REVISTA JUSTIÇA DO DIREITO
DOI 10.5335/rjd.v36i1.13379

Principais disposições da governança em privacidade à luz da Lei Geral de Proteção de Dados no Brasil[1]

Main provisions of governance in privacy concerning of the general data protection law in Brazil

Grace Ladeira Garbaccio[2]
Lorenzo-Mateo Bujosa Vadell[3]
Bruno Torchia[4]

Resumo

O tema abordou as principais disposições da Lei Geral de Proteção de Dados (LGPD) no Brasil, os elementos e os parâmetros da governança em privacidade. Constatou-se que a Lei Geral de Proteção de Dados é uma norma complexa, que exige muitas medidas para sua adequação, estando inserida numa economia digital. Sua edição foi necessária, uma vez que as normas anteriores não eram totalmente capazes de proteger a privacidade das pessoas naturais. Defende-se que a responsabilidade é subjetiva, seja cível ou administrativa, com exceção da responsabilidade cível quando houver relação de consumo, que será objetiva, em razão de expressa previsão legal. A natureza da pesquisa é de cunho jurídico-dogmático, com a qual objetiva-se investigar como nova legislação poderia ser cumprida por uma organização privada, com uma contribuição para o estudo prospectivo do direito positivo.

Palavras-chave: Governança em privacidade. Lei Geral de Proteção de Dados. Responsabilidade administrativa. Responsabilidade cível. Responsabilidade subjetiva.

[1] Recebido em: 3/1/2022. Aprovado em: 29/3/2022.
[2] Professora Convidada da Universidade Laval, Québec, Canadá. Professora do Mestrado em Direito da CESMAC. Pós-doutoranda pela Universidade de Limoges/França. Doutora e mestre em Direito pela Universidade de Limoges/ França – reconhecido pela Universidade Federal de Santa Catarina (UFSC). Professora do curso de pós-graduação lato sensu da ESPM e FIA. E-mail: glgarbaccio@hotmail.com.
[3] Doctor and master's in law. Professor at the Faculty of Law at the University of Salamanca. E-mail: lbujosa@usal.es.
[4] Doutorando em Direito Constitucional (IDP). Mestre em Direito Público (FUMEC), especialista em Prevenção e Repressão à Corrupção (Estácio de Sá) e em Combateao Crime Organizado (Universitàdegli Studi di Roma – Tor Vergata). Coordenador do MBA de Governança, Riscos, Regulação e Compliance, Gestão Inovadora em Serviços da Saúde e Segurança do Paciente e Gestão Estratégica em Saúde (FaculdadeUnimed). E-mail: profbrunotorchia@gmail.com

DOI 10.5335/rjd.v36i1.13379

Abstract

The topic addressed the main provisions of the General Data Protection Law (GDPL) in Brazil, the elements and parameters of privacy governance. It was found that the General Data Protection Law is a complex norm, which requires many measures for its adequacy, being inserted in a digital economy. Its approval was necessary since the previous norms were not fully capable of protecting the privacy of natural persons. It is argued that liability is subjective, whether civil or administrative, except for civil liability when there is a consumer relationship, which will be objective, due to an express legal provision. The nature of the research is of a legal-dogmatic nature, with which the objective is to investigate how new legislation could be fulfilled by a private organization, with a contribution to the prospective study of positive law.

Keywords: Administrative responsibility. Civil liability. General Data Protection Law. Privacy governance. Subjective responsibility.

Introdução

A Lei n.º 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados (LGPD), trouxe, para o ordenamento jurídico brasileiro, disposições que objetivam regular o tratamento de dados pessoais, seja este tratamento realizado por pessoa física ou jurídica. Segundo seu artigo 3º, aplica-se a lei em comento a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada no território nacional, a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional.[5]

Estudar e compreender a governança em privacidade é essencial para não só demonstrar pró-atividade e ética corporativa, como também buscar prevenir ou minorar as sanções. É objetivo geral deste trabalho avaliar os principais parâmetros e diretrizes da governança em privacidade exposto na Lei Geral de Proteção de Dados. São objetivos específicos compreender as principais características e o objeto de proteção da Lei Geral de Proteção de Dados? O que é a governança em privacidade? Quais os principais parâmetros e diretrizes deste programa de governança em

[5] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 fev. 2022a.

DOI 10.5335/rjd.v36i1.13379

privacidade para ser considerado efetivo? O que este programa de governança em privacidade contribui para a organização privada?

O gênero da pesquisa é teórico, uma vez que objetiva analisar e rever teorias doutrinárias, sendo de cunho jurídico-dogmático. Objetiva-se investigar como a nova legislação, referente à proteção de dados, poderia ser cumprida por uma organização privada, com uma contribuição para o estudo prospectivo do direito positivo, com base no exame de referências de artigos e estudos bibliográficos.

1. Da Lei Geral de Proteção de Dados

A Lei n.º 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), teve sua vigência postergada, conforme verifica-se ao analisar suas alterações posteriores, quais sejam, a Lei n.º 13.853, de 08 de julho de 2019, e a Lei n.º 14.010 de 10 de junho de 2020.[6]Ainda assim, a vigência da LGPD não foi plena, uma vez que as normas atinentes à Autoridade Nacional de Proteção de Dados (ANPD) entraram em vigor somente no dia 28 de dezembro de 2018, bem como as disposições gerais em dia 18 de setembro de 2020; e por fim, as sanções administrativas somente no dia 01 de agosto de 2021.

Portanto, as organizações, públicas e privadas, e a sociedade tiveram tempo razoável para compreender as disposições gerais da lei, a importância da ANPD e o processo de sua adequação, antes de sua plena vigência. Inevitável comparar que até mesmo o Código Civil de 2002, legislação que possui 2.046 (dois mil e quarenta e seis) artigos e trata de todos os assuntos da vida privada, teve um *vacatio legis* de 1 (um) ano, sendo, portanto, inferior ao da Lei Geral de Proteção de Dados.

A referida lei objetiva traçar regras para o tratamento de dados pessoais[7] para que, reflexamente, haja proteção à privacidade da pessoa natural. Através da proteção de tais dados, resguarda-se a intimidade, a vida privada, a honra e a imagem

[6] Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019) I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019) I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020) II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019). BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados.

[7] A LGPD define tratamento no artigo 5º, inciso X, como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração". BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados.

DOI 10.5335/rjd.v36i1.13379

da pessoa natural. O ordenamento jurídico brasileiro já possuía, antes da Lei Geral de Proteção de Dados, outras disposições normativas, com a pretensão semelhante de tutelar esses direitos, tais como a Lei n.º 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), a Lei n.º 10.406, de 10 de janeiro de 2002 (Código Civil), a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet) e o Decreto-Lei n.º 2.848, de 07 de dezembro de 1940 (Código Penal),[8] além disso, é claro, a própria Constituição Federal de 1988, que estabelece em seu artigo 5º, como direito e garantia fundamental, a inviolabilidade da intimidade, da vida privada, da honra e da imagem da pessoa, das suas correspondências e das comunicações telegráficas.

Se o ordenamento jurídico brasileiro já dispunha de regras para proteção da privacidade da pessoa natural, inclusive com embasamento constitucional, pode-se questionar a utilidade de mais uma norma, a Lei Geral de Proteção de Dados, para tratar o mesmo assunto. Contudo, na atual era tecnológica, com a disposição de dados, da economia digital, através da qual há uma coleta maciça de dados, que muitas vezes não encontra limites e despreza a intimidade e a vida privada dos usuários, as normas, até então vigentes, não estavam preparadas para lidar com esta nova economia e com tamanho volume de informações pessoais, demandando um novo modelo de gestão dos dados pessoais.[9]

Sobre o atual modelo de negócio do século XXI, há um traço característico importante: muitas empresas não são mensuradas economicamente pelos seus bens materiais, ou seja, seus imóveis, equipamentos, etc., mas sim pela detenção de dados e pela potência e capacidade de seus softwares em extrair valor destes. Por isso, é clássica a frase: os dados são o novo petróleo.[10] Os modelos de negócios são disruptivos e têm potencial até mesmo para alterar arcabouços regulatórios até então estabelecidos.[11]

[8] As condutas que atentam contra a honra e a divulgação do segredo estão tipificadas, como regra geral, nos artigos 138, 139, 140, 153 e 154, do Código Penal.

[9] SANTOS, Marcela de Oliveira; MOTTA, Fabrício. 3. Regulação administrativa de dados. In: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Coords). **LGPD e administração pública: uma análise ampla dos impactos**. 1ª edição. São Paulo: Thomson Reuters Brasil, 2020.

[10] NOLIN, Jan Michael. Data as oil, infrastructure or asset? Three metaphors of data aseconomic value. **Journal of Information, Communication and Ethics in Society**, Vol. 18 No. 1, p. 28-43. Disponível em:https://www.emerald.com/insight/content/doi/10.1108/JICES-04-2019-0044/full/html.Acessoem 10 set. 2020.

[11] BENACCHIO, Marcelo; MACIEL, Renata Mota. 2. A Lei Geral de Proteção de Dados sob a perspectiva da regulação do poder econômico. In: DE LIMA, Cíntia Rosa Pereira (Coord). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020, p. 43-49.

DOI 10.5335/rjd.v36i1.13379

Essa busca incessante por lucros faz com que muitas organizações atuem de maneira antiética, desprezando os direitos não só das pessoas físicas, como também das pessoas jurídicas com as quais concorre, podendo haver, em ambos os casos, a violação da Lei Geral de Proteção de Dados.[12] Embora tal conclusão possa parecer equivocada aprioristicamente, porquanto a lei volta-se a proteger a pessoa natural, importante realçar que dentre seus fundamentos temos a livre iniciativa e a livre concorrência, conforme exposto no artigo 2º, inciso VI.

Ainda no tocante à estrutura e à dimensão de proteção da Lei Geral de Proteção de Dados, é imprescindível que as organizações, públicas e privadas, criem mecanismos para cumprimento de suas disposições. Elas podem ser jurídicas, tais como obediência aos seus princípios (da boa-fé, transparência, finalidade, adequação, etc.), aos seus fundamentos (privacidade, direitos humanos, livre iniciativa, etc.), à eleição adequada da base legal, atendimento aos direitos dos titulares, entre outros, como também podem ser técnicas, como adequação e revisão dos mecanismos de segurança da informação, tais como *firewall*, controles de acesso, políticas de segurança de informação, entre outros. A complexidade da governança em privacidade será proporcional aquela da atividade empresarial, do volume e natureza de dados tratados (comuns ou sensíveis).

Tendo em vista um dos objetivos de a governança ser a prevenção de responsabilidades, analisar-se-á a responsabilidade cível e administrativa, preconizada na Lei Geral de Proteção de Dados Pessoais, ressaltando, porém, que a governança vai muito além dessa prevenção, não devendo ser esse seu objetivo principal, como se mostrará no capítulo 3 deste trabalho.

DOI 10.5335/rjd.v36i1.13379

2. Responsabilização cível e administrativa prevista na Lei Geral de Proteção de Dados

Discorrer sobre a responsabilidade cível e administrativa da Lei Geral de Proteção de Dados é tarefa complexa, pois ainda que haja uma vasta doutrina, o tema carece de ser amadurecido pelos nossos tribunais.[13]

De maneira geral, a finalidade da responsabilidade cível é a recomposição das perdas e danos, a qual será proporcional à extensão do dano ou do prejuízo sofrido pela vítima, a teor do que estabelece os artigos 927 e 944, do Código Civil.[14]Já a responsabilidade administrativa se funda não no dano, mas sim na necessidade de respeito às normas produzidas pelo Estado. O seu descumprimento pressupõe o exercício do poder sancionatório do Estado, dispondo de vários critérios, dentre eles o dissuasório (sanção que realmente cause um efeito punitivo) e da prevenção geral (demostrar à sociedade que cumprir uma norma é vantajoso).

Faz-se necessária a análise dos institutos da responsabilidade cível e administrativa para demonstrar como a governança em privacidade é importante para as organizações manterem seu patrimônio e reputação íntegros. De início, o que está nítido na Lei Geral de Proteção de Dados, segundo o disposto no artigo 6º, inciso X, é seu alicerce na responsabilização e na prestação de contas, impondo ao agente adotar "medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".[15]

Entende-se que a responsabilidade cível, prevista na referida lei, é de natureza subjetiva, em razão da ausência de disposição legal expressa que regula o tema, tal como acontece com o Código de Defesa do Consumidor e na Política Nacional do Meio Ambiente. Contudo, a própria Lei Geral de Proteção de Dados

[13] Um estudo publicado em julho de 2021, demonstrou haver cerca de 600 decisões sobre o tema Lei Geral de Proteção de Dados Pessoais, contudo sobre diferentes temáticas. Disponível em: <https://www1.folha.uol.com.br/mercado/2021/07/justica-ja-tem-600-decisoes-envolvendo-lei-de-protecao-de-dados.shtml> Acesso em: 10 fev. 2022.

[14] Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem. [...] Art. 944. A indenização mede-se pela extensão do dano. Parágrafo único. Se houver excessiva desproporção entre a gravidade da culpa e o dano, poderá o juiz reduzir, eqüitativamente, a indenização. BRASIL. **Lei n. 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 10 fev. 2022c.

[15] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados.

estabelece que a responsabilidade será objetiva somente se os titulares de dados estiverem envolvidos em uma relação de consumo.[16] No mesmo sentido, Flávio Henrique Unes Pereira e Rafael da Silva Alvim[17] esclarecem que o artigo 42 é verdadeira cláusula geral de responsabilização e que a irregularidade no tratamento de dados é o pressuposto autorizador da responsabilidade, conforme artigo 44. Já o artigo 43 estabelece rol taxativo de excludentes, sendo que o inciso II estabelece que a licitude da conduta exclui a responsabilidade. A responsabilidade cível seria subjetiva porque não se pode inferir responsabilidade objetiva, ela deve decorrer de menção legal expressa.

Com relação à responsabilidade administrativa, a análise se mostra mais complexa. Aqui, há previsão expressa das sanções em seu artigo 52, as quais devem ser tratadas no rol taxativo. Contudo, não há delimitação na lei a respeito de quais são as infrações administrativas que ensejariam a aplicabilidade das respectivas sanções. Na ausência de norma expressa estabelecendo as infrações, não se mostra possível o sancionamento pela via administrativa por parte da ANPD,[18] ainda que sua competência prevaleça sobre outras entidades da Administração Pública.[19]Mas para efetivar tais sanções, a referida Agência publicou a Resolução CD/ANPD nº 1, de 28 de outubro de 2021, denominada Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador. Pelo que se vê, as sanções administrativas podem ser aplicadas sempre que houver violação à legislação de proteção de dados pessoais - o que é um conceito bem amplo de descumprimento - já que essa é a disposição do artigo 37, do referido Regulamento: "O processo administrativo

[16] TORCHIA, Bruno Martins; MACHADO, Tacianny Mayara Silva. 45. A responsabilidade subjetiva prevista na Lei Geral de Proteção de Dados e a relação jurídica entre controlador e o encarregado de proteção de dados. Augusto Neves; MARTINS, Ricardo Marcondes (Coords). L**GPD e administração pública: uma análise ampla dos impactos**. 1ª edição. São Paulo: Thomson Reuters Brasil, 2020.
[17] PEREIRA, Flávio Henrique Unes; ALVIM, Rafael da Silva. 44. A responsabilidade civil do Estado por danos decorrentes do tratamento de dados pessoais: um estudo de caso. Augusto Neves; MARTINS, Ricardo Marcondes (Coords). **LGPD e administração pública: uma análise ampla dos impactos**. 1ª edição. São Paulo: Thomson Reuters Brasil, 2020.
[18] Art. 55-J. Compete à ANPD: [...] IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso. BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados.
[19] Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados.

DOI 10.5335/rjd.v36i1.13379

sancionador destina-se à apuração de infrações à legislação de proteção de dados de competência da ANPD, nos termos do artigo 55-J, IV, da LGPD".[20]

As sanções podem ser publicização da infração, eliminação dos dados pessoais a que se refere a infração, suspensão parcial do funcionamento do banco de dados, suspensão do exercício da atividade de tratamento, proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. Todas elas podem impactar diretamente o negócio de uma organização punida.

As infrações administrativas, ainda que descritas por ato regulamentar, devem obedecer aos princípios da legalidade, da tipicidade e até mesmo da culpabilidade, geralmente estudados na seara penal, mas plenamente aplicáveis ao direito administrativo sancionador. Isso porque, defende-se a existência de um direito público punitivo que irradia seus efeitos tanto para as sanções administrativas quanto penais, ainda que os critérios dos regimes jurídicos sejam distintos, falhos e lacunosos.[21] No mesmo sentido, Diogo de Figueiredo Neto ensina que há necessidade de importar ao Direito Administrativo sancionador todos os princípios constitucionais atinentes à tipologia penal.[22] A inexorável conclusão é que a responsabilidade administrativa é também subjetiva.

Todavia, o tal direito administrativo sancionador é um ramo mais permissivo que o direito penal, tendo em vista que não experimentou anos de evolução e sistematização deste. No direito penal os princípios se encontram melhor definidos e as principais garantias com assento constitucional. Já o direito administrativo sancionador brasileiro dispõe de uma lei geral com tais vedações, regras e

[20] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados**. Brasília, 2021a.

[21] OSÓRIO, Fábio Medina. **Direito administrativo sancionador**. São Paulo: Revista dos Tribunais, 2015, p. 123.

[22] É atemporal o escólio de Diogo de Figueiredo Moreira Neto e Flávio Amaral Garcia: "Assim, como exemplo, não se admite a existência de crime sem lei anterior que o defina, nem pena sem prévia cominação legal (princípio da legalidade - art. 5o, XXXIX); estabelece-se a previsão de que a lei penal não retroagirá, salvo para beneficiar o réu (princípio da irretroatividade - art. 5o, XL); prevê-se a vedação de que a pena não passará da pessoa do condenado (princípio da intranscendência da pena - art. 5o, XLV) e de que qualquer indivíduo seja privado da liberdade ou dos seus bens sem o devido processo (princípio do devido processo legal - art. 5o, LIV) e se afirma o direito, assegurado a todo e qualquer litigante, em processo judicial ou administrativo, de ampla defesa (princípio da ampla defesa e do contraditório - art. 5o, LV)". MOREIRA NETO, Diogo de Figueiredo; GARCIA, Flavio Amaral. A principiologia no direito administrativo sancionador. **Revista Eletrônica de Direito Administrativo Econômico (REDAE)**, Salvador, Instituto Brasileiro de Direito Público, no. 28, novembro/dezembro/janeiro, 2011/2012. Disponível em: < http://www.direitodoestado.com.br/codrevista.asp?cod=702>. Acesso em: 10 fev. 2022, p. 4-5.

DOI 10.5335/rjd.v36i1.13379

procedimentos, aplicáveis à União, aos Estados-membros e aos Municípios, na medida de cada regulamentação.

Como a Lei Geral de Proteção de Dados já estabelece uma quantidade considerável de medidas, tanto técnicas como jurídicas, que devem ser adotadas pelas organizações (públicas ou privadas), não se vislumbra, em princípio, ilegalidade na descrição por atos regulamentares de suas infrações, porque o princípio da tipicidade no direito administrativo não é tão rígido como no direito penal.

Em razão de tal circunstância, a governança poderá contribuir para a aplicação de tal legislação, pois a implementação de suas disposições potencializa-se em um eficiente mecanismo de obediência à norma, evidenciando medidas que, segundo disposição legal, serão avaliadas pela ANPD na aplicação de uma eventual sanção.

3. Governança e *Compliance*: Principais distinções

A Lei Geral de Proteção de Dados estabelece, em seu Capítulo VII, denominado Da Segurança e Boas Práticas, duas seções: sendo a primeira denominada Da Segurança e do Sigilo de Dados e a segunda Das Boas Práticas e da Governança. Na visão de ALMEIDA e SILVA,[23] a Lei Geral de Proteção de Dados procura definir em duas seções os parâmetros mínimos relacionados às medidas de segurança a serem adotadas pelos agentes de tratamento.

Antes de adentrar, especificamente, na discussão sobre a governança em privacidade, expressamente mencionada em lei, é relevante distinguir, inicialmente, que *compliance* e governança corporativa são institutos distintos.

A governança corporativa não é um conceito jurídico, mas sim administrativo-econômico, por ter uma ligação muito estreita com gestão e corresponder a submissão, da organização e de seus órgãos de gestão e de controle, a um sistema de regras impositivas de conduta com conteúdo ético, para atingir o fim social com parâmetros razoáveis e corretos.[24]

[23] ALMEIDA, Felippe Guerra Veiga de; SILVA, João Pedro Brígido Pinheiro da. Capítulo VII. Segurança e boas práticas. In: FEIGELSON; Bruno et al (coord). **Comentários à lei geral de proteção de dados**. 1ª ed. São Paulo: Thomson Reuters, 2020.
[24] SIMÃO FILHO, Adalberto. 13. A governança corporativa aplicada às boas práticas e compliance na segurança de dados. In: DE LIMA, Cíntia Rosa Pereira (Coord). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020, p. 329-330.

DOI 10.5335/rjd.v36i1.13379

A governança em privacidade, em um aspecto mais restrito/específico, deve estar atrelada e imbricada na governança corporativa de cada organização, sendo esta intenção do legislador, quando, expressamente, prevê no artigo 50, parágrafo 2º, alínea "f", da Lei Geral de Proteção de Dados, que o programa de governança deve estar "integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos".[25]

Já o *compliance* pode ser compreendido como um conjunto de medidas através das quais se busca cumprir a ordem vigente, observando os princípios da ética e integridade corporativa, se constituindo de procedimentos internos que objetivam evitar práticas ilícitas no âmbito de uma estrutura organizada. O programa surge da necessidade de mitigar os riscos gerados pela atividade corporativa.[26]

A origem dos programas de *compliance* não é de conformidade com dados pessoais, mas sim para evitar crimes econômicos, que ofendem os bens jurídicos mais relevantes para a sociedade, tutelando bens jurídicos de natureza supraindividual. Veja-se o escólio de Márcio Adriano Anselmo ensina:

> O início das preocupações com o tema a partir de casos famosos de falhas de governança mundial (Barings, Enron, World Com, Parmalat), tendo seu auge com a crise financeira de 2008. Some-se a esses fatos a crescente preocupação internacional com o fenômeno da lavagem de dinheiro, sobretudo a partir da criação do Grupo de Ação Financeira (GAFI), no âmbito da OCDE, bem como outras iniciativas internacionais, como, por exemplo, a Declaração de Princípios da Basileia, voltada ao sistema financeiro.[27]

No Brasil, os programas de *compliance*, já estavam previstos na Lei n. 9.613, de 03 de março de 1998, denominada Lei Lavagem de Dinheiro, a qual impõe, desde 1998, às pessoas físicas ou jurídicas obrigações de identificação dos clientes e manutenção de cadastros, ao registro das transações e à comunicação de operações suspeitas, sob pena de imposição de sanções administrativas.[28]Após a Lei n. 12.846/2013, de 01 de agosto de 2013, a Lei Anticorrupção,[29] o *compliance* é

[25] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados.
[26] RIOS, Rodrigo Sánchez; ANTONIETTO, Caio. Criminal compliance – Prevenção e minimização de riscos na gestão da atividade empresarial. **Revista Brasileira de Ciências Criminais**, vol. 114/2015, p. 341-375, Maio - Jun / 2015, p. 2.
[27] ANSELMO, Márcio Adriano. Compliance, direito penal e investigação criminal: uma análise à luz da ISO 19600 e 37001. **Revista dos Tribunais**, Vol. 979/2017, p. 53 – 67, 2017, p. 1.
[28] VERÍSSIMO, Carla. **Compliance: incentivos à adoção de medidas anticorrupção**. São Paulo: Saraiva, 2017, p. 15-17.
[29] BRASIL. **Lei n. 12.846, de 01 de agosto de 2013**. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira,

DOI 10.5335/rjd.v36i1.13379

remodelado e ampliado como mecanismo que busca evitar a prática de atos lesivos contra a administração pública nacional ou estrangeira, não se restringindo apenas às instituições financeiras.[30]

O *compliance,* na vertente da busca da ética corporativa, surge normativamente com a edição da Lei n.º 12.846/2013, que no artigo 7º, inciso VIII, o menciona como "mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica" que podem ser levados em consideração na dosimetria da pena.[31] Eles foram regulamentados de maneira bastante completa com a edição do Decreto n.º 8.420/2015, mais precisamente no artigo 42, que estabeleceu 16 parâmetros.

Atualmente, verifica-se que sempre que se quer discorrer sobre conformidade de alguma legislação, o termo *compliance* é utilizado de forma genérica, não na vertente para a qual foi concebido legalmente no Brasil: antilavagem e anticorrupção.

Ana Frazão, ao escrever sobre os programas de *compliance* na Lei Geral de Proteção de Dados, ensina que o *compliance* pode ser visto como um conjunto de ações a serem adotadas no ambiente corporativo, reforçando a anuência da empresa à legislação vigente prevenindo a ocorrência de infrações, ou se já tendo ocorrida, que possa propiciar o imediato retorno à legalidade. Mas o *compliance* vai muito além, objetivando disseminar a cultura de respeito às normas e ética, e que no caso do *compliance* de dados, todos esses objetivos estarão relacionados ao cumprimento dos direitos dos titulares de dados. Além disso, a autora inclui no programa de *compliance* de dados todas as questões referidas no Capítulo VII (Da Segurança e Das Boas Práticas), da Lei Geral de Proteção de Dados.[32]

e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm >. Acesso em 10 fev. 2022d.

[30] Carla Veríssimo distingue o compliance das normas relacionadas à prevenção à lavagem de dinheiro e o compliance aplicável à Lei Anticorrupção. No primeiro caso o mecanismo é obrigatório, ensejando aplicação de sanções administrativas às pessoas físicas e jurídicas. E no segundo facultativo, sendo sua ausência fator que resultaria apenas na impossibilidade de mitigação da pena de multa administrativa. VERÍSSIMO, Carla. ***Compliance*: incentivos à adoção de medidas anticorrupção**. São Paulo: Saraiva, 2017.

[31] BRASIL. **Lei n. 12.846, de 01 de agosto de 2013**.

[32] FRAZÃO, Ana. Propósitos, desafios e parâmetros gerais dos programas de *compliance* e das políticas de proteção de dados. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. ***Compliance* e política de proteção de dados [livro eletrônico]**. 1ª edição. São Paulo: Thomson Reuters Brasil, 2022.

DOI 10.5335/rjd.v36i1.13379

Para outros autores,[33] os programas de *compliance* representam a meta de se alcançar a plena observância das normas legais, desde a prevenção até a reparação do dano porventura causado pelo eventual descumprimento da lei, criando mecanismos de governança no ambiente corporativo para assegurar a adesão às regras legais e às políticas da entidade, carregando muitas vantagens, dentre as quais acurada gestão de riscos, identificação de eventual descumprimento, criação de cultura corporativa, inspiração de maior credibilidade aos *stakeholders* e servem como atenuante em caso de punições administrativas.

Sempre que os autores mencionam o *"compliance"* ou o "*compliance* de dados", utilizam, basicamente, os parâmetros do programa de *compliance* fixados ou pela Lei n.º 12.846/2013 e o Decreto n.º 8.420/2015.

Oliva *et al*[34] afirmam que são elementos para um programa de *compliance* efetivo a avaliação contínua de riscos e atualização do programa; elaboração de códigos de ética e de conduta; organização compatível com o risco da atividade; comprometimento da alta administração; autonomia e independência do setor de *compliance*; cultura corporativa de *compliance*; treinamentos periódicos; monitoramento constante dos controles e processos; e detecção, apuração e punição de condutas contrárias ao programa de *compliance*.

Ou seja, os autores fizeram uma "releitura" dos programas de *compliance* nascidos na Lei n.º 12.846/2013 aplicados à Lei Geral de Proteção de Dados, pretendendo considerá-los mais extensos, com viés mais jurídicos e com a finalidade de prevenção e remediação de atos ilícitos. Em contrapartida, ao lecionar sobre governança, pretendem apresentá-los como um sistema mais genérico.

Adalberto Simão Filho esclarece que a Lei Geral de Proteção de Dados adota claros princípios de governança nos artigos 46 a 51, mas afirma que:

[33] OLIVA, Milena Donato; ABÍLIO, Vivianne da Silveira; COSTA, André Brandão Nery. 5. Elementos essenciais para estruturação de efetivos programas de *compliance* de proteção de dados. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. ***Compliance* e política de proteção de dados [livro eletrônico]**. 1ª edição. São Paulo: Thomson Reuters Brasil, 2022.

[34] OLIVA, Milena Donato; ABÍLIO, Vivianne da Silveira; COSTA, André Brandão Nery. 5. Elementos essenciais para estruturação de efetivos programas de compliance de proteção de dados. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. ***Compliance* e política de proteção de dados [livro eletrônico]**. 1ª edição. São Paulo: Thomson Reuters Brasil, 2022.

> [...] efetivamos a opção de ajustar o conteúdo proposto, ao sistema clássico de governança corporativa, no âmbito do que terminologicamente se convencionou a denominar de *compliance*, aqui visto no sentido de buscar conformidades com leis e regulamentos externos e internos.[35]

A análise das ideias expostas evidencia que há uma certa indefinição conceitual do que se trata sobre *compliance,* governança corporativa, *compliance* de dados, governança em privacidade e até mesmo governança de dados. As expressões são indistintamente utilizadas, mas ao fim e ao cabo pretendem informar a mesma ideia: a adequação da Lei Geral de Proteção de Dados, ou por *compliance* ou por governança.

Veja que Adalberto Simão Filho conclui que governança corporativa "é vista como um sistema é instituto que contribui para que empresas e instituições possam bem adaptar certas regras advindas da lei geral de proteção de dados".[36]Ou seja, o conceito utilizado para governança seria o mesmo do *compliance:* conformidade.

Oliva et al (2022) lecionam os principais elementos de um programa de *compliance* em proteção de dados, a saber:

> a) Avaliação contínua de riscos e atualização do programa. [...]
> b) Elaboração de Códigos de Ética e de Conduta. [...]
> c) Organização compatível com o risco da atividade. [...]
> d) Comprometimento da alta administração. [...]
> e) Autonomia e independência do setor de compliance. [...]
> f) Cultura corporativa de compliance. [...]
> g) Treinamentos periódicos. [...]
> h) Monitoramento constante dos controles e processos [...].
> i) Canais seguros e abertos de comunicação de infrações e mecanismos de proteção dos informantes. [...]
> j) Detecção, apuração e punição de condutas contrárias ao programa de compliance. [...][37]

Veja-se que os principais elementos do *compliance* seriam também elementos da governança em privacidade, dispostos expressamente no artigo 50, da

[35] SIMÃO FILHO, Adalberto. 13. A governança corporativa aplicada às boas práticas e compliance na segurança de dados. In: DE LIMA, Cíntia Rosa Pereira (Coord). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020, p. 327-328.
[36] SIMÃO FILHO, Adalberto. 13. A governança corporativa aplicada às boas práticas e compliance na segurança de dados. In: DE LIMA, Cíntia Rosa Pereira (Coord). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020, p. 329.
[37] OLIVA, Milena Donato; ABÍLIO, Vivianne da Silveira; COSTA, André Brandão Nery. 5. Elementos essenciais para estruturação de efetivos programas de compliance de proteção de dados. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. **Compliance e política de proteção de dados [livro eletrônico]**. 1ª edição. São Paulo: Thomson Reuters Brasil, 2022.

DOI 10.5335/rjd.v36i1.13379

Lei Geral de Proteção de Dados, em uma leitura mais ampla e com uma interpretação teleológica.

Também, não se pode conceber que uma organização implante a governança em privacidade sem buscar todas as finalidades de um programa de *compliance,* que é de cumprir os direitos dos titulares de dados, atender todos os princípios da lei (boa-fé, transparência, prevenção, segurança e responsabilização), possuir mecanismos que possa prevenir os atos ilícitos, além de seguir todos as obrigações regulatórias, que permeia toda a legislação.

À vista disso, neste trabalho utiliza-se a expressão governança em privacidade para se referir aos pontos necessários de adequação à Lei Geral de Proteção de Dados, que é a conformidade. Governança em privacidade é o *nomen iuris* atribuído na Lei Geral de Proteção de Dados e abarca, no artigo 50, parágrafo 2º, todos os elementos que seriam de um programa de *compliance* (ou *compliance* de dados). Contudo, entende-se que a utilização da expressão *compliance* também é adequada, desde que faça um recorte prévio do significado da expressão.

4. Programa de Governança em privacidade e seus principais elementos

A Lei Geral de Proteção de Dados traz no título do seu Capítulo VII, a expressão Segurança e Boas Práticas, que impõe à organização[38]- referida na lei como agente de tratamento[39], principalmente ao controlador - o dever de implementar um complexo sistema de governança que abranja 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 (artigo 46); que garanta segurança da informação em quaisquer das fases de tratamento que intervenha (artigo 47); que os agentes comuniquem os incidentes de segurança que possam causar risco ou dano aos titulares (artigo 48); que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta lei

[38] Utiliza-se no trabalho a expressão organização como aquela que implanta o programa de governança em privacidade. Mas é importante lembrar que a pessoa natural que exerce atividade com fins lucrativos também está sujeita à Lei Geral de Proteção de Dados e consequentemente obrigada a implantar seu programa.

[39] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Brasília, 2021b.

DOI 10.5335/rjd.v36i1.13379

e às demais normas regulamentares (artigo 49) e que os agentes de tratamento devem formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (artigo 50), sem prejuízo de padrões técnicos estimulados pela ANPD (artigo 51).[40]

Como se vê, conformar-se às disposições da Lei Geral de Proteção de Dados com Segurança e Boas Práticas é tarefa complexa, densa e que demandará custos humanos e pecuniários. Vejamos agora, de maneira mais detalhada, as disposições de cada uma das Seções.

4.1. Da Segurança e Sigilo de Dados

A Seção I, do Capítulo VII, denominada Da Segurança e Sigilo dos Dados, é regulamentada pelos artigos 46 a 49, da Lei Geral de Proteção de Dados.

Sobre a norma do artigo 46, Almeida e Silva ensinam:

> Entre as diretrizes apresentadas, ressaltamos as que consideramos principais, quais sejam: (i) o estabelecimento de um controle estrito sobre o acesso dos dados coletados, (ii) a previsão de um mecanismo de autenticação de registros, e (iii) a criação de um inventário detalhado de acesso e o uso de técnicas de inviolabilidade dos dados, tais como a criptografia e anonimização dos dados coletados.[41]

O artigo 46, da Lei Geral de Proteção de Dados, portanto, é de crucial importância, pois de plano já estabelece que as organizações devem estabelecer governança em privacidade com adoção de medidas de segurança, técnicas e administrativas. Ou seja, não basta apenas a instalação de um software ou estruturação de processos, é importante trabalhar com este tripé. Por outro lado, a governança em privacidade não tem apenas o fito de impedir ataques *hackers*, por exemplo, mas de proteger a organização também de outras condutas, inclusive culposas, que possam representar um tratamento inadequado. Deve-se mudar a

[40] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados.
[41] ALMEIDA, Felippe Guerra Veiga de; SILVA, João Pedro Brígido Pinheiro da. Capítulo VII. Segurança e boas práticas. In: FEIGELSON; Bruno et al (coord). **Comentários à lei geral de proteção de dados**. 1ª ed. São Paulo: Thomson Reuters, 2020.

DOI 10.5335/rjd.v36i1.13379

cultura da organização. A lei é clara ao impor que tais medidas devem ser 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.[42]

O estabelecido no artigo 46 - aliado ao previsto no artigo 50 - pavimenta o caminho para a responsabilidade cível dos agentes de tratamento na Lei Geral de Proteção de Dados. Esse amplo dever de proteção deve existir em qualquer fase de tratamento dos dados, inclusive desde a concepção do serviço ou produto. Os conceitos *privacybydesing* e *privacy by default* (privacidade desde a concepção e privacidade por padrão, respectivamente) são distintos, sendo o primeiro entendido como a privacidade em toda e qualquer ação das suas atividades e o último entendido como a configuração de privacidade mais rígida presente por padronização nos seus sistemas.[43]

O artigo 47, da referida lei, estabelece que os agentes de tratamento devem garantir a segurança da informação em relação aos dados pessoais, mesmo após o seu término. Isso significa que a lei tem efeitos ultrativos, porque deve a organização providenciar segurança da informação, inclusive no período pós-contratual, sob pena, também, de eventual responsabilização cível.[44] A lei não estabelece padrões objetivos de segurança da informação, e nem poderia, porque estes padrões dependem do momento em que se realiza esta análise, o que irá variar de ano em ano ou de décadas em décadas. A lei, enquanto norma geral e abstrata deve ser atemporal, razão pela qual esta avaliação será realizada no caso concreto e com critérios vigentes à época. Ao contrário do que muitos pensam, a lei também não estabelece qualquer necessidade de certificação.

Já o artigo 48 trata do incidente de segurança, o qual impõe à organização uma série de providências sempre que verificar algum evento que possa ter acarretado risco ou dano relevante aos titulares, tudo no intuito de promover a proteção dos dados pessoais e da privacidade das pessoas.[45] Para além das

[42] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**.
[43] MARTINS, Guilherme Magalhães; JÚNIOR, José Luiz de Moura Faleiros. 14. Segurança, boas práticas, governança e compliance. In: DE LIMA, Cíntia Rosa Pereira (Coord). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020, p. 350-352.
[44] MARTINS, Guilherme Magalhães; JÚNIOR, José Luiz de Moura Faleiros. 14. Segurança, boas práticas, governança e compliance. In: DE LIMA, Cíntia Rosa Pereira (Coord). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020, p. 354.
[45] **Lei n. 13.709, de 14 de agosto de 2018**.

DOI 10.5335/rjd.v36i1.13379

providências exigidas, o dever de comunicação de incidente de segurança repousa num contexto mais amplo de governança corporativa. Objetiva cumprir os princípios da transparência, segurança e prevenção previstos no artigo 6º, da Lei Geral de Proteção de Dados. Como decorrência, necessário se faz incutir a cultura de ética, incentivando as organizações a cooperarem na persecução com as autoridades públicas. Este *disclousure*[46] "nada mais é que um atributo desdobrado da ética empresarial que deve reinar em todas as etapas de desenvolvimento e implementação dos processos de coleta, tratamento, e armazenagem de dados pessoais".[47]A ideia é a mesma da Lei n, 12.846/2013, que de forma indireta delega a atividade fiscalizatória às pessoas jurídicas, mantendo-se, por óbvio, suas atribuições e competências hígidas.

Essa comunicação de incidente de segurança vai representar um grande dilema para as organizações, porque se assemelha à uma confissão de um ato ilícito, que gerará, inevitavelmente, repercussão reputacional e financeira por se tornar alvo de demandas judiciais individuais e coletivas[48], além de deixar a organização vulnerável a processos administrativos instaurados pela ANPD. Por outro lado, a não comunicação do incidente, além de revelar uma cultura de *non compliance*, poderá representar um sancionamento mais severo por parte da ANPD quando do exercício do seu poder sancionatório.

O artigo 49, da Lei Geral de Proteção de Dados, indica o dever de as organizações estruturarem de maneira adequada seus sistemas utilizados nos tratamentos de dados.[49] Os sistemas, portanto, devem ser conformes aos requisitos de segurança, padrões de boas práticas e de governança, adequar-se aos princípios da Lei Geral de Proteção de Dados e de outras normas regulamentares aplicáveis.[50]

[46] *Disclousure* é o processo de tornar fatos ou informações conhecidas do público. É a divulgação adequada através da qual as organizações informam seus clientes, investidores e quaisquer pessoas envolvidas as informações pertinentes.
[47] MARTINS, Guilherme Magalhães; JÚNIOR, José Luiz de Moura Faleiros. 14. Segurança, boas práticas, governança e compliance. In: DE LIMA, Cíntia Rosa Pereira (Coord). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020, p. 355.
[48] Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.
[49] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**.
[50] MARTINS, Guilherme Magalhães; JÚNIOR, José Luiz de Moura Faleiros. 14. Segurança, boas práticas, governança e compliance. In: DE LIMA, Cíntia Rosa Pereira (Coord). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020, p. 354.

DOI 10.5335/rjd.v36i1.13379

Em outras palavras, os sistemas devem observar tanto os padrões técnicos como os padrões jurídicos da Lei Geral de Proteção de Dados.

Ainda, quanto aos sistemas, importante citar o Guia Orientativo Sobre Segurança da Informação para Agentes de tratamento de pequeno porte, publicado pela ANPD.[51]

Compreendida as principais disposições sobre as primeiras normas acerca do Capítulo VII, passa-se a análise segunda seção, na qual se analisa efetivamente a governança em privacidade.

4.2. Das Boas Práticas e da Governança

A segunda seção, do Capítulo VII, é denominada Das Boas Práticas e da Governança*,* é tratada na Lei Geral de Proteção de Dados nos artigos 50 e 51[52]. Não é objetivo deste estudo aprofundar na evolução e conceito da governança corporativa, mas é importante expor algumas definições adicionais, em acréscimo ao estabelecido no capítulo anterior.

Governança corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselhos 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.[53]

A governança corporativa, nascida no século XX, teve longa evolução nos Estados Unidos e uma série de acontecimentos que foram remodelando esse sistema. Desde o caso *Watergate* de 1974, a edição do *Foreign Corrupt Pratices Act* em 1977, a Lei *Sarbanes Oxley* de 2002 - apenas para citar as principais - há uma série de mecanismos que foram aperfeiçoados, dentre eles o *compliance*, que pode ser visualizado como um mecanismo da governança corporativa.

[51] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia **Orientativo Sobre Segurança da Informação para Agentes de tratamento de pequeno porte**. Brasília, 2021c.
[52] **Lei n. 13.709, de 14 de agosto de 2018**.
[53] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. 5.ed. São Paulo: IBGC, 2015.

DOI 10.5335/rjd.v36i1.13379

A governança corporativa é resultante da adoção de princípios tidos por norteadores da conduta dos administradores, com reflexos na gestão *interna corporis* e entre acionistas e o mercado, lastreando-se tal conduta em princípios éticos aceitos como ideias pelos seus instituidores.[54]

Todavia, considerando que o disposto na Lei Geral de Proteção de Dados é para implantar a governança em privacidade, passa-se ao seu estudo, tópico por tópico.

4.3. Dos parâmetros mínimos da governança em privacidade

O artigo 50, parágrafo 2º, inciso I, da Lei Geral de Proteção de Dados, mencionando os princípios da segurança e prevenção, estabelece os parâmetros mínimos do programa de governança em privacidade. Ou seja, as organizações podem ir além, sendo o previsto na lei apenas uma moldura básica daquilo que seria necessário.

O primeiro parâmetro é demonstrar "o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais".[55] Tem-se aqui o apoio da alta direção, também denominado *tone from the top.* Sem o envolvimento da alta direção, não há governança. É a alta direção que deve garantir recursos humanos e financeiros para a implantação dos mecanismos e, mais, fiscalizar seu desenvolvimento e monitorar sua efetividade. Aqui, também, é importante a elaboração das políticas e códigos de ética e de conduta necessários à proteção dos dados pessoais.

O segundo parâmetro é que "seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta".[56] Impõe-se que a organização mapeie e insira medidas de controle em todos os processos nos quais haja tratamento de dados pessoais, sejam físicos ou digitais. A governança em privacidade deve abranger todo e qualquer tratamento realizado pela organização. Além disso, a profundidade dos controles a

[54] SIMÃO FILHO, Adalberto. 13. A governança corporativa aplicada às boas práticas e compliance na segurança de dados. In: DE LIMA, Cíntia Rosa Pereira (Coord). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020, p. 337.
[55] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**.
[56] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**.

DOI 10.5335/rjd.v36i1.13379

serem implantados é proporcional à sensibilidade dos dados tratados e dos riscos mapeados.

O terceiro parâmetro é que "seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados".[57] Não adianta uma organização copiar as medidas de controle, políticas e processos de outra organização. Cada pessoa jurídica é específica e detentora de identidade própria, com fragilidades e operações diversas. As medidas de controle jamais podem ser mais onerosas que a própria operação. Mas há que se ter cautela quando se lida com dados pessoais sensíveis, já que seu tratamento inadequado representará maior dano à pessoa natural. Nesse sentido, as organizações ainda que pequenas, devem estar atentas à sensibilidade dos dados que realiza o tratamento.

O quarto parâmetro da governança em privacidade é estabelecer "políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade".[58] A Lei Geral de Proteção de Dados objetiva a publicação e políticas, até para que seja demonstrada a transparência no tratamento de dados pessoais. Mas uma política só é efetiva se corresponder à avaliação de riscos realizada e for disseminada, com treinamento de todos os níveis hierárquicos. A mera publicação de políticas não se mostrará suficiente para proteção de dados.

O quinto parâmetro orienta que a governança em privacidade estabeleça "relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular".[59] Essa é uma decorrência da própria essência da lei, que insere o particular como figura central, empoderado e com vários direitos que possam ser exigidos, sob pena de tutela administrativa ou judicial. Para além, essa relação entre agente de tratamento e titular não deve ser litigiosa, mas amistosa e pautada na boa-fé.

O sexto parâmetro menciona que o programa de governança em privacidade "esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos".[60] O objetivo é claro: todos da organização devem atuar para a proteção de dados, sem exceção, devendo a organização zelar para que haja *due diligence* tanto com relação aos empregados

[57] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**.
[58] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**.
[59] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**.
[60] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**.

DOI 10.5335/rjd.v36i1.13379

como também aos terceiros. O programa deve ser monitorado e aperfeiçoado de acordo com aquilo que ocorre na organização, inclusive com as falhas de conformidade e com eventuais incidentes de segurança.

O sétimo parâmetro exige que o programa "conte com planos de resposta a incidentes e remediação".[61]Pretende-se que a organização inclua no seu programa mecanismos efetivos para detecção e remediação de eventuais tratamentos ilícitos no intuito de comunicar a ANPD e os titulares acerca de possíveis violações à lei, tal como incidentes de segurança, sem olvidar do embasamento de um plano para remediar tais irregularidades, ou ilicitudes.

Por fim, o oitavo e último parâmetro, exige que o programa "seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas".[62]O programa de governança em privacidade deve ser atualizado continuamente, aperfeiçoado. Dessa forma, o inventário de dados, avaliação de legítimo interesse e os relatórios de impacto à proteção de dados pessoais devem ser continuamente revistos e adequados para o cenário fático vivenciado.

Estes são parâmetros mínimos que devem ser seguidos por cada organização, mas de acordo com a sua realidade. O artigo 51, da Lei Geral de Proteção de Dados, deixa claro que a ANPD poderá estabelecer critérios, ou seja, redimensionar as exigências.

4.4. Qual a contribuição do programa de governança em privacidade para a organização?

A decisão de uma organização em se dedicar à temática governança é crucial para sua perenidade no mercado, dos profissionais que irão se interessar em fazer parte de sua missão, bem como dos consumidores que pretende atingir. Estar em conformidade não é uma escolha fundada apenas com base em disposições regulatórias, mas sim o quanto aquela pessoa jurídica quer ir além, atuar com ética e disseminar boas práticas comerciais e não comerciais (ambientais e sociais). Mas não

[61] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**.
[62] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**.

DOI 10.5335/rjd.v36i1.13379

se engane, estar em *compliance,* como se diz, é também crucial para a prevenção de responsabilidades cível, administrativa e até criminal, a depender dos casos.[63]

No que toca à Lei Geral de Proteção de Dados, está prevista expressamente as disposições referentes para configuração de responsabilidade cível, bem como as sanções inerentes à responsabilidade administrativa. O que se extrai da literalidade da Lei Geral de Proteção de Dados é sua natureza principiológica, exigindo que as organizações atuem com boa-fé, transparência, segurança, prevenção e prestação de contas. E o descumprimento destes princípios, assim como – é claro – de todas as suas outras regras, representará um tratamento irregular, que é pressuposto de responsabilidade cível e provavelmente da responsabilidade administrativa.

Um eficiente programa de governança em privacidade irá, no mínimo, zelar para que a organização cumpra todos os mandamentos legais, inclusive dos princípios da Lei Geral de Proteção de Dados–que também são normas -, prevenindo a responsabilização em qualquer destas esferas, pelo menos é o que se espera. Não obstante, carecemos de jurisprudência sobre o tema, o artigo 52, parágrafo 1º, da Lei Geral de Proteção de Dados é claro ao mencionar os parâmetros a ser observado pela autoridade no sancionamento. Veja-se:

> 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**:
> I – a gravidade e a **natureza das infrações** e dos direitos pessoais afetados;
> II –a **boa-fé** do infrator;
> III – a vantagem auferida ou pretendida pelo infrator;
> IV –a condição econômica do infrator;
> V –a**reincidência**;
> VI –o grau do dano;
> VII – a **cooperação** do infrator;
> 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**; e
> XI – a proporcionalidade entre a gravidade da falta e a intensidade da sanção".[64] (grifo nosso).

[63] Principalmente quando se trata dos crimes de corrupção, previstos nos artigos 317 e 333, do Código Penal.
[64] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**.

DOI 10.5335/rjd.v36i1.13379

As organizações que adotarem um efetivo programa de governança em privacidade terão em comparação com as organizações que não o possuem uma situação muito mais vantajosa para apresentar sua defesa no eventual processo administrativo, que repercutirá positivamente em muitos parâmetros estabelecidos pelo legislador, como exemplificadamente discorre-se abaixo.

Porém, perceba, não se pode dizer que um programa de governança em privacidade evitará os atos ilícitos e irregularidades na sua totalidade, mas a tendência é que este programa pelo menos evite atos mais gravosos ou infrações mais primárias, já que se predispõe a analisar todos os dados da organização com uma avaliação de riscos (inciso I). A boa-fé é uma decorrência da ética empresarial, e embora a organização entenda o lucro como necessário, não persegue ele como seu único objetivo (inciso II). Um programa de governança em privacidade funciona de forma a continuamente se aprimorar, analisando cada descumprimento como uma verdadeira oportunidade de melhoria, reduzindo de sobremaneira a reincidência (inciso V). A organização em conformidade busca prevenir, mitigar ou remedir o ato ilícito praticado dentro dos seus limites, de forma que não pugna pela ocultação de irregularidades, mas sim atuando ao lado do Estado para se descubra a verdade e a punição dos envolvidos, dentro do mais amplo e irrestrito devido processo legal (inciso VII e X). E tudo isso será feito com a adoção de boas práticas, políticas, processos e medidas corretivas, que é a base de todo programa de *compliance* (inciso VIII e IX).

Assim, entende-se que a implementação da governança em privacidade é crucial para que se cumpra as diversas obrigações impostas à organização (ou ao controlador), sejam elas de natureza jurídica ou técnica. Não menos importante, estar em conformidade com a lei repercutirá positivamente na sociedade e nas relações com as partes envolvidas, já que todos preferem se relacionar com empresas éticas. Para além, os mecanismos da governança contribuirão para que as organizações não respondam ou respondam de forma mais amena quanto aos casos específicos de responsabilização cível ou administrativa.

DOI 10.5335/rjd.v36i1.13379

Considerações finais

A Lei Geral de Proteção de Dados traça regras para o tratamento de dados pessoais para que, reflexamente, haja proteção à privacidade da pessoa natural. As normas até então vigentes, ainda que com esteio constitucional, não estavam preparadas para lidar com esta nova economia digital que impõe um novo modelo de gestão dos dados pessoais.

A mesma possui suas bases fundadas nos princípios da responsabilização e da prestação de contas, impondo ao agente adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

O descumprimento das disposições legais pode ensejar responsabilidade cível, que visa a recomposição das perdas e danos e a responsabilidade administrativa, que persegue a manutenção das normas de conteúdo público, decorrendo do poder punitivo do Estado. A responsabilidade cível prevista na referida lei é de natureza subjetiva como regra geral, salvo se os titulares envolvidos estiverem em uma relação de consumo, que será objetiva. Quanto à responsabilidade administrativa, entende-se que a mesma será sempre subjetiva.

Ao analisar o artigo 50, parágrafo 2º, da Lei Geral de Proteção de Dados, observa-se que muitos dos parâmetros previstos para o programa de governança em privacidade são similares aos parâmetros do programa de integridade regulamentado pelo Decreto n. 8.420/2015. A decisão de uma organização em se dedicar à temática governança, ou *compliance,* é crucial para sua perenidade no mercado, dos profissionais que irão se interessar em fazer parte de sua missão, bem como dos consumidores que pretende atingir.

Um efetivo programa de governança em privacidade tem cunho preventivo, de forma a mitigar o risco de descumprimento da legislação, em especial a Lei Geral de Proteção de Dados, evitando-se responsabilização em qualquer destas esferas e atuando de maneira proativa na proteção da privacidade e dignidade da pessoa humana**.**

DOI 10.5335/rjd.v36i1.13379

Referências

ALMEIDA, Felippe Guerra Veiga de; SILVA, João Pedro Brígido Pinheiro da. Capítulo VII. Segurança e boas práticas. In: FEIGELSON; Bruno *et al* (coord). **Comentários à lei geral de proteção de dados**. 1ª ed. São Paulo: Thomson Reuters, 2020.

ANSELMO, Márcio Adriano. Compliance, direito penal e investigação criminal: uma análise à luz da ISO 19600 e 37001. **Revista dos Tribunais**, Vol. 979/2017, p. 53 – 67, 2017.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados**. Brasília, 2021a.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Brasília, 2021b.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo Sobre Segurança da Informação para Agentes de tratamento de pequeno porte**. Brasília, 2021c.

BENACCHIO, Marcelo; MACIEL, Renata Mota. 2. A Lei Geral de Proteção de Dados sob a perspectiva da regulação do poder econômico. In: DE LIMA, Cíntia Rosa Pereira (Coord). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020, p. 39-67.

BRASIL. **Constituição da República Federativa do Brasil**, de 05 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm>. Acesso em: 10 fev. 2022b.

BRASIL. **Decreto n. 8.420, de 18 de março de 2015**. Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/d8420.htm >. Acesso em 10 fev. 2022e

BRASIL. **Lei n. 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 10 fev. 2022c.

BRASIL. **Lei n. 12.846, de 01 de agosto de 2013**. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm >. Acesso em 10 fev. 2022d.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 fev.2022a.

economic value. **Journal of Information, Communication and Ethics in Society**, Vol. 18No. 1, p. 28-43. Disponível em: <https://www.emerald.com/insight/content/doi/10.1108/JICES-04-2019-0044/full/html>. Acesso em 10 fev. 2022.

FRAZÃO, Ana. Propósitos, desafios e parâmetros gerais dos programas de compliance e das políticas de proteção de dados. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. **Compliance e política de proteção de dados** [livro eletrônico]. 1ª edição. São Paulo: Thomson Reuters Brasil, 2022.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. 5.ed. São Paulo: IBGC, 2015.

MARTINS, Guilherme Magalhães; JÚNIOR, José Luiz de Moura Faleiros. 14. Segurança, boas práticas, governança e compliance. In: DE LIMA, Cíntia Rosa Pereira (Coord). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020, p. 349-371.

MOREIRA NETO, Diogo de Figueiredo; GARCIA, Flavio Amaral. A principiologia no direito administrativo sancionador. **Revista Eletrônica de Direito Administrativo Econômico (REDAE)**, Salvador, Instituto Brasileiro de Direito Público, no. 28, novembro/dezembro/janeiro, 2011/2012. Disponível em: < http://www.direitodoestado.com.br/codrevista.asp?cod=702>. Acesso em: 10 fev. 2022.

NOLIN, Jan Michael. Data as oil, infrastructure or asset? Three metaphors of data as

OLIVA, Milena Donato; ABÍLIO, Vivianne da Silveira; COSTA, André Brandão Nery. 5. Elementos essenciais para estruturação de efetivos programas de compliance de proteção de dados. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. **Compliance e política de proteção de dados** [livro eletrônico]. 1ª edição. São Paulo: Thomson Reuters Brasil, 2022.

OSÓRIO, Fábio Medina. **Direito administrativo sancionador**. São Paulo: Revista dos Tribunais, 2015.

PEREIRA, Flávio Henrique Unes; ALVIM, Rafael da Silva. 44. A responsabilidade civil do Estado por danos decorrentes do tratamento de dados pessoais: um estudo de caso. Augusto Neves; MARTINS, Ricardo Marcondes (Coords). **LGPD e administração pública: uma análise ampla dos impactos.** 1ª edição. São Paulo: Thomson Reuters Brasil, 2020.

RIOS, Rodrigo Sánchez; ANTONIETTO, Caio. Criminal compliance – Prevenção e minimização de riscos na gestão da atividade empresarial. **Revista Brasileira de Ciências Criminais**, vol. 114/2015, p. 341-375, Maio - Jun / 2015.

SAAVEDRA, Giovani Agostini; CRESPO, Liana. I. A. Cunha. 1. Compliance: origem e aspectos práticos. In: CRESPO, Marcelo Xavier Freitas (Coord). **Compliance no Direito Digital - Vol. 3**. 1ª edição. São Paulo: Thomson Reuters Brasil. 2021.

SANTOS, Marcela de Oliveira; MOTTA, Fabrício. 3. Regulação administrativa de dados. In: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Coords). **LGPD e administração pública: uma análise ampla dos impactos.** 1ª edição. São Paulo: Thomson Reuters Brasil, 2020.

SIMÃO FILHO, Adalberto. 13. A governança corporativa aplicada às boas práticas e compliance na segurança de dados. In: DE LIMA, Cíntia Rosa Pereira (Coord). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020, p. 327-347.

TORCHIA, Bruno Martins; MACHADO, TaciannyMayara Silva. 45. A responsabilidade subjetiva prevista na Lei Geral de Proteção de Dados e a relação jurídica entre controlador e o encarregado de proteção de dados. Augusto Neves; MARTINS, Ricardo Marcondes (Coords). **LGPD e administração pública: uma análise ampla dos impactos.** 1ª edição. São Paulo: Thomson Reuters Brasil, 2020.

VERÍSSIMO, Carla. **Compliance: incentivos à adoção de medidas anticorrupção**. São Paulo: Saraiva, 2017.