DOI 10.5433/24157-108104-1.2023v18n2p.30

A ANPD E A FISCALIZAÇÃO DA GOVERNANÇA CORPORATIVA DE PROTEÇÃO DE DADOS

BRAZILIAN NATIONAL DATA PROTECTION AUTHORITY AND THE OVERVIEW OF PERSONAL DATA PROTECTION POLICIES

Ana Elizabeth Neirão Reymão*
Lis Arrais Oliveira**
Suzy Elizabeth Cavalcante Koury***

*Professora do Programa de Pós-Graduação Stricto Sensu em Direito, Políticas Públicas e Desenvolvimento e da graduação em Direito do Centro Universitário do Pará (CESUPA). Professora da Faculdade de Economia da Universidade Federal do Pará (UFPA). Doutora em Ciências Sociais pela Universidade de Brasília (UnB). Mestra em Economia pela Universidade Estadual de Campinas (UNICAMP). Líder do grupo de pesquisas Min Amazônia – CNPq. E-mail: bethrey@uol.com.br

**Graduada em Direito pelo Centro Universitário do Estado do Pará – CESUPA. Advogada. Mestranda em Direito, Políticas Públicas e Desenvolvimento Regional pelo Programa de Pós Graduação em Direito do Centro Universitário do Estado do Pará (PPGD/CESUPA).
E-mail: minamazonia@gmail.com

***Doutora em Direito pela Faculdade de Direito da Universidade Federal de Minas Gerais (UFMG). Desembargadora do Trabalho. Ex-presidente do TRT da 8ª Região (2016-2018). Professora do Programa de Pós-Graduação em Direito, Políticas Públicas e Desenvolvimento e da graduação do Centro Universitário do Pará (CESUPA). Líder do grupo de pesquisas CNPq Emprego, Subemprego e Políticas Públicas na Amazônia. E-mail: suzykoury@gmail.com

Como citar: REYMÃO, Ana Elizabeth Neirão; OLIVEIRA, Lis Arrais.; KOURY, Suzy Elizabeth Cavalcante. A ANPD e a fiscalização da governança corporativa de proteção de dados. **Revista do Direito Público**, Londrina, v. 18, n. 2, p. 30-47, ago.2023. DOI 10.5433/24157-108104-1.2023v18n2p.30. ISSN: 1980-511X

Resumo: O presente artigo discute a importância da governança corporativa de proteção de dados, destacando a função preventiva e educativa da Autoridade Nacional de Proteção de Dados (ANPD). Argumenta-se, com base na análise da Lei Federal nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), que um atributo fundamental dessa Autoridade é o incentivo às boas práticas, ao instituto do *compliance* ou governança corporativa de proteção de dados pessoais pelas empresas privadas, bem como a fiscalização sobre a conformidade dessas práticas com o dispositivo legal. Trata-se de uma pesquisa aplicada, de abordagem qualitativa, tendo como procedimentos o levantamento bibliográfico e a análise documental. Conclui-se pelo importante papel do *accountability*, princípio basilar da governança corporativa dos programas de proteção de dados nas empresas, devendo elas demonstrarem a conformidade e a efetividade desses programas, bem como serem estimuladas pela ANPD à adoção de padrões técnicos que facilitem o controle dos dados pelos seus titulares, evitando o seu uso indevido por agentes privados.

Palavras-chave: ANPD; LGPD; governança corporativa; *compliance;* prevenção.

Abstract: This paper discusses the importance of data protection corporate governance, highlighting the preventive and educational role of the National Data Protection Authority (ANPD). Based on the analysis of Federal Law nº 13.709/2018, the General Data Protection Law (LGPD), the paper argues that a fundamental

attribute of this Authority is the encouragement of good practices, the compliance or corporate governance to protect personal data by private companies, as well as the supervision of the compliance of these practices with the legal provision. This is an applied research, with a qualitative approach, using as procedures the bibliographic survey and document analysis. It is concluded by the important role of accountability, a basic principle of corporate governance of data protection programs in companies, which must demonstrate the compliance and effectiveness of these programs, as well as be encouraged by the ANPD to adopt technical standards that facilitate the control of data. data by their holders, preventing their misuse by private agents.

Keywords: ANPD; GDPR; corporate governance; compliance; prevention.

INTRODUÇÃO

A gestão de riscos, a conformidade aos regramentos e os programas de governança corporativa assumiram um papel de destaque na política nacional de proteção de dados pessoais e da privacidade, consolidada pela Lei Federal nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD). Nesse contexto, para alcançar a proteção almejada, é importante que boas práticas de gestão e governança sejam adotadas por agentes públicos e privados.

A LGPD destinou uma seção inteira ao tema, a fim de garantir que a atuação dos controladores de dados ocorra em conformidade ao regramento, minimizando os riscos de descumprimento da norma. Faz-se necessário, então, a instauração de programas de governança corporativa que fomentem boas práticas de proteção de dados pessoais por agentes privados, conforme está expressamente previsto na legislação, como consequência lógica de um princípio norteador da LGPD, o da prevenção.

Nessa linha, a criação de autoridades responsáveis por promover o cumprimento da legislação vem sendo uma prática recorrente em políticas de proteção de dados pessoais no mundo. No Brasil, a LGPD criou a Autoridade Nacional de Proteção de Dados (ANPD), órgão integrante da Presidência da República, dotado de autonomia para supervisionar e consolidar a instauração da política pública, especialmente por meio de seu papel preventivo, pelo qual deve fiscalizar os agentes públicos e privados a fim de averiguar se a atuação destes está em conformidade à legislação (DONEDA, 2021, p. 464).

O incentivo à implementação de políticas de governança corporativa de proteção de dados no setor privado é essencial, sendo essa uma maneira de o Estado exercer sua atividade pública como garantidor do cumprimento da legislação com os agentes privados, e, ainda, um mecanismo para firmar e fomentar a política pública na temática (CARVALHO; MATTIUZZO; PONCE, 2020, p. 364).

Este é o ponto de partida do presente estudo, que discute a importância da fiscalização da governança corporativa de proteção de dados, destacando a função preventiva e educativa da ANPD. A partir de uma interpretação do texto legal e de uma análise das funções inerentes de autoridades responsáveis por regular as atividades econômicas, entende-se que essa agência tem como um atributo fundamental o incentivo às boas práticas, ao instituto do *compliance* ou governança corporativa de proteção de dados pessoais pelas empresas privadas, bem como a fiscalização se tais práticas estão efetivamente em conformidade com o dispositivo legal.

Argumenta-se que a LGPD atribuiu à ANPD a função de fiscalizar e incentivar os programas de governança corporativa de proteção de dados nas empresas privadas, sendo essa função decorrente do princípio da prevenção, o qual norteia o dispositivo legal.

A pesquisa usa o método indutivo, tendo-se como ponto de partida a observação do texto legal e a identificação dos encargos atribuídos pela LGPD à ANPD acerca dos programas de governança corporativa de proteção de dados pelas empresas. A abordagem é qualitativa e a pesquisa de natureza aplicada, tendo como procedimentos o levantamento bibliográfico e a análise documental.

A primeira seção do artigo apresenta a ANPD; a seção seguinte analisa o instituto do *compliance* e da governança corporativa em uma perspectiva voltada para a proteção de dados pessoais; a terceira seção mostra que a LGPD destacou as boas práticas, a governança e sua importância para a consolidação da política nacional de proteção de dados e da privacidade. Na quarta seção, o texto dispõe sobre a necessidade destas medidas serem implantadas com transparência ou *accountability* e ressalta sua importância como um princípio norteador das políticas de governança corporativa. Por fim, a última seção se ocupa em destacar, com base no dispositivo legal, o encargo atribuído pela LGPD à ANPD em fiscalizar e incentivar a adoção de programas de governança corporativa de proteção de dados pelas empresas.

1 A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

A ANPD é um órgão integrante da Presidência da República, tendo sua estrutura sido estabelecida pela Lei 13.853, de 8 de julho de 2019, que converteu em lei a medida provisória nº 869, de 27 de dezembro de 2018, criando a ANPD, nos termos do artigo 55-A da LGPD.

Trata-se de uma agência autônoma, sendo comum que o Estado recorra a órgãos administrativos independentes, visando atender demandas relacionadas à regulação de alguns mercados. Essas agências se caracterizam como entes ou órgãos públicos, dotados de independência do governo e autonomia de organização, financiamento e contabilidade (DONEDA, 2021, p. 642).

Dessa forma, a autonomia técnica, financeira e a independência funcional da ANPD, juntamente com a composição multissetorial do Conselho Nacional de Proteção de Dados e da Privacidade, composto por membros da sociedade civil, da academia, do Poder Público e do mercado, confere aspectos essenciais para dar efetividade ao sistema de proteção de dados no país (LUCCA; LIMA, 2020, p. 375).

O uso de agências reguladoras, lembra Vilela (2020, p. 93), é uma tendência que se iniciou no Brasil na década de 1990, quando o Estado envidou esforços para reduzir a atuação direta na economia, transferindo a execução de atividades públicas ao setor privado e assumindo funções de fiscalização e regulação de atividades econômicas.

Diante dessa nova, à época, atuação do Estado na economia e do fortalecimento do papel privado em setores estratégicos e atividades econômicas relevantes, tornou-se imprescindível a

readequação do aparato estatal, para que se atinja a almejada eficiência. Dessa forma, autarquias e fundações, as quais exerciam atividades exclusivas de Estado, transformaram-se em agências autônomas, dotadas de autonomia, criadas com a finalidade de disciplinar e controlar certas atividades de setores e mercados específicos (VILELA, 2020, p. 97).

Conforme aduz Doneda (2021, p. 463), mais recentemente verificou-se que muitas características destes órgãos, criados para responder de forma mais direta e dinâmica as demandas de natureza econômica, poderiam ser igualmente relevantes no papel da defesa e da promoção de direitos do cidadão, sendo possível distinguir a atuação de dois tipos de autoridades, as de regulação e as de garantia:

> Às autoridades de regulação, cuja competência costuma ser ligada a um determinado serviço público, são destinadas funções similares àquelas da própria administração pública, com vantagens quanto à dinamicidade de sua estrutura e outras. Por sua vez, as autoridades de garantia possuem a missão de proteção de direitos ou situações subjetivas específicas, para cuja defesa foram constituídas. Um organismo com a proposta da proteção de um direito como o da proteção de dados pessoais (a ANPD, por exemplo), estaria enquadrada, portanto, como uma autoridade de garantia (DONEDA, 2021, p. 463).

A autoridade de garantia se difere da autoridade de regulação por estar envolvida diretamente no papel da proteção de direitos específicos. Em um contexto de colisão de direitos e de busca por equilíbrio entre diversas garantias e direitos de natureza constitucional, a autoridade de garantia assume o papel de promover um "equilíbrio dinâmico" entre estas dicotomias, organizando uma convivência plural de valores (DONENA, 2021, p. 464).

Assim, visando a tutela da proteção de dados, a instauração da ANPD no Brasil foi essencial para a Política de Proteção de Dados e da privacidade, visto que o tratamento de dados pessoais é raramente acompanhado pelos cidadãos de forma eficaz, assim como há necessidade de constante atualização da disciplina, em função do desenvolvimento tecnológico crescente.

Ademais, a autoridade independente é útil ao setor privado por garantir a uniformização da aplicação da lei, em circunstâncias nas quais tribunais ou reguladores setoriais tendem a produzir soluções heterogêneas quanto à interpretação da legislação de proteção de dados. Dessa forma, essa consistência é importante para impedir que empresas que eventualmente não cumpram com a LGPD acabem por obter vantagens competitivas em relação às demais (DONEDA, 2021, p. 265).

Dentre os diversos níveis de atuação dessa agência, destaca-se a sua função preventiva e educativa. É essencial que a ANPD tenha condições para atuar diante da complexidade do tema da proteção e tratamento de dados pessoais, possuindo o papel de educar e incentivar as organizações, informar os consumidores sobre o uso de dados no contexto de produtos e serviços, de forma clara e transparente. Deve, ainda, estabelecer limites apropriados para o seu processamento, visando garantir que esse seja feito em observância aos direitos e interesses dos titulares dos dados.

Faz-se necessário, também, garantir que as discussões sobre educação, cumprimento da lei e penalidades se estabeleçam em conformidade aos princípios consonantes na legislação. Diante disso, a autoridade se torna uma referência e orientadora para o cidadão e para as instituições na matéria.

O tratamento de dados é uma atividade complexa, realizada por entidades cujas práticas podem não ser suficientemente transparentes. Com isso, a existência de uma autoridade que atue de forma coordenada para prevenir e reprimir abusos, fiscalizando o tratamento de dados é fundamental para diminuir a assimetria entre o cidadão e os entes que coletam e tratam seus dados (DONEDA, 2021, p. 466).

Dessa forma, enquanto a educação e a informação não alcançam o patamar almejado de efetivamente implementar uma cultura de privacidade e proteção de dados pessoais, é mister que haja uma fiscalização consistente da Autoridade no que tange ao tratamento de dados por agentes públicos e privados, para que se verifique se a atuação destes agentes está ocorrendo em conformidade ao regramento, em respeito e atenção à proteção de dados pessoais e à privacidade de indivíduos.

Por esta razão, a atuação da ANPD em prol do estabelecimento e funcionamento de programas de governança de proteção de dados no setor privado deve ser bem explorada, desenvolvida e realçada, visto que é uma maneira de assegurar a implementação da política pública e, conforme exposto anteriormente, a atuação fiscalizadora e preventiva é necessária para que o objetivo principal da política pública seja alcançado.

Dessa forma, fomentar diálogos frutíferos com agentes de tratamento, assegurando que a inovação seja inserida em uma cultura que tenha respeito pela privacidade é um importante encargo da ANPD, assim como é a criação de programas de incentivo de boas práticas, aplicáveis em modelos nos quais as organizações descrevem claramente o processamento de dados pessoais.

Para compreender como a Autoridade pode fomentar as boas práticas nas empresas, a seguir serão destacados os pontos principais sobre programas de conformidade, *compliance*, ou governança, em um contexto específico de proteção de dados pessoais.

2 O COMPLIANCE, A GOVERNANÇA CORPORATIVA DE PROTEÇÃO DE DADOS E O PRINCÍPIO DA PREVENÇÃO

O termo *compliance* é um substantivo proveniente da língua inglesa, decorrente do verbo *to comply*, que significa conformidade, obediência, observância e submissão. O uso do termo se tornou comum na atualidade para fazer alusão à implementação de políticas internas de integridade às normas e regramentos. Freitas e Blanchet (2020, p. 34) destacam que o *compliance* surgiu inicialmente no setor privado, com a execução de procedimentos internos aptos a pautar a atuação das empresas de acordo com a legislação e regulamentos vigentes:

> Trata-se, pois, de um conjunto de regras e modelos que envolvem procedimentos éticos suficientes a orientar o comportamento de uma empresa no mercado em que se insere, seja local ou internacional, envolvendo todos os seus agentes e relações desenvolvidas em seu respectivo ramo de atuação, com preocupações transcendentes, como no aspecto de marca, nome e do respeito para com a própria sociedade (FREITAS; BLANCHET, 2020, p. 34).

Esse sistema implica em uma alteração completa do funcionamento da entidade que objetiva adotá-lo, razão pela qual é sempre fruto da instalação de uma política de governança corporativa, elaborada em consonância aos valores éticos assumidos pela empresa, ao controle de riscos e a conformidade às regras jurídicas preestabelecidas.

Alguns de seus pilares essenciais são os códigos de conduta; a avaliação e contingenciamento de riscos; o controle interno por meio de procedimentos capazes de diagnosticar, apurar e sanar não conformidades; treinamentos e comunicações para propagar uma cultura concernente às políticas previamente definidas; assim como os canais pelos quais é possível denunciar não conformidades e as investigações internas que permitem descobri-las (MARTINS; FALEIROS JUNIOR, 2020, p. 359).

Portanto, trata-se de um sistema complexo, que não está restrito ao mero "fazer cumprir" a legislação. Estas práticas devem acarretar uma significativa mudança de mentalidade e preocupação das empresas, e gerar uma atuação em conformidade com o ordenamento jurídico, princípios e normas regulamentares e administrativas. Dessa forma, o controle de riscos e a preservação de valores intangíveis devem configurar um compromisso efetivo assumido pela empresa e ser coerentes com a sua estrutura e estratégia (FREITAS; BLANCHET, 2020, p. 35).

Sendo assim, a governança corporativa aplicada à atividade empresarial é o resultado da adoção de princípios norteadores considerados como ideais pelos seus instituidores, os quais se tornam a base de toda a conduta empresarial, o que traz reflexos na gestão da empresa e em sua relação com acionistas, com o mercado e com os consumidores (SIMÃO FILHO, 2020, p. 337).

A governança corporativa enseja a adoção de boas práticas, que podem ser implementadas por meio de associações ou de forma individual pela empresa. Quando implementadas individualmente, são chamados de programas de conformidade, integridade ou *compliance.* Quando implementados no âmbito de associações, os mecanismos de boas práticas são chamados simplesmente de "autorregulação" (CARVALHO; MATTIUZZO; PONCE, 2020, p. 365).

Implementada individualmente ou por meio de associações, nessa governança vigora a lógica na prevenção, como se observa no caso da proteção de dados pessoais, onde ela assume um papel de destaque para que a almejada segurança de informação seja alcançada.

A experiência internacional sobre o tema demonstra que a preocupação com a adoção de práticas de prevenção e segurança pelos controladores de dados está presente há décadas.

Em 1980, na publicação do influente texto "*OCDE Guidelines on the protection privacy and transborder flows of Personal Data"* o *accountabily principle* foi mencionado pela primeira vez como uma diretriz para a proteção de dados pessoais e da privacidade. Esse princípio pode ser traduzido pela necessidade dos agentes de tratamento de dados se comprometerem com a adoção de medidas que deem real efetividade às regras a eles aplicáveis (CARVALHO; MATTIUZZO; PONCE, 2020, p. 363).

A valoração da prevenção ocorre porque o objetivo da política pública é sempre o seu cumprimento, e não a responsabilização diante de desvios. Essa lógica fica evidente na análise de

políticas de proteção de dados, nas quais o objetivo principal é mitigar os riscos de vazamento de dados, as violações de privacidade e o acúmulo excessivo de informações pessoais de indivíduos por agentes específicos.

Ademais, trata-se de uma seara em que os danos de pequena monta são comuns, o que diminui a propensão para que se postule individualmente sua reparação a partir dos institutos tradicionais de responsabilidade civil. Com isso, a utilização de uma tutela baseada na responsabilidade civil não é um instrumento capaz de tutelar na medida necessária o direito fundamental à proteção de dados, podendo até mesmo incentivar a consolidação de práticas de utilização indevida de dados pessoais (DONEDA, 2021, p. 646).

Dessa forma, ainda que as sanções sejam necessárias para efetivar a aplicação de uma política pública, vale ressaltar que o objetivo principal da política é sempre gerar o cumprimento e adequação comportamental dos agentes, e não a mera punição. Sendo assim, a prevenção e a orientação são peças-chaves do sistema que se pretende construir, razão pela qual a prevenção é um princípio geral de tratamento de dados pessoais (CARVALHO; MATTIUZO; PONCE; 2020, p. 361).

Conforme será abordado a seguir, esta premissa fica evidente diante de uma análise da LGPD, a qual dispõe expressamente sobre a importância e o dever dos agentes privados de instaurarem programas de conformidade e adequação às diretrizes estabelecidas pelo dispositivo legal, em respeito à segurança da informação e a proteção dos dados pessoais.

3 AS BOAS PRÁTICAS E GOVERNANÇA NA LGPD

Antes do advento da legislação em foco, a autorregulação das empresas era a regra, visto que, diante da ausência do poder público em regular a matéria, o próprio mercado estabelecia as regras de conduta e normas padrão de tratamento de dados pessoais (ARAUJO; CAVALHEIRO, 2014).

Ocorre que, com o avanço exponencial da economia movida a dados, a autorregulação passou a ser um cenário propício para a economia digital inidônea, especialmente quando agentes econômicos passam a vender informações pessoais de indivíduos para terceiros sem a anuência destes. Sendo assim, perante uma crescente preocupação com a temática, o arcabouço legal sobre a matéria é uma tentativa de "regular a autorregulação", de maneira que a liberdade das empresas no espaço virtual seja resguardada (ARAUJO; CAVALHEIRO, 2014).

A LGPD destinou uma seção inteira às regras de boas práticas e governança, que ocupam um lugar de destaque entre os artigos 46 a 51. Estas práticas se caracterizam como instrumentos de governança corporativa que visam estabelecer procedimentos que facilitem e viabilizem o cumprimento da legislação. Nesse sentido, a adoção destes mecanismos por parte dos agentes de tratamento de dados pessoais possui o condão de facilitar o processo e consolidá-lo.

As políticas de governança propostas pela LGPD assemelham-se à modalidade de autorregulação da atividade empresarial. Entretanto, se diferenciam do modelo tradicional, posto

que devem ser elaboradas e implementadas com base nas diretrizes estipuladas pela legislação, que exigem que estes programas reflitam efetivamente a estrutura, a escala e o volume das operações da empresa. Entende-se que, assim, os riscos de violação à privacidade dos indivíduos serão minimizados, com o tratamento das informações pessoais sempre pautado na segurança (CARVALHO; MATTIUZZO; PONCE, 2020, p. 366).

Não obstante, ao atribuir aos controladores e operadores de dados a possibilidade de elaborarem, individualmente ou por meio de associações, as boas práticas e as próprias regras de governança, a legislação estabeleceu um mecanismo de "corregulação". Com isso, destacam Lucca e Lima (2020, p. 376), a regulação da atividade é realizada tanto pelos agentes privados quanto pela ANPD, a quem cabe fiscalizar e incentivar os mecanismos de governança e as boas práticas:

> A opção brasileira é justamente a corregulação, ou seja, a ANPD desempenhará suas funções fiscalizadora, reguladora e sancionatórias, sem excluir a possibilidade de os agentes de tratamento de dados pessoais estabelecerem "Boas Práticas" (LUCCA; LIMA, 2020, p. 376).

Os padrões de boas práticas e os princípios gerais previstos na lei devem ser observados pelas entidades na implementação de seus programas de governança corporativa. Nesse sentido, o artigo 50 da LGPD impõe um rol de obrigações relacionadas à governança e boas práticas, impondo atenção redobrada à natureza, ao escopo, e à finalidade dos dados, bem como, à gravidade dos riscos e aos benefícios decorrentes de tratamento de dados do titular (MARTINS; FALEIROS JUNIOR, 2020, p. 357).

As premissas principais desse sistema norteiam a conduta do agente responsável para que forneça ao titular conhecimento sobre o tratamento a ser empreendido aos dados e ao fluxo das informações, de maneira concisa, transparente, inteligível e de fácil acesso, com uma linguagem clara e simples (SIMÃO FILHO, 2020, p. 328).

Muito embora não exista um modelo rígido de orientação aos programas de conformidade para fins de tratamento de dados pessoais no Brasil, fica assegurada a capacidade da ANPD expedir orientações nesse sentido posteriormente.

Ademais, o comprometimento na adoção de programas internos que assegurem o cumprimento de normas relativas à temática, a adequação de condutas com base em um processo de avaliação sistemática de impactos e riscos à privacidade, e o objetivo de estabelecer uma relação de confiança com o titular dos dados por meio de uma atuação transparente, que assegure mecanismos de participação, são requisitos que devem ser observados em qualquer programa de proteção de dados (CARVALHO; MATTIUZZO; PONCE, 2020, p. 366).

É essencial identificar todos os processos, procedimentos e sistemas internos que estejam relacionados ao tratamento de dados pessoais na empresa, para que, por meio de um levantamento de todos estes processos seja possível avaliar os riscos. Sendo assim, é elaborado um verdadeiro mapa dos fluxos internos de diferentes classes de dados pessoais usados e processados pela empresa.

Dessa forma, é possível analisar a adequação das práticas mapeadas com a LGPD. Entretanto, "não serão poucas as medidas de adequação necessárias. Nesse cenário, desenhar uma matriz de riscos para criar um cronograma de adequação da empresa é uma medida comum e eficaz" (CARVALHO; MATTIUZZO; PONCE, 2020, p. 367).

É imprescindível que a probabilidade e gravidade dos riscos sejam consideradas no desenvolvimento de medidas de governança, para que então, seja possível adequar os sistemas, documentos, processos e procedimentos internos à legislação.

Com isso, as atividades empresariais são complemente transformadas, visando um objetivo comum, a mitigação dos riscos identificados e a redução de ocorrência de desvios legais. Não obstante, o compromisso firmado pela entidade é o ponto chave capaz de efetivamente alterar toda a conduta corporativa nesse sentido, a qual deve estar em conformidade com valores e práticas consoantes com os princípios de tratamento de dados pessoais.

Além disso, é de suma importância que a entidade tenha uma cultura que não valorize somente resultados financeiros acima de tudo. Certamente, em observância à atividade empresarial, a obtenção de lucro será sempre o objetivo final, entretanto, há uma clara diferença entre a valorização de resultados e a adoção de práticas fora da conformidade apenas para a obtenção de benefícios lucrativos. Nesse sentido, é necessário que aquilo que é exigido no dia a dia da corporação, dos funcionários e colaboradores, esteja de acordo com as boas práticas e com a política de governança corporativa implementada (CARVALHO; MATTIUZZO; PONCE, 2020, p. 370).

Os instrumentos de boas práticas e governança não pretendem eliminar por completo os incidentes de segurança, porém, objetivam minimizar as possibilidades de ocorrência, e criar mecanismos para que eventuais equívocos sejam devidamente identificados e combatidos de forma eficaz, rápida e adequada (CARVALHO; MATTIUZZO; PONCE, 2020, p. 364).

A exigência de controles preventivos capazes de mitigar os riscos do tratamento de dados é o reflexo de um fundamento primordial do regramento, o da segurança da informação. Toda informação adquire dimensão relevante na medida em que conduz à personalização do indivíduo a quem faz referência. Dessa forma, os mecanismos usados para atender ao imperativo da segurança reverberam na proteção de atributos da personalidade do titular dos dados (MARTINS; FALEIROS JUNIOR, 2020, p. 350).

Dessa forma, os dados pessoais coletados e tratados pelas empresas devem estar protegidos pelas medidas de segurança técnicas e administrativas capazes de proteger as informações de acessos não autorizados, de situações acidentais ou ilícitas de destruição, de perdas, alterações, ou qualquer forma de tratamento inadequado ou ilícito, desde a fase da concepção do dado até o seu descarte (MARTINS; FALEIROS JUNIOR, 2020, p. 351; SIMÃO FILHO, 2020, p. 338).

Assim, são criadas salvaguardas em casos de eventuais riscos de acidentes, bem como, sistemas que possibilitem o exercício de direitos dos titulares de terem acesso aos dados tratados; de solicitarem a correção de dados incompletos, inexatos ou desatualizados; de solicitar a anonimização, o bloqueio ou eliminação de dados desnecessários, etc. (CARVALHO; MATTIUZZO; PONCE,

2020, p. 368).

No artigo 49 da LGPD, o legislador estipulou como um dever que os sistemas utilizados para o tratamento de dados estejam estruturados para atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos demais princípios previstos na lei (MARTINS; FALEIROS JUNIOR, 2020, p. 357; SIMÃO FILHO, 2020, p. 338).

Diante disso, observa-se o objetivo da legislação em incentivar a adoção do *compliance* das empresas, por meio da implementação de uma política de governança que determina a adoção de boas práticas. Essas práticas deverão ser observadas e adotadas em conjunto ao princípio do *privacy by design*, que dispõe sobre a necessidade de os sistemas utilizados para o tratamento de dados pessoais serem estruturados seguindo padrões de boas práticas e governança, os princípios de tratamento de dados pessoais e os requisitos de segurança (CARVALHO; MATTIUZZO; PONCE, 2020, p. 362).

Dessa maneira, a transparência, a segurança e a prevenção são parâmetros inegociáveis, que ultrapassam a atuação estatal repressiva, pautada no instituto da responsabilidade civil, e, pautados na boa fé objetiva, na inserção da ética nas relações negociais, na prevenção e na efetivação dos direitos fundamentais à privacidade e proteção de dados, transitam para um imperialismo da governança – ou *compliance* (MARTINS; FALEIROS JUNIOR, 2020, p. 357).

Nesse diapasão, conforme será abordado a seguir, a legislação não apenas dispôs quanto à necessidade de implementação de políticas de governança de proteção de dados, como também atribuiu às empresas o encargo de comprovar a sua adoção, a efetividade destas práticas e a adequação dos seus sistemas internos à legislação. Com isso, o *accountability* é um instrumento a ser observado pela ANPD na fiscalização da conduta empresarial.

4 O *ACCOUNTABILITY* E AS POLÍTICAS DE PROTEÇÃO DE DADOS

A partir de uma análise do dispositivo legal, nota-se a relevância da segurança da informação, do princípio da prevenção e da mitigação de riscos diante do tratamento de dados pessoais por agentes privados. Dessa maneira, conforme exposto acima, é imprescindível que as empresas contribuam e mudem práticas que não estejam em conformidade com o exigido.

Não obstante, é imprescindível que esta mudança de comportamento e a adequação das práticas internas sejam feitas de maneira transparente, para que, desta forma, o poder público e a sociedade sejam capazes de fiscalizar a atuação destes agentes econômicos. Por esta razão, é possível recorrer à noção de *accountability* para fazer alusão à necessidade de transparência da governança corporativa das empresas para com a Autoridade e os consumidores.

Accountability, em sentido amplo, corresponde à preocupação central da ética da responsabilidade. Em sentido estrito e aplicado, refere-se às relações sociais circunscritas, como as previstas nos sistemas racional-burocráticos de prestação de serviços, por exemplo. Dessa maneira, a *accountability* está diretamente relacionada à genuína eficácia organizacional, e, portanto, deve

ser uma preocupação inerente de qualquer administrador ou funcionário, seja ele público ou privado, visto que, a ética da responsabilidade se ocupa em colocar o detentor de expectativas frente ao agente encarregado de sua satisfação (ETZIONI, 2014, p. 312).

Trata-se de um termo importante para os administradores de instituições em geral, o qual se aproxima das ideias de responsabilidade, prestação de contas, satisfação, explicação e atendimento. Conforme explicita Etzioni (2014, p. 297), a demanda por mais *accountability* pode ser observada, normalmente, em três contextos concretos, seja para referir-se à exigência de mais responsabilidade e sensibilidade; à necessidade de maior atenção ou consideração para com a comunidade, ou para exigir maior compromisso com "valores".

É cediço que os administradores respondem as articulações de direitos apresentadas pela comunidade, por seus líderes ou pela imprensa. Dessa forma, a *accountability* é observada como uma instância efetiva real na qual a administração dá respostas aos reclamos e demandas de interesses particulares de diversos grupos (ETZIONI, 2014, p. 307).

Entretanto, cumpre mencionar que o dever de prestar contas não se limita à capacidade em dar respostas. A prestação de contas deve ser tratada como uma estratégia para administração de expectativas, visto que a capacidade para dar respostas acaba por ser insatisfatória quando envolve apenas respostas limitadas, diretas e meramente formais. Dessa maneira, a prestação de contas envolve os meios pelos quais as organizações administram as diversas expectativas geradas dentro e fora da organização (ETZIONI, 2014, p. 314).

Em que pese a complexidade do termo utilizado, para fins do presente estudo, a perspectiva analisada de *accountability* deve ser interpretada em conjunto à transparência, e traduz-se na obrigação dos agentes privados prestarem contas à ANPD sobre as suas políticas de governança corporativa, ou *compliance,* de proteção de dados, de maneira que seja possível comprovar, com transparência, a adequação das práticas internas com a legislação.

Uma análise acerca das políticas de proteção de dados ao redor do mundo esclarece que estas foram desenvolvidas com base no *accountability principle,* ao atribuir aos próprios agentes de tratamento de dados pessoais a responsabilidade de comprovarem a adoção de medidas que efetivem as regras que são a eles aplicáveis (CARVALHO; MATTIUZZO; PONCE, 2020, p. 362).

Dessa forma, uma vez implementada a política de governança de proteção de dados por agentes privados, a *accountability* é um recurso por meio do qual o poder público é capaz de fiscalizá-la. Este princípio está inserido no artigo 6º, X da LGPD, intitulado como "princípio da responsabilização e da prestação de contas". Trata-se da obrigação do controlador de dados de adotar medidas eficientes e capazes de comprovar a observância e o cumprimento às normas de proteção de dados pessoais.

É de suma importância que as entidades que estão sob regulação da ANPD contribuam para que a Autoridade possa cumprir suas incumbências. Dessa maneira, diante de qualquer processamento de dados, as organizações devem aferir previamente os riscos da atividade, contabilizar e mitigar possíveis danos, contando com as diretrizes de interpretação e aplicação da lei pelas autoridades competentes. Nesse cenário, usos inovadores de dados não devem ser

presumidos como ilegais, entretanto, diante de processamentos inéditos, o processo de aferição prévia de riscos e a mitigação de danos será sempre necessário (ARBIX, 2020, p. 62).

A governança corporativa parte do pressuposto da necessidade da transparência em relação ao mercado, especialmente no que tange a elaboração e disponibilização do seu sistema de informações contábeis. Estas informações devem retratar o estado atual da organização, em observância as regras que dispõem sobre os deveres de informação, diligência e lealdade (SIMÃO FILHO, 2020, p. 335).

Portanto, é imprescindível que as empresas mantenham um conjunto de documentos capazes de evidenciar que as obrigações estão sendo satisfeitas, os quais podem ser extraídos do mesmo artigo 6º da LGPD, como no registro de operações de tratamento, no relatório de impacto e nos registros de incidentes de segurança (CARVALHO; MATTIUZZO; PONCE, 2020, p. 369).

As empresas devem desenvolver minutas destes documentos para comunicação à ANPD. O relatório de impacto, por exemplo, deve consistir efetivamente no resultado do mapeamento e da mensuração de riscos realizados na implementação do programa de governança. Sendo assim, deverá descrever os tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações, bem como, medidas, salvaguardas e mecanismos de mitigação de riscos adotados pela organização (CARVALHO; MATTIUZZO; PONCE, 2020, p. 369).

Diante de incidentes de segurança que possam acarretar risco ou dano aos titulares de dados pessoais, a comunicação imediata à ANPD é obrigatória e urgente, para que a autoridade possa verificar a gravidade do incidente e determinar a adoção de providencias, como a ampla divulgação do fato em meios de comunicação e a adoção de medidas para reverter ou mitigar os efeitos do incidente, nos termos do art. 48 §2º da LGPD (SIMÃO FILHO, 2020, p. 339; MARTINS; FALEIROS JUNIOR, 2020, p. 356).

Na análise da gravidade e alcance do incidente, a ANPD deve solicitar aos agentes comprovações de que foram adotadas medidas técnicas adequadas capazes de tornar os dados pessoais afetados ininteligíveis para que terceiros não autorizados não consigam acessá-los. Sendo assim, a aferição do impacto levará em conta todas as medidas de segurança implementadas na instituição para a prevenção do evento danoso (SIMÃO FILHO, 2020, p. 339; MARTINS; FALEIROS JUNIOR, 2020, p. 356).

Com isso, o registro de incidentes de segurança assume um papel central, especialmente diante de riscos ou ocorrência de incidentes. Nesse caso, a LGPD dispõe sobre quais informações detalhadas devem constar na comunicação da organização à ANPD e aos titulares de dados que sejam eventualmente prejudicados: a descrição da natureza dos dados pessoais afetados; as informações sobre os titulares envolvidos; a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados; os riscos relacionados ao incidente e as medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo (CARVALHO; MATTIUZZO; PONCE, 2020, p. 370; SIMÃO FILHO, 2020, p. 339).

No caso de incidentes de segurança, é essencial que a organização desenvolva sistemas que possibilitem rapidamente sua identificação, a resposta e a remediação. Devem, ainda, ser

comunicados o quanto antes à ANPD e aos titulares de dados pessoais afetados (CARVALHO; MATTIUZZO; PONCE, 2020, p. 368).

A elaboração, manutenção e apresentação desses documentos é de total responsabilidade das empresas. Nesse sentido, é necessário que a empresa norteie toda a sua atividade de tratamento de dados com base neles. Dessa forma, "é disso que se trata a *accountability,* que em sentido lato se pode traduzir como a obrigação de prestar contas aos portadores de expectativas" (ETZIONI, 2014, p. 313).

Observa-se que a intenção é criar um sistema em que agentes de tratamento estão em efetivo diálogo com as autoridades, de modo que os parâmetros de atuação da iniciativa privada são revisados e debatidos com os agentes públicos e segmentos da sociedade civil interessados (CARVALHO; MATTIUZZO; PONCE, 2020, p. 363).

O controle exercido pela administração pública surge da necessidade de correção de rumos frente aos interesses das sociedades. Nesse cenário, diante da *accountability* prestada pelas empresas, o controle não deve ficar restrito exclusivamente ao poder público, visto que, além de um controle administrativo e hierárquico exercido no âmbito das instituições, existe ainda um controle democrático ou social, exercido sob as organizações por meio da democracia representativa (DEPRÁ; LEAL, 2017, p. 227).

Apesar deste não ser o foco da pesquisa, ressalta-se que, não apenas o controle institucional, porém o controle social também decorre da concepção de *accountability*. O controle social é corolário a democracia e proporciona uma característica dialógica entre o Estado e a sociedade civil, "especialmente por fatores ligados com a prestação de contas, a responsabilidade dos agentes e também a burocracia estatal, fatores esses que assentam, em última análise, a consolidação da nossa democracia" (DEPRÁ; LEAL, 2017, p. 233).

Dessa forma, a noção de *accountability* está relacionada com a responsabilização democrática referente a dois mecanismos, um vertical, referente ao controle social; e um horizontal, que se efetiva mediante a fiscalização mútua entre os poderes, ou por meio de outras agências governamentais que monitoram e fiscalizam o poder público e a atividade econômica quando necessário (DEPRÁ; LEAL; 2017, p. 234).

Conforme será exposto na próxima seção, a função fiscalizadora atribuída pelo dispositivo legal à ANPD permite que a Autoridade utilize dos relatórios e instrumentos supracitados para que possa fiscalizar as práticas de governança de proteção de dados implementadas nas empresas privadas.

5 A ANPD E A FISCALIZAÇÃO E INCENTIVO À ADOÇÃO DE BOAS PRÁTICAS PELAS EMPRESAS

A LGPD centralizou na ANPD o encargo de editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como, normas, orientações e procedimentos

simplificados e diferenciados, para que, dessa forma, seja possível que as entidades conheçam as regras e possam se adequar previamente (LUCCA; LIMA, 2020, p. 375).

Entretanto, o tratamento de dados pessoais é uma atividade que perpassa e gera implicações em diversos segmentos de mercado, razão pela qual, é inviável que a ANPD estipule diretrizes claras e específicas para cada um deles. Não obstante, ela possui um arsenal específico de medidas regulatórias a sua disposição, dentre as quais se destacam as medidas que visam a incutir e fomentar boas práticas no tratamento de dados por meio das regras de *accountability* (DONEDA, 2021, p. 265).

Por essa razão, a legislação estabelece o modelo da "corregulação", a partir do momento em que as próprias empresas assumem a capacidade de desenvolverem os seus próprios sistemas de boas práticas e as suas políticas de governança, e, portanto, passam a regular o exercício de sua atividade de tratamento de dados em conjunto com a Autoridade.

A corregulação advém da legislação europeia, na qual a autoridade de controle analisa previamente os códigos de conduta das empresas, os quais ficam pendentes de aprovação e registro para efeitos de comprovação da conformidade com o regramento e posterior disponibilização ao público. Além disso, posteriormente a autoridade também supervisiona os códigos que aprova (SIMÃO FILHO, 2020, p. 342).

Mecanismos semelhantes podem ser encontrados na LGPD, visto que a lei estipula que os programas de governança corporativa devem ser constantemente monitorados, atualizados, e submetidos a avaliações periódicas. Dessa maneira, a pedido da ANPD, o agente de tratamento deve demonstrar a conformidade e efetividade do seu programa de governança, que deve ser reconhecido e divulgado pela autoridade, a quem cabe estimular a adoção de padrões técnicos que facilitem o controle dos dados pelos seus titulares (SIMÃO FILHO, 2020, p. 343).

Nesse aspecto, enquanto as empresas devem adequar controles internos de proteção, segurança e sigilo, bem como elaborar documentos internos que estejam alinhados aos princípios de tratamento de dados pessoais, compete à ANPD fiscalizá-los.

O art. 38 da lei atribui à ANPD a capacidade de solicitar o relatório de impacto à proteção de dados pessoais, que deve ser elaborado obrigatoriamente pelas empresas. Ocorre que, a LGPD não desenvolve hipóteses especificas de quando a autoridade deverá fazê-lo. Sendo assim, a legislação deixa a critério da ANPD determinar em quais circunstâncias o relatório deverá ser requisitado:

> No caso brasileiro, a LGPD não chega a prever hipóteses específicas de requisição do documento, estabelecendo apenas a incumbência da ANPD para sua requisição, ou para a indicação do nível de detalhamento esperado. Existe, portanto, considerável espaço para posterior regulação por parte da ANPD acerca da exata operacionalização dos relatórios de impacto à proteção de dados pessoais (CARVALHO; MATTIUZZO; PONCE, 2020, p. 369).

A prestação de contas, ou *accountability*, das entidades deve ser observada para que a

ANPD possa cumprir a sua função fiscalizadora dos programas de governança de proteção de dados nas empresas. Dessa forma, a fiscalização e cobrança constante dos relatórios de impacto, de segurança e atuação, que devem ser entregues de maneira minuciosamente detalhada, são imprescindíveis para que as empresas alterem efetivamente a sua conduta moral e ética, e respeitem definitivamente a privacidade dos indivíduos.

Não obstante, outro fator capaz de ensejar uma atuação cada vez mais responsável dos agentes de tratamentos de dados são os critérios usados pela ANPD para estipular sanções administrativas, visto que, o art. 52, IX da lei dispõe que a Autoridade levará em consideração a adoção de políticas de boas práticas e governança adotadas por empresas ao aplicá-las. Sendo assim, diante de uma atuação incisiva da Autoridade neste sentido, as entidades privadas se sentirão compelidas a adotarem as medidas de prevenção, seja por vontade própria de mudar a corporação, ou por receio das consequências que descenderão caso elas não o façam.

Por fim, o artigo 51 da LGPD prevê que cabe à ANPD promover a adoção de padrões para a facilitação técnica do controle de dados pelos titulares. Isso significa que a ANPD é corresponsável por propiciar a materialização do rol de direitos do titular de dados, previsto no art. 18 da lei, dentre os quais se destacam o acesso, a anonimização, o bloqueio, a exclusão ou correção dos dados pessoais (MARTINS; FALEIROS JUNIOR, 2020, p. 367).

Sendo assim, a consolidação de uma política pública preventiva propalada pela ANPD, que objetiva promover a adoção de padrões técnicos que facilitem o acesso do titular, assim como, as boas práticas e a instauração de programas de governança de proteção de dados por entes privados, dependerá desta conjugação de fatores que, estando presentes, será propícia e condizente aos propósitos indicados no texto legal (MARTINS; FALEIROS JUNIOR, 2020, p. 367).

Conforme já exposto, a LGPD trouxe diversos dispositivos que proporcionam uma fiscalização séria e consistente da ANPD do tratamento de dados efetuado por agentes privados. Sendo assim, o uso prudente destes instrumentos é de suma importância para que a conduta das instituições privadas se altere e paulatinamente configure um âmbito de atuação respeitoso com as informações pessoais de indivíduos, independente de sua origem.

Diante disso, observa-se que a consolidação da política de proteção de dados pessoais e da privacidade em muito dependerá da atuação da ANPD, especialmente no estímulo e na fiscalização de políticas de governança de proteção de dados em instituições privadas.

CONCLUSÃO

O presente estudo destacou a função preventiva e educativa da ANPD, discutindo a importância da fiscalização da governança corporativa de proteção de dados. Buscou-se demonstrar a importância do *compliance* ou governança para que a política de proteção de dados pessoais e da privacidade, implementada no Brasil com o advento da LGPD, seja bem-sucedida.

Conforme apontado, a lógica da prevenção está presente nessa análise desde quando a

proteção de dados pessoais se tornou uma temática digna de atenção e regulação. Dessa forma, a LGPD destinou vários dispositivos que demonstram a importância da adoção de políticas de boa governança e boas práticas pelos agentes privados, razão pela qual é imprescindível que as empresas destinem tempo e verba para a implementação de políticas internas de privacidade e se adéquem as regras previstas pela legislação.

Não obstante, a mera adequação à norma não é suficiente, posto que a legislação exige que os agentes privados sejam capazes de demonstrar aos titulares dos dados e à ANPD que estão atuando em conformidade ao regramento e a adequação de todos os seus sistemas internos a ele. Por essa razão, o artigo destacou o *accountability principle*, o qual estabelece aos controladores de dados a responsabilização por uma prestação adequada e transparente de contas.

Nesse sentido, a LGPD exige dos controladores de dados a elaboração de relatórios de impacto, de registros de reação aos incidentes de segurança e outros documentos indispensáveis, assim como, a sua constante atualização e monitoramento.

Esses instrumentos são importantes para que a ANPD efetivamente fiscalize e conduza estes agentes para uma atuação em prol da prevenção, da segurança da informação, da privacidade e da proteção de dados.

Com isso, destacou-se a importância da atuação da Autoridade para regular a política de proteção de dados e contribuir para a sua consolidação, especialmente por meio do incentivo e da fiscalização de políticas de governança corporativa de proteção de dados em empresas privadas.

REFERÊNCIAS

ARAUJO, Luiz Ernani Bonesso; CAVALHEIRO, Larissa Nunes. A proteção de dados pessoais na sociedade informacional brasileira: o direito fundamental a privacidade entre a autorregulação das empresas e a regulação protetiva do internauta. **Revista do Direito Público**, Londrina, v. 9, n. 1, p. 209-226, jan./abr. 2014. DOI 10.5433/1980-511X.2014v9n1p209

ARBIX. Daniel. A importância da privacidade por Design e por Default (Privacy by Design and by Default). In: DONEDA, Danilo; MENDES, Laura Schertel (coord.) **Lei Geral de proteção de dados (Lei nº 13.709/2018). A caminho da efetividade: contribuições para a implementação da LGPD**. São Paulo: Thomson Reuters, 2020. p. 55-62.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 maio 2021.

CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. Boas Práticas e Governança na LGPD: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. *In*: BIONI, Bruno; DONEDA, Danilo; JUNIOR, Otavio Luiz Rodrigues; MENDES, Laura Schertel; SARLET, Ingo Wolfgang. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

DEPRÁ, Vinicius Oliveira Braz; LEAL, Mônica Clarissa Hennig. Fiscalização do orçamento público: accountability e controle social da atividade financeira do Estado. **Revista do Direito Público**, Londrina, v. 12, n. 3, p. 216-241, dez. 2017. DOI 10.5433/1980-511X2017v12n3p216

DONEDA, Danilo. A autoridade nacional de proteção de dados e o conselho nacional de proteção de dados. *In*: BIONI, Bruno; DONEDA, Danilo; RODRIGUES JUNIOR, Otavio Luiz; MENDES, Laura Schertel; SARLET, Ingo Wolfgang. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

ETZIONI, Amitai. Concepções alternativas de *accountability*: exemplo da gestão da saúde. *In*: HEIDEMANN, Francisco G.; SALM, José Francisco. **Políticas públicas e desenvolvimento**: bases epistemológicas e modelos de análise. Brasília: Editora Universidade de Brasília, 2014.

FREITAS, Daniel Paulo Paiva de; BLANCHET, Luiz Alberto. A adoção explícita do compliance pela Administração Pública Direta. **Revista do Direito Público**, Londrina, v. 15, n. 3, p. 30-47, dez. 2020. DOI 10.5433/24157-108104-1.2020v15n3p. 30

LUCCA, Newton; LIMA, Cíntia Rosa Pereira. Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. *In*: DE LIMA, Cíntia Rosa Pereira (org.). **Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019**. São Paulo: Almedina, 2020.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Segurança, boas práticas, Governança e *Compliance*. *In*: DE LIMA, Cíntia Rosa Pereira (org.). **Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019**. São Paulo: Almedina, 2020.

SIMÃO FILHO, Adalberto. A Governança Corporativa Aplicada às Boas práticas e *compliance* na Segurança dos dados. *In*: DE LIMA, Cíntia Rosa Pereira (org.). **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019. São Paulo: Almedina, 2020.

VILELA, Danilo Vieira. A nova lei geral para as agências reguladoras no Brasil – Lei n.º 13.848/2019. **Revista do Direito Público**, Londrina, v. 15, n. 2, p. 91-115, ago. 2020. DOI 10.5433/24157-108104-1 2020, v.15, n.2, p.91

Recebido em: 17/05/2022

Aceito em: 24/03/2023