata-se de mais um reflexo dos valores promovidos pela Governança Corporativa no âmbito do *Compliance*, o qual propõe um regime de corresponsabilidade entre as companhias e suas redes de contratos. Para fins de reputação frente a investidores e consumidores e por demandas legais, têm-se que a integridade da companhia passa a ser não só uma meta interna da organização, como também passa a ser pré-requisito para os seus parceiros de negócio (REINEKE & ANSARI, 2016).

9 Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

10 Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

11 "A organização e reúne os presidentes executivos de 181 das maiores corporações dos Estados Unidos [...] Desde 1978, publica declarações sobre os princípios de governança corporativa." Recuperado de: https://epocanegocios.globo.com/Empresa/noticia/2019/08/poderosa-tavola-redonda-de-megaempresas-que-quer-redefinir-regras-do-capitalismo-americano.html.

12 "O Fórum Econômico Mundial é conhecido por congregar grandes líderes e organizações para a realização de debates sobre a economia mundial." Recuperado de: https://brasilescola.uol.com.br/geografia/forum-economico-mundial.html.

13 Informação recuperada de: https://www.linkedin.com/pulse/o-que-esg-e-lei-geral-de-proteção-dados-tem-em-comum-lewis-delgado/.

14 Recentemente tem sido exigido às organizações a se adaptarem à um modelo, o qual denomina-se ESG. As questões abordadas pelas ESG's (Environmental, Social and Governance), são: mudanças climáticas e riscos de sustentabilidade, igualdade entre identidades (baseados, por exemplo, em raça, gênero, etnia ou deficiência), diversidade de atributos ou competências (baseados em identidade, por exemplo, em habilidade, experiência ou idade), diversidade na força de trabalho e inclusão, boa gestão de capital humano, igualdade de pagamento no ambiente de trabalho, levando em consideração segurança, saúde, bem-estar, direitos humanos, contribuições para movimentos de ativismo político, programas de *Compliance* para cadeias de fornecedores, entre outros (Atkins, Gerber & King, 2021).

15 Embora o consentimento do titular seja a principal base legal ao se pensar em tratamento de dados, são ressalvadas as demais hipóteses que dispensam consentimento, descritas nos art. 7º ao 10 da LGPD, como, por exemplo, o cumprimento de obrigação legal ou regulatória, execução de contratos, interesse legítimo do controlador, entre outros. Ainda que seja prescindível o consentimento nesses casos, a aplicação dos princípios ainda se faz obrigatória.

16 O art. 2º, V da LGPD menciona expressamente que "a disciplina da proteção de dados pessoais tem como fundamentos: [...] o desenvolvimento econômico e tecnológico e a inovação". Nessa linha de raciocínio, "é certo que a LGPD representa uma necessidade de mudança na forma em que os negócios são realizados atualmente, porém nunca deve ser considerada como barreira que veda o acesso a qualquer tipo de mercado" (Russo, 2019).

17 Art. 5º Para os fins desta Lei, considera-se: XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

18 Art. 6º. As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] IV. livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V. qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

20 Igual à nota anterior.

21 Igual à nota anterior.

22 Ainda não é claro na jurisprudência se o regime de responsabilidade civil dentro da LGPD terá caráter objetivo, isto é, se ocorrerá de forma independente à comprovação da hipótese de que o agente de tratamento deu causa ao dano ou não, não sendo possível, assim, considerar todos os danos causados aos titulares presumíveis. Além disso, convém considerar que os tribunais superiores delimitam situações excepcionais para incidência de danos morais presumidos, a fim de evitar banalização do instituto. No que se refere à reparação de danos no decreto, o art. 42 apenas define que "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo" (Martins, Thomé & Tavora, 2021).

23 Para maior esclarecimento, salienta-se que "uma organização estar em *Compliance* significa que ela está cumprindo as leis, normativas dos órgãos reguladores e regulamentos internos e externos e, para atingir seu objetivo, é necessário instituir controles eficazes e avaliar suas atividades sob o crivo da conformidade." (Redecker, 2020).

24 Art. 42, §1º, I. o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador se equipara ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei; II. os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

25 Conceitua-se como inibitória a tutela jurídica que é "voltada a evitar o ilícito, ou seja, um ato contrário ao direito, que pode acarretar em violação a uma situação jurídica subjetiva", além de buscar "prevenir riscos e ameaças daqueles danos tidos por irreversíveis, principalmente dos que lesionam a dignidade humana, por meio de instrumentos preventivos [...]" (Rodrigues, 2020).

26 Art. 52 § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: [...] VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX - a adoção de política de boas práticas e governança; X - a pronta adoção de medidas corretivas [...].

27 *In casu*, no Brasil, a função de fiscalizar, sancionar e elaborar diretrizes no âmbito da Lei

Geral de Proteção de dados é atribuída à Autoridade Nacional de Proteção de Dados (ANPD).

28 Ver tópico 2.1.2 do presente artigo para fins de conceituação do *Accountability*.

29 Art. 5º. XIX. Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

30 "Considere os seguintes exemplos de decisões do controlador, segundo a finalidade do tratamento: utilização de dados pessoais para o pagamento de empregados, a realização de uma pesquisa com clientes, a promoção de uma campanha de marketing, o armazenamento seguro de informações ou a emissão de passagens aéreas" (BRASIL, 2021).

31 Igual à nota anterior.

32 Conforme a seção I da LGPD.

33 A respeito disso, "não é possível que a organização se considere em conformidade com a LGPD, seja pela ausência da estruturação da ANPD, ou até que tenha avaliado seus processos e seus mecanismos de controle, bem como se tais mecanismos estão realmente sendo observados no ambiente de negócios" (Redecker, 2020).

34 Igual à nota anterior. Ver o tópico 3.2. para compreender o conceito de "dados sensíveis".

35 Igual à nota anterior.

36 "O Grupo de Trabalho do Artigo 29.º (GT Art. 29.º) é o grupo de trabalho europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018 (data de aplicação do RGPD)" Disponível em: https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_pt.

BIBLIOGRAFIA

Atkins, P. A., Gerber, M. S. & King, K. J. (2021). Directors' Oversight Role Today: Increased Expectations, Responsibility and Accountability—A Macro View. Recuperado de: https://corpgov.law.harvard.edu/2021/05/10/directors-oversight-role-today-increased- expectations-responsibility-and-accountability-a-macro-view/.

Autoridade Nacional de Proteção de Dados (2021) Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. Recuperado de: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-orientativo-sobre-gentes-de-tratamento-e-encarregado.

Blok, M. (2020). *Compliance* e governança corporativa. (3a ed). Rio de Janeiro: Freitas Bastos Editora.

Lei nº 13.709, de 14 de agosto de 2018. (2018). Institui a Lei Geral de Proteção de Dados Pessoais. Brasília/ DF: presidência da república. Recuperado de: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Constituição da República Federativa do Brasil. (1988). Brasília, DF: Presidência da República. Recuperado de http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

Canto, A. P. et al. (2019). O tratamento de dados pessoais na LGPD: transparência e dever de informação. P. M. Saldanha (Coord.). OAB Pernambuco. O que estão fazendo com os meus dados? A importância da Lei Geral de Proteção de Dados. Recife: SerifaFina.

De Lima, Cíntia Rosa Pereira. (2020). Autoridade Nacional de Proteção de Dados e a efetividade da Lei Geral de Proteção de Dados. São Paulo: Almedina.

Lucca, N. de & Lima, C. R. P. de. (2020). Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. C. R. P. de Lima (Coord.). Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019. São Paulo: Almedina.

Teffé, C. S. de. & Viola, M. (2020). Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Civilistica.com, Rio de Janeiro, 9(1), 1-38. Recuperado de https://civilistica.emnuvens.com.br/redc/article/view/510.

Falcão, C. M. R. & Keller, E. Z. (2021). Terceirização do tratamento de dados – a relação entre controlador e operador. A. P. M. C. de. Lima et al. (Org.). LGPD Aplicada. São Paulo:Atlas.

BIBLIOGRAFIA

Flumignan, S. J. G. & Flumignan, W. G. G. (2020). Princípios que regem o tratamento de dados no Brasil. C. R. P. de Lima (Coord). Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019. São Paulo: Almedina.

Gellert, Raphaël. (2016). We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-based Approaches to Data Protection. N. Dijk, R. Gellert & K. Rommetveit, A risk to a

right? Beyond data protection risk assessments. Computer Law & Security Review, 32(2). Recuperado de https://www.sciencedirect.com/science/article/pii/S026736491500182X?via%3Dihub.

Giacomelli, G. (2017). Governança corporativa. São Paulo: SAGAH.

Gomes, M. C. O. (2019). Relatório de impacto à proteção de dados. Uma breve análise da sua definição e papel na LGPD. Revista da AASP, (144).

Gonzales, J. R., Rhee, J. S. & Herzog, S. C. (2020). FTC Seeks Information Regarding Companies' Data Collection, Use, and Advertising Practices. Recuperado de https://corpgov.law.harvard.edu/2021/01/21/ftc-seeks-information-regarding-companies-data-collection-use-and-advertising-practices/.

Grupo de Trabalho Interagentes. (2016). Código Brasileiro de Governança Corporativa: Companhias Abertas. São Paulo: IBGC.

IIA - The Institute of Internal Auditors. (2020). The II-A's three lines model: An update of the Three Lines of Defense. Lake Mery: Global. Recuperado de https://na.theiia.org/about-ia/PublicDocuments/Three-Lines-Model-Updated.pdf.

Instituto Brasileiro de Governança Corporativa. (2015). Código das melhores práticas de governança corporativa. (5a.ed). São Paulo: IBGC. Recuperado de https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=21138.

Souza Júnior, G. de. Cristo, T. K. de. (2015). Ronald Dworkin: leitura moral e sua aplicabilidade no sistema romano-germânico brasileiro. Lages, C. G., Durães, M. G. & Santos, M. C. R. A compreensão dos direitos humanos e fundamentais no direito brasileiro. (pp. 343-435). Belo Horizonte: Editora D'Plácido.

Keay, A. & Loughrey, J. (2014). The framework for board accountability in corporate governance. N. G. Thomas & B. Wardhaugh. Legal Studies. 41(2). The Society of Legal Scholars.

BIBLIOGRAFIA

Kiss, A. & Szoke, G. L. (2014). Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation. S. Gutwirth, R. Leenes & P. de Hert (eds). Reforming European Data Protection Law. Law, Governance and Technology Series. Dordrecht: Springer.

Kloza, D. (et al.). (2017). Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals. Brussels: Brussels Laboratory for Data Protection & Privacy Impact Assessments. Recuperado de https://www.prio.org/Publications/Publication/?x=10579.

KPMG Board Leadership Center. (2021). Top emerging risks 2021. Michigan: ACI Institute. Recuperado de https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24408.

Lima, C. C. (2020). Proteção de dados nas relações de consumo: CDC, Marco Civil e LGPD. EBRADI.

Martins, P. H., Thomé, B. B. & Tavora, B. V. (2021). O dano moral por violação à LGPD. São Paulo: revista Consultor Jurídico. Recuperado de https://www.conjur.com.br/2021-mai-31/opiniao-dano-moral-violacao-lgpd.

O'Kelley, R., Goodman, A. & Sanderson, L. (2021). 2021 Global and Regional Trends in Corporate Governance. EUA: Russell Reynolds Associates. Recuperado de https://www.russellreynolds.com/insights/thought-leadership/2021-global-and-regional-trends-in-corporate-governance#.

Pestana, M. (2020). Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais). São Paulo: revista Consultor Jurídico. Recuperado de https://www.conjur.com.br/2020-mai-25/marcio-pestana-principios-tratamento-dados-lgpd.

Pinheiro, P. P. (2020). Proteção de dados: comentários à lei nº 13.709/2018 (LGPD). (2a. ed.). São Paulo: Saraiva Educação.

Lima, C. C. Proteção de dados nas relações de consumo: CDC, Marco Civil e LGPD. EBRADI, 2020.

Quelle, C. (2018). Enhancing *Compliance* under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach. European Journal of Risk Regulation. Board, France, 9(3).

Quelle, C. (2017). The 'risk revolution' in EU data protection law: We can't have our cake and eat it, too. Data Protection and Privacy: The Age of Intelligent Machines (Hart Publishing, Forthcoming). Tilburg Law School Research Paper (17). Recuperado de https://ssrn.com/abstract=3000382.

BIBLIOGRAFIA

Redecker, A. C. (2020). *Compliance* de dados pessoais. Porto Alegre: Academia da Escrita.

Reineke, J. & Ansari, S. (2016). Taming wicked problems: the role of framing in the construction of corporate social responsibility. Journal of Management Studies, 53(3).

Rodrigues, C. M. (2020). Reparação de danos e função preventiva da responsabilidade civil: parâmetros para o ressarcimento de despesas preventivas ao dano. Civilistica.com. Rio de Janeiro, 9(1). Recuperado de https://civilistica.emnuvens.com.br/redc/article/view/505.

Rossetti, J. P. & Andrade, A. (2004). Governança corporativa: Fundamentos, desenvolvimento e tendências. (7a. ed.) São Paulo: Atlas.

Russo, R. A. (2019). A tutela da privacidade de dados na era do Big Data. Dissertação de Mestrado, Programa de Estudos Pós-Graduados em Direito, Pontifícia Universidade Católica de São Paulo, São Paulo.

Sharma, S. (2019). Data Privacy and GDPR Handbook. Hoboken: John Wiley & Sons, Inc.

Soares, P. B. D. & Câmara, A. A. F. (2011). A quebra do contrato e do pré-contrato a partir da violação da boa-fé objetiva. Scientia Iuris, Londrina, 15(2), 9-30.

Sombra, T. L.S. (2019). Direito à privacidade e proteção de dados no ciberespaço: a accountability como fundamento da Lex Privacy. Tese de Doutorado, Universidade de Brasília, Brasília.

Teixeira, T. & Armelim, R. M. G. da F. (2020). Responsabilidade e Ressarcimento de Danos por Violação às Regras Previstas na LGPD: um Cotejamento com o CDC. C. R. P. de Lima (Coord.). Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019. São Paulo: Almedina.

União Europeia. (2016). Regulamento nº 2016/679. Institui o Regulamento Geral sobre a Proteção de Dados. Recuperado de https://gdprinfo.eu/pt-pt/pt-pt-article-1.

Vainzof, R. & Frabretti, H. Proteção de dados - Governança e o DPO como núcleo da jornada de conformidade com a LGPD. 2020. Recuperado de https://www.jota.info/opiniao-e-analise/artigos/governanca-e-o-dpo-como-nucleo-da-jornada-de-conformidade-com-a-lgpd-23032020.

Ziegler, S., Evequoz, E. & Huamani, A. M. P. (2018). The Impact of the European General Data Protection Regulation (GDPR) on Future Data Business Models: Toward a New Paradigm and Business Opportunities. A. Aagaard (eds) Digital Business Models. Palgrave Macmillan, Cham.