Revista Direito em Debate

Revista do Curso de Graduação em Direito da Unijuí

Editora Unijuí – Ano XXXII – n. 59 – jan./jun. 2023 – ISSN 2176-6622 – e12451

A PROTEÇÃO DE DADOS PESSOAIS COM O ADVENTO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): Boas Práticas no Tratamento e na Proteção de Dados Pessoais em Empresas Nacionais

http://dx.doi.org/10.21527/2176-6622.2023.59.12451

Submetido em: 21/6/2021
Aceito em: 20/4/2022

Ronny Max Machado

Autor correspondente: Centro Universitário das Faculdades Metropolitanas Unidas – FMU. São Paulo/SP, Brasil.
http://lattes.cnpq.br/3526842654606450. https://orcid.org/0000-0003-2142-0090.
ronnymaxm@yahoo.com.br

Osmar Fernando Gonçalves Barreto

Faculdade Autônoma de Direito de São Paulo – Fadisp. São Paulo/SP, Brasil.
http://lattes.cnpq.br/1063688454568879. https://orcid.org/0000-0003-4204-0847.

Karem Luiza da Costa

Centro Universitário das Faculdades Metropolitanas Unidas. São Paulo/SP, Brasil.
http://lattes.cnpq.br/7804620888391716. https://orcid.org/0000-0003-1799-8199

RESUMO

O presente trabalho tem como objetivo geral apresentar os principais princípios e temas relacionados à privacidade, abarcando os aspectos fundamentais da lei de proteção de dados, passando pela corrupção e responsabilidade dos administradores, apresentando alguns exemplos a respeito de vazamento de dados. O objetivo específico consiste em analisar a aplicabilidade do Programa de *Compliance* que as empresas devem seguir para atendimento dos requisitos impostos na Lei Geral de Proteção de Dados, Lei 13.709/2018 ("LGPD"). A metodologia utilizada foi a pesquisa bibliográfica sobre o tema, por meio de artigos científicos, doutrinas, revistas jurídicas, manuais e periódicos, além de legislação específica e jurisprudências.

Palavras-chave: proteção de dados pessoais; governança corporativa; boas práticas

PROTECTION OF PERSONAL DATA WITH THE ADVENT GENERAL DATA PROTECTION LAW (LGPD): GOOD PRACTICES IN TREATMENT AND PROTECTION OF PERSONAL DATA IN NATIONAL COMPANIES

ABSTRACT

This work has the general objective to present the main principles and themes related to privacy, covering the main aspects of the law of data protection, corruption and the responsibility of the administrators, presenting some examples regarding data leakage. The specific objective is to analyze the applicability of the Compliance Program that companies must follow in order to comply with the requirements imposed by the General Law of Data Protection, Law 13709/2018 ("LGPD"). The methodology used was the bibliographical research on the subject, by the scientific articles, doctrines, legal journals, manuals and periodicals, besides specific legislation and jurisprudence.

Keywords: protection of personal data; corporate governance; good habits.

1 INTRODUÇÃO

O que vemos hoje sendo aplicado pelas empresas que fornecem serviços e produtos, principalmente nos meios digitais, no que diz respeito à regulamentos de sigilo e privacidade de dados que são coletados por usuários e consumidores desses serviços e produtos, são contratos de adesão de uso com termos e condições longos, rebuscados, em que esses usuários e consumidores devem obrigatoriamente aceitá-los para poder utilizar as facilidades que o provedor destas empresas oferece e cuja não aceitação desses termos e condições é motivo de rejeição ao acesso ao referido sistema. Com o crescimento das relações digitais, das tecnologias e da facilidade da coleta de dados pessoais pelas empresas, faz-se necessário pensar em meios mais seguros e transparentes na captura e tratamento desses dados. Com este cenário, a Lei Geral de Proteção de Dados, Lei n. 13.709/2018 ("LGPD"), foi criada para regular o tratamento de proteção dos dados e impor penas em caso de utilização de uso de forma indevida pelas empresas. A aplicabilidade de um Programa de *Compliance* para atender os requisitos desta lei irá trazer mudanças não somente na forma de proteger a privacidade das pessoas, mas também irá gerar novas maneiras de fazer negócios, com maior segurança jurídica, criando novas oportunidades comerciais e investimentos em soluções para a privacidade e segurança de dados, principalmente em relação à mudança cultural, para evitar a coleta indiscriminada de dados.

Deste modo, com o presente artigo, intitulado *A proteção de dados pessoais com o advento da Lei Geral de Proteção de Dados (LGPD): boas práticas no tratamento e na proteção de dados pessoais em empresas nacionais,* procura-se responder a seguinte questão: Qual o papel do Programa de *Compliance* a ser aderido pelas empresas nacionais ante a adequação no tratamento das informações pessoais por pessoa jurídica privada sob a égide do LGPD? A proposta de pesquisa abordará as boas práticas (*compliance*) das empresas privadas em relação ao tratamento dos dados pessoais, tendo como base a LGPD, com o propósito de compreender as novas atribuições, as obrigações e responsabilidades daqueles que manuseiam e tratam os dados pessoais nas relações digitais. O método a ser utilizado será o hipotético-dedutivo, tomando por base legislação específica, doutrinas e jurisprudências. A pesquisa bibliográfica sobre o tema será por meio de artigos científicos, doutrinas, revistas jurídicas, manuais e periódicos.

2 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei 13.709/2018 – Lei Geral de Proteção de Dados –, conhecida como "LGPD", é destinada ao tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, por meio digital ou não. Destaca-se que não é destinada à proteção de dados de pessoa jurídica, mas de pessoa natural. Esta lei irá trazer mudanças na forma de proteger a privacidade das pessoas, bem como irá gerar novas maneiras de fazer negócio com maior segurança jurídica. Como consequência, as empresas brasileiras deverão alterar suas políticas internas, adaptar seus processos de tratamento de dados pessoais (desde a sua coleta até seu descarte), e, principalmente, repensar sua cultura para estarem em conformidade com essa nova legislação. Antes de tomarmos conhecimento dos principais pontos da LGPD, precisamos entender o significado de "dados". Segundo Thomas Davenport e Laurence Prusak (1999):

> Num contexto organizacional, dados são utilitariamente descritos como registros estruturados de transações. Quando um cliente vai a um posto de gasolina e enche o tanque do seu carro, essa transação pode ser parcialmente descrita como dado, assim quando ele faz compras, quantos livros consome, quanto ele pagou (p. 2).

Ainda, conforme os supracitados autores,

> Quantitativamente, as empresas avaliam a gestão de dados em termos de custo, velocidade e capacidade: quanto custa obter ou recuperar um dado? Com que velocidade podemos lançá-lo e recuperá-lo no sistema? Qual a capacidade de armazenamento no sistema? Indicadores qualitativos são a prontidão, a relevância e a clareza: temos acesso a eles quando necessitamos? Eles são aquilo que precisamos? Podemos extrair significado deles? Todas as organizações precisam de dados e alguns setores dependem fortemente deles, como bancos, seguradoras, serviços públicos, Receita Federal, Previdência Social, dentre outros. O registro e manutenção de dados estão no cerne dessas culturas de dados, e a efetiva gestão de dados é fundamental para o

> seu sucesso. Para muitas empresas, acumular dados por criarem a ilusão de exatidão científica. Dados demais podem dificultar a identificação e extração de significado de dados que realmente importam (DAVENPORT; PRUSAK, 1999, p. 3).

É necessário, também, entender o que são dados de natureza pública, dados manifestamente públicos e dados de natureza privada. Observamos que, por vezes, há certa confusão no entendimento dessas naturezas. Por isso, é necessário considerar o nível de exposição do titular, que varia de acordo com o caso e suas circunstâncias. A natureza privada refere-se aos aspectos privados e particulares da vida pessoal do titular, posto que a natureza pública se refere aos aspectos de interesse público, os quais poderão ser utilizados de forma livre. Como exemplo citamos as informações pessoais compartilhadas em rede social, as quais são divulgadas indiscriminadamente ao público. Neste caso, ainda que essas informações tenham sido publicamente divulgadas, permanecem na esfera privada. Nos dizeres de Bruno Ricardo Bioni (2019), o" que é público e privado é o que normatiza o conteúdo do direito à privacidade, sendo a sua lógica centrada na liberdade negativa de o indivíduo não sofrer interferência alheia." (BIONI, 2019, p. 96). Neste sentido, vejamos o entendimento do STF a respeito da informação produzida e gerenciada pelo governo:

> Toda informação produzida ou gerenciada pelo governo é pública? Como princípio geral, sim, salvaguardando-se as informações pessoais e as exceções previstas na lei. A informação produzida pelo setor público deve estar disponível a quem este serve, ou seja, à sociedade, a menos que esta informação esteja expressamente protegida. Daí a necessidade de regulamentação, para que fique claro quais informações são reservadas e por quanto tempo". O entendimento sobre informações pessoais como "aquelas relacionadas à pessoa natural identificada ou identificável, cujo tratamento deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. As informações pessoais terão seu acesso restrito, independentemente de classificação de sigilo, pelo prazo máximo de 100 (cem) anos a contar da sua data de produção (STF, 2021).

Para uso dos dados manifestamente públicos, conforme parágrafo 4º do artigo 7º da LGPD, não se exige o consentimento, a exemplo, informações de perfil em rede social. Devem, no entanto, estar resguardados os direitos do titular e os princípios estipulados na lei. Devem ter tratamento com informações claras e atualizadas sobre previsão legal, finalidade, procedimento e práticas realizadas em veículos de fácil acesso, uma vez que a autoridade competente poderá dispor de formas de publicidade das operações de tratamento, devendo sempre respeitar os princípios de proteção de dados elencados no artigo 6º desta lei. Como assevera Bruno Bioni (2019),

> Em qualquer caso, a definição da legalidade do tratamento dos dados é a sua compatibilidade com a finalidade e o interesse público pelo qual tais dados são de acesso público. Necessário análise contextual para saber se houve publicização da informação, o que calibrará os possíveis (re)usos que dela podem ser feitos. A mesma lógica pode ser transposta no que diz respeito aos chamados "dados manifestamente públicos". Da mesma forma que dados de acesso público, deve ser levado em consideração o contexto em que tal informação foi disponibilizada. Ao ressaltar que os direitos do titular e os princípios previstos na lei estariam resguardados. O parágrafo 4º do artigo 7º da LGPD não autoriza o uso indiscriminado dessas informações (p. 270).

Ademais, o autor citado entende que:

> Ao se analisar o regime jurídico do LGPD dispensado ao legítimo interesse e aos dados públicos e manifestamente públicos, há uma espécie de consentimento contextual em que o cidadão também exerce domínio sobre seus dados, ainda que sem declarar sua vontade, se estes forem tratados de forma previsível, de acordo com as suas legítimas expectativas (p. 273).

Por isso, deve-se considerar a finalidade dos dados pessoais, ou seja, se um titular de dados pessoais disponibilizou seus dados em rede social ou outra mídia social, considerando que um terceiro não pode coletar esses dados e dissociá-lo de sua finalidade e utilizá-lo indevidamente. O parágrafo 3º do artigo 7º da LGPD determina expressamente que o dado pessoal cujo acesso seja público deve considerar a finalidade, a boa-fé e o interesse público que justifiquem sua disponibilização, ou seja, deve levar em conta o contexto pelo qual o dado foi publicamente acessível, por exemplo, dado disponibilizado em base de dados da Administração Pública (certidões, Diário Oficial, certidões de processos judiciais, etc.). Estes podem ser utilizados. A origem

dos dados, entretanto, não retira sua natureza, não importando o meio em que foi divulgado, pois continua sendo dado pessoal. Deve-se fazer seu tratamento de acordo com a base legal aplicável ao caso.

Vale mencionar, também, que o direito à informação está inserido no rol dos direitos fundamentais à dignidade da pessoa humana. A exemplo, *Habeas Data,* remédio constitucional previsto no artigo 5º, inciso XXXIII da Constituição Federal do Brasil. O seu objetivo é acessar as informações que o Poder Público ou entidade de caráter público tem a seu respeito para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, e para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo. Em tal sentido, Michel Temer (1999) ressalta que

> No *Habeas Data*, todos os dados referentes ao impetrante devem ser fornecidos. Não valerá, na hipótese do *Habeas Data*, a alegação de sigilo em nome da segurança do Estado. Tal restrição está expressamente prevista no caso do artigo 5º, inciso XXXIII, por meio do qual se autoriza a certificação de informações, ressalvando-se "aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado". No preceito referente ao *Habeas Data* não se verifica essa restrição. Não há como, em matéria de direito individual, utilizar-se de interpretação restritiva. Ela há de ser, nessa matéria, ampliativa (p. 212).

Lembramos, ainda, que a Constituição Federal já tem regulado a respeito de informações obtidas de órgãos públicos, em seu artigo 5º, inciso XXXIII. Segundo determina a Lei 9.507/1997, que regula o direito de acesso a informações e disciplina o rito processual do *Habeas Data*, as informações cadastrais de fontes públicas são consideradas de caráter público. Como exemplo, informações extraídas de serviços notarias e de registro públicos.

Alguns julgados, por exemplo, têm sido consolidados no entendimento da relatividade do direito à informação, a saber: conforme julgado do STJ (2021), "(...) a liberdade de informação e manifestação do pensamento não constituem direitos absolutos (...) o direito à informação não elimina as garantias individuais, porém encontra nelas os seus limites, devendo atentar ao dever de veracidade. Tal dever, ao qual estão vinculados os órgãos de imprensa não deve consubstanciar-se dogma absoluto." (*grifos nossos*).

Em Julgado do TRT da 3ª Região: "(...) Além disso, os dados contidos no *Facebook* estão disponíveis na rede mundial de computadores, não havendo falar em violação à intimidade e à vida privada." (TRT, 2021) (*grifos nossos*).

Antes da criação da Lei Geral de Proteção de Dados, o país dispunha de leis esparsas para o tema de acesso a dados e informações; por exemplo, a Lei 12.965/2014 (Marco Civil da Internet); Lei 8.078/1990 (Código de Defesa do Consumidor); Lei 12.527/2011 (Acesso à Informação); dentre outras. Essas leis, no entanto, não têm o cunho geral como a LGPD apresenta, além de possuírem certos conflitos em determinados temas.

Por isso da importância da criação de uma lei geral que envolvesse todos os setores e atingisse, de forma mais ampla, o tratamento de dados. Então, para a criação de uma lei geral foi promovida, pelo Ministério da Justiça, em 2010, a primeira consulta pública sobre o tema. Após dois anos o Plenário da Câmara dos Deputados aprovou Projeto de Lei 4.060/12, do deputado Milton Monti (PR-SP), que regulamentava o tratamento de dados pessoais no Brasil, tanto pelo poder público quanto pela iniciativa privada, e a matéria foi enviada ao Senado. Em 2013 ocorreu a apresentação pelo senador Antônio Carlos Valadares do Projeto de Lei PLS 330/2013. Em 2016 resultou outro Projeto de Lei, 5.276/2016, de autoria do Poder Executivo, que foi apensado ao PL 4.060/12. Ocorre que ambos os projetos foram substituídos pelo Projeto de Lei da Câmara, PLC 53/2018. Este, em julho de 2018, foi aprovado pelo presidente Michel Temer, passando a ser a Lei 13.709/2018 (ABEMD, 2021).

Alguns artigos desta Lei haviam sido vetados no que diz respeito à criação da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade por vício na forma, uma vez que o seu Projeto de Lei, PL 53/2018, fora de autoria da Câmara, incorrendo na sua inconstitucionalidade, afrontando o artigo 61, parágrafo 1º, inciso II, letra "e", que dispõe que é de iniciativa do Presidente da República leis que disponham de criação e extinção de Ministérios e órgãos da administração pública. Desta feita, para sanar esse vício foi editada a Medida Provisória, MP 869/2018 para criar a figura da

Autoridade Nacional e do Conselho e outras providências. Essa Medida Provisória também alterou o prazo de vigência da LGPD para 24 meses da promulgação da lei, com exceção para a vigência dos artigos pertinentes à ANPD e ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, que entraram em vigor em 28 de dezembro de 2018, inclusive alterou alguns artigos da LGPD. Em julho de 2019 a referida MP 869/19 foi convertida em Lei 13.853/2019, alterando a Lei 13.709/2018 e assim, criando, de fato, a ANPD.

A LGPD dispõe sobre o tratamento de dados pessoais, em meios digitais ou não, por pessoas naturais ou pessoas jurídicas de direito privado ou público. Tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre-desenvolvimento da personalidade da pessoa natural, atingindo, inclusive, o âmbito internacional (extraterritorialidade). Esta lei também dispõe sobre a alteração da Lei 12.965/2014, conhecida como Marco Civil da Internet (MCI), em seu inciso X do artigo 7º, incluindo esta lei de proteção de dados para o regulamento de guarda obrigatório de registro, além do previsto no próprio MCI, e em seu inciso II do artigo 16 para constar a vedação da guarda de dados pessoais excessivos à finalidade, exceto as hipóteses previstas na lei de proteção de dados.

O Marco Civil da Internet (MCI), Lei 12.965/2014, é uma lei que visa a estabelecer princípios, garantias, direitos e deveres para o uso da *internet* no Brasil. Desde 2010 tem-se feito debates públicos a respeito do uso da *internet*. Como pontua o CGI.br, "a iniciativa e a proposição do Marco Civil da Internet, desde sua origem foi motivado por princípios estabelecidos pelo CGI.br." (CGI, 2021). O MCI disciplina o uso da *internet*, a neutralidade da rede, a proteção de registros, dados pessoais e comunicações privadas e das responsabilidades gerados pelos conteúdos de terceiros. Também determina o fornecimento de dados mediante consentimento e trata da privacidade, mas no âmbito da *internet*. A MCI, porém, ainda tem algumas lacunas em determinadas matérias, e, por isso, a importância da criação da LGPD para regulá-las.

Em linhas gerais, a LGPD, sancionada em 14 de agosto de 2018, tem o condão de garantir o direito à privacidade e à proteção de dados das pessoas naturais; destaca a observância da boa-fé e que o tratamento deve conter regras claras, buscando, também, promover o desenvolvimento econômico e tecnológico, a segurança jurídica e fortalecer a defesa do consumidor. Por ser uma lei geral, afeta não somente as empresas do setor de tecnologia, mas qualquer empresa de qualquer setor ou indústria que realize operação de tratamento de dados, inclusive nos meios digitais.

Quanto aos direitos fundamentais, privacidade e o livre-desenvolvimento da personalidade da pessoa natural, objetivados na LGPD, temos a observar na Constituição Federal, em seu Título II, os Direitos e Garantias Fundamentais, notadamente em seu artigo 5º, caput e inciso X do mesmo artigo. O que diz a respeito à privacidade e personalidade da pessoa natural também observamos em algumas leis de nosso ordenamento jurídico, no Código Civil, artigo 21, artigo 2º, artigo 11, artigo 12; no Código de Defesa do Consumidor, incisos I e II do artigo 6º; no Decreto n. 7.963/2013, inciso VII do artigo 2º, inciso IV do artigo 6º; no Marco Civil da Internet, inciso II do artigo 2º, incisos I, II e III do artigo 3º, inciso I do artigo 7º. Neste sentido, Patrícia Peck Pinheiro (2018) entende:

> O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócio da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização (p. 17).

Atualmente todos os serviços e produtos que adquirimos giram em torno de dados, seja na divulgação de dados na *Internet*, em aplicativos e redes sociais, seja na utilização de análise de dados massificados ("Big Data") pelas empresas, dentre outros meios. As discussões mundiais a respeito de direitos fundamentais dos cidadãos, da privacidade e da liberdade na divulgação destes dados, levaram à criação de leis gerais que pudessem regular a sua proteção. A exemplo, a GDPR, Lei Federal Mexicana de Proteção de Dados, Lei de Dados Pessoais da Argentina, a própria LGPD, dentre outras, em vários países.

A LGPD tem fundamentos pautados na proteção dos direitos fundamentais contemplados no artigo 2º, devendo o tratamento de dados observar a boa-fé e os princípios de finalidade, adequação, necessidade, dentre outros estipulados no artigo 6º. Sua aplicação também possui caráter extraterritorial. No caso, o tratamento de dados é realizado por pessoa natural ou por pessoa jurídica de direito público ou privado no

país de sua sede ou do país onde estejam localizados os dados, desde que esta operação de tratamento ou de coleta seja realizada no território nacional, ou que bens ou serviços tenham sido ofertados no território nacional.

A aplicação da LGPD, no entanto, tem exceções. Ela não será aplicada ao tratamento de dados nos casos, como exemplo, de uso pessoal para fins particulares e não econômicos, para fins jornalísticos, artísticos ou acadêmicos, segurança pública, defesa nacional, dentre outros casos elencados no artigo 4º. Patrícia Peck Pinheiro (2018) ensina que "(...) a necessidade do consentimento na coleta dos dados, principalmente no ambiente virtual, foi ganhando importância em razão da sensibilidade e vulnerabilidade que as informações pessoais foram adquirindo com o desenvolvimento da tecnologia" (p. 65). A Lei traz alguns conceitos, em seu artigo 5º, como dado pessoal, dados sensíveis, dados anonimizados, distinção de titular, de operador, controlador e encarregado e, principalmente, conceito de consentimento, que precisa ser livre, informado e inequívoco e deve ser para finalidade determinada, que é ponto importante para entender como este deve ser formalizado.

O conceito de dados pessoais é bem amplo, pois é relacionado a uma pessoa identificada ou identificável, ou seja, que permita a identificação da pessoa isoladamente ou em conjunto com outro dado, utilizando meios razoáveis, como endereço de *e-mail,* endereço de IP, e combinado com outros dados que possam identificar a pessoa. Este conceito é abrangente, pois foi pensado não somente para abarcar a informação identificável atualmente, mas a informação que possa ser identificável como a tecnologia do futuro. Já os dados considerados sensíveis, ou seja, aqueles que possam sujeitar o indivíduo às práticas discriminatórias, por exemplo a origem racial, os dados genéticos, os dados biométricos e as convicções religiosas, devem ser tratados de forma diferenciada, com maior segurança e com o consentimento específico do titular. Deve-se observar, no entanto, as hipóteses para o tratamento de dados sensíveis, elencadas no artigo 11, como o tratamento mediante o consentimento expresso do titular, no cumprimento de obrigação legal (sem o consentimento), e demais casos descritos no referido artigo. Quanto aos dados anonimizados, são aqueles relativos a um titular que não pode ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Observa-se que se os dados anonimizados puderem ser revertidos, por meios próprios ou esforços razoáveis (fatores objetivos), estes serão considerados dados pessoais. Ainda, o tratamento de dados somente poderá ser realizado se garantida, sempre que possível, a anonimização dos dados pessoais (os quais não precisam de consentimento, conforme artigo 7º, IV). Ou seja, a anonimização é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a impossibilidade de associação, direta ou indireta, a um indivíduo. Deve-se atentar-se, também, ao conceito de pseudonimização, que é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Outro aspecto importante nesta lei é o legítimo interesse, que é uma novidade em nosso sistema jurídico. A lei não conceitua o legítimo interesse e este deve ser objeto de regulamentação específica pela autoridade competente. A lei traz este requisito de forma generalista, ou seja, para finalidades legítimas, consideradas a partir de situações concretas e observados os segredos comercial e industrial, mas entendemos que este pode ser utilizado pela empresa para, por exemplo, justificar oferta de novos produtos e serviços personalizados ou para atender uma finalidade específica, sem a necessidade de consentimento do titular do dado, bastando o responsável confirmar a existência do tratamento do dado.

Conforme dispõe o artigo 10º em seus parágrafos, o controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas a partir de situações concretas, respeitando as legítimas expectativas do titular, seus direitos e liberdades fundamentais, e, ainda, quando dados pessoais forem estritamente necessários para a finalidade pretendida, devendo adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse, posto que, neste caso, a autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, observando, sempre, os segredos comercial e industrial. O término do tratamento de dados pessoais ocorrerá quando a finalidade for alcançada, no fim do período de tratamento, da revogação do consentimento e dentre outras hipóteses elencadas nos artigos 15 e 16 da Lei. Assim, descreve Patrícia Peck Pinheiro (2018):

> Claramente, a intenção das instituições é preservar a manutenção da base de dados pessoais, evitando as hipóteses de eliminação sempre que possível, visto que há um alto valor na preservação da informação. O descarte pode e deve ocorrer, já que é um direito, mas será observado se recairá alguma previsão de justificativa legal de retenção que permita a manutenção do dado por um prazo até a sua eliminação definitiva (se esta vier a ocorrer). Grande parte do trabalho recairá sobre a análise da possibilidade de apagamento ou retenção. O direito ao apagamento (direito ao esquecimento) e ao direito à portabilidade de dados pessoais são os dois direitos de maior impacto sobre as operações nas organizações. E, devido à necessidade de continuar com a informação, surge a oportunidade da aplicação da anonimização como último recurso viável (p. 77-78).

O nível de proteção de dados deverá ser avaliado por autoridade competente, assim como a definição de conteúdo de cláusulas-padrão contratuais, verificação de normas globais, certificados e aprovações de normas corporativas globais. As transferências internacionais deverão ocorrer apenas para aqueles que proporcionarem grau de proteção de dados pessoais adequado ao previsto na lei ou quando o controlador oferecer e comprovar a conformidade.

A Lei define como agentes de tratamento o controlador e o operador, sendo o controlador pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões; e o operador, pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento em nome do controlador. Eles deverão manter o registro das operações, especialmente quando baseado no legítimo interesse. O controlador deverá elaborar relatório de impacto que é documentação do controlador, que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. Além disso, deverá comunicar à autoridade nacional e ao titular do dado a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, inclusive para os casos em que envolver dados sensíveis.

A responsabilidade dos agentes de tratamento, o controlador e o operador, é solidária quando descumprir as obrigações da legislação de proteção de dados, quando o tratamento decorrer em danos ao titular dos dados, ao deixar de adotar as medidas de segurança ou quando o operador não tiver seguido as instruções lícitas do controlador, hipótese em que o operador se equipara ao controlador. Há, no entanto, casos de exclusão de responsabilidade dos agentes, elencados no artigo 43, mediante prova.

A Medida Provisória, MP 869/2018, publicada em 28 de dezembro de 2018, criou a ANPD e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, bem como alterou o prazo de vigência da LGPD, inclusive alterando alguns artigos e a sua vigência para 24 meses da promulgação desta, com exceção para a vigência dos artigos pertinentes à ANPD e ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, que entraram em vigor em 28 de dezembro de 2018. Em julho de 2019 a referida MP 869/19 foi convertida em Lei 13.853/2019, alterando a Lei 13.709/2018 e, assim, criando, de fato, a ANPD.

A Autoridade Nacional é órgão da administração pública federal, integrada à Presidência da República, cuja natureza jurídica é transitória e será reavaliada após 2 anos da data da entrada em vigor de sua estrutura regimental, podendo ser transformada em administração pública federal indireta vinculada à Presidência da República. Os cargos e funções estarão condicionados à autorização física e financeira da Lei de Orçamentos Anual e da Lei de Diretrizes Orçamentárias. Este órgão terá autonomia técnica e decisória e será responsável, em linhas gerais, por zelar, criar mecanismos e fiscalizar o cumprimento da LGPD, editar normas, orientações, procedimentos simplificados e regulamentos sobre proteção de dados, aplicar sanções quando do descumprimento desta legislação, arrecadar receitas, além de difundir na sociedade o conhecimento sobre as normas e as políticas públicas de proteção de dados pessoais e sobre as medidas de segurança; elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; dentre outras atividades.

O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, por sua vez, irá propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade; elaborar relatórios anuais de avaliação da referida política; disseminar o conhecimento sobre o tema e sugerir ações a serem realizadas pela ANPD, dentre outros.

Observa-se que, de acordo com o artigo 52, parágrafo 3º, a Autoridade Nacional não será penalizada monetariamente, mas cabe outras sanções, como improbidade administrativa, descrita no artigo 55-F e seu parágrafo primeiro.

Levantamos um ponto importante quanto à independência da Autoridade Nacional, que tem sido de grande discussão quando da promulgação da MP869/2018 e ratificada na Lei 13.853/2019. Tem gerado grande preocupação para alguns especialistas no que se refere ao atendimento da GDPR, pois esta demanda que os modelos estrangeiros de autoridades para a proteção de dados ajam com total independência no exercício de seus poderes e, atualmente, a ANPD não é órgão independente, uma vez que a Autoridade Nacional é órgão da administração pública federal, integrante da Presidência da República. Haverá a revisão desta natureza jurídica, mas somente após dois anos da data da entrada em vigor de sua estrutura regimental. Uma autoridade independente é requisito essencial para viabilizar a inserção do Brasil às exigências de mercado internacional

3 O TRATAMENTO DE DADOS PESSOAIS

O artigo 7º traz as hipóteses legais para o tratamento de dados pessoais. A primeira hipótese sempre será o consentimento, que é a hipótese legal básica. Nos demais casos elencados nos incisos do referido artigo, o consentimento não será necessário, bastando o tratamento de dados se enquadrar em um dos requisitos descritos. As hipóteses legais são: mediante consentimento; no cumprimento de obrigação legal; pela administração pública; para realização de estudos por órgão de pesquisa; para execução de contrato; exercício regular de direito em processos judiciais, administrativos ou arbitral; para a proteção da vida; para a tutela da saúde; e, quando necessário, atender interesse legítimo e para proteção de crédito.

O consentimento deve ser manifestado de forma livre, informada e inequívoca, por escrito ou por outro meio que demonstre a manifestação de vontade do titular. Não deve haver, portanto, vício no consentimento. Não pode ser autorização genérica, sob pena de nulidade. É nulo, também, caso o consentimento tenha sido fornecido de forma abusiva, não apresentada de forma clara, inequívoca ou transparente. Ainda, o consentimento poderá ser revogado a qualquer tempo. Neste caso, ficam ratificados os tratamentos realizados em consentimento anterior. Observe-se que a Lei não descreve de forma “expressa” como definido no MCI (artigo 7º, VII). Como já informamos, deve haver consentimento específico no tratamento de dados de crianças e adolescentes, transferência internacional de dados e para dados sensíveis.

A aplicação da base legal, notadamente o legítimo interesse, deve estar de acordo com a legítima expectativa do titular, verificando-se se sua aplicabilidade é estritamente necessária para a finalidade e se o fluxo de informação é íntegro e apropriado, estabelecendo políticas e salvaguardas adequadas de transparência e privacidade. O tratamento de dados pessoais de crianças e adolescentes deverá ser realizado com o consentimento específico e em destaque dado por, pelo menos, um dos pais ou responsável legal, salvo quando necessário para contatar os pais ou responsável legal destes.

Deve-se quantificar e classificar os dados em um mapeamento de dados previamente obtidos, separando e delimitando o nível de tratamento, o sigilo, sua criticidade, daqueles que não são pertinentes à finalidade da obtenção do dado, posto que, neste caso, esses devem ser eliminados da base de dados, com identificação correta do indivíduo e dados personalizados, devendo haver especial cuidado no tratamento de dados sensíveis e observar-se os requisitos para se utilizar a base legal de legítimo interesse.

É preciso levar em consideração as políticas internas no tratamento desses dados, utilizar apropriadas tecnologias para tratamento e armazenamento, atender às necessidades da empresa e do indivíduo sem infringir os direitos, legislação e regulamentos, reconhecer a importância da privacidade e do direito à informação, evitando abusos e obedecendo os limites, sem gerar danos ao indivíduo, e ponderar liberdade à informação e privacidade.

É necessário, também, considerar a devida e efetiva capacidade tecnológica para a proteção dos dados a fim de evitar *cyberattacks*, incidentes de vazamento de dados pelos seus funcionários, *malwares*, suspensão temporária de acesso, integridade e confidencialidade das informações. Com base na análise do risco e do dano gerado, deve-se formalizar um relatório de incidente com todo o fluxo do tratamento dos dados,

notificando o responsável pela proteção de dados (no caso o ANPD) e providenciar a devida correção. Neste sentido, Bruno Bioni (2019) destaca:

> Devem-se esgotar os elementos contextuais da relação sob análise, verificando-se, dentre outros aspectos: (i) quais são os propósitos do tratamento dos dados pessoais, levando-se em consideração o contexto da relação subjacente ao fluxo informacional: (ii) como terceiros poder estar inseridos no fluxo informacional e sob quais condições; (iii) quais são as implicações no tratamento dos dados pessoais sobre seu titular; (iv) no que diz respeito ao desenvolvimento da sua personalidade; e (v) para que ele se relacione livremente em outras e nas diversas esferas sociais. deve-se reunir, pois, todo um conjunto de informações necessárias para verificar a integridade do fluxo informacional, observando-se o valor social da privacidade informacional e negociabilidade limitada dos direitos da personalidade (p. 238).

Será necessário avaliar o grau e a qualidade de todo o processo do tratamento de dados, identificar os atores envolvidos no fluxo, parametrizar esse fluxo, qualificar esses dados de acordo com sua criticidade e finalidade, verificar quais informações devem ser mantidas, com quem são compartilhadas, qual o dever legal de retenção de dados, quais dados deverão ter consentimento de acordo com a base legal na norma. Enfim, prover tratamento adequado previsto na LGPD.

4 REVISÃO DE POLÍTICAS E PROCESSOS INTERNOS

Um processo de gestão do Programa de *Compliance* bem maduro deve conter um inventário de políticas e procedimentos com o intuito de classificar os riscos de acordo com sua natureza, alinhados aos objetivos do processo e das estratégias da organização, assim como considerar o nível de segurança e os processos internos. Esse gerenciamento é feito por meio de uma matriz de *compliance*, sendo de grande importância incluir um monitoramento às mudanças regulatórias pertinentes, bem como incluir uma lista de responsáveis pelos documentos e pelos prazos de atendimento e de revisão da documentação. Segundo Marco Assi (2018), um gestor de *Compliance,* para melhor *performance* na gestão do Programa deve-se familiarizar com as ferramentas que normalmente são utilizadas em *compliance,* por exemplo ISO 27001, ISO 37001, dos modelos de gestão Cobit, Itil, Coso, assim como fazer parceria com empresas especialistas para reforçar a utilização dessas ferramentas, alinhando-as aos negócios da organização (ASSI, 2018, p. 17).

As múltiplas funções de conformidade exigem uma operação integrada de conscientização e de responsabilidade de cada área, seus funcionários, colaboradores e gestores. Marcos Assi (2018) considera o modelo de "Três Linhas de Defesa" uma forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos e controle por meio do esclarecimento dos papéis e responsabilidades essenciais. Com efeito, Marcos Assi (2018) ainda ressalta:

> Segundo o modelo das três linhas de defesa, apresentado pelo *The Institute of Internal Auditors* (IIA), o controle da gerência é a primeira linha de defesa no gerenciamento de riscos. As diversas funções de controle de riscos e a supervisão de conformidade estabelecidas pela gerência são a segunda linha de defesa. A avaliação independente é a terceira. Cada uma dessas três "linhas" representa um papel distinto dentro da estrutura mais ampla de governança da organização (p. 32).

Na revisão de políticas e nos processos internos, Assi (2018) ainda sugere que um Programa de *Compliance* deve-se considerar:

> A validação da qualidade e da velocidade das interpretações regulatórias distribuídas e estudadas por todos os envolvidos na organização, por políticas internas e procedimentos de *compliance* mais efetivos e que demonstrem a realidade dos negócios e dos seus processos relacionados; buscar sempre o aprimoramento do relacionamento da empresa com órgãos reguladores e exercer a cobrança no retorno das revisões dos supervisores e fiscalizadores; identificar possíveis falhas no atendimento e nos canais de relacionamento com os clientes, além de avaliar as falhas, proporcionar treinamentos para capacitação de todos e melhorias profissionais ou pessoais dos colaboradores; dar suporte às decisões de negócio para que estejam sempre em conformidade, buscando a sinergia com os principais gestores da empresa, para entender todas as necessidades; a cada lançamento de novos produtos, proporcionar maior velocidade e segurança para que estejam de acordo com o mercado e para que possamos avaliar suas fraquezas e vulnerabilidades; proporcionar uma cultura de disseminação de eleva-

> dos padrões éticos e culturais de C*ompliance* pela organização, cobrando todos sobre os exemplos de comportamento e postura dentro dos padrões exigidos; e estar presente e fazer o acompanhamento das correções e deficiências de não conformidades apresentadas por auditorias ou fiscalizações e realmente cobrar todos que realizem as melhorias e aprimorem a forma de cumprimento das regras. (ASSI, 2018, p. 29-30).

A seguir, a *Legal Ethics Compliance (LEC)* define os principais passos para a efetivação de um Programa de *Compliance*:

- Análise de riscos: essa etapa consiste na avaliação de todos os problemas de conduta que a empresa pode estar sujeita de acordo com a sua área de atuação.
- Plano de ação: trata-se de planejar uma estratégia para a implementação de um Programa de *Compliance*. Nele deve ser descrita cada etapa, como será realizada, além de pontos como a divulgação, a capacitação dos colaboradores e o monitoramento.
- Código de conduta: documento precisa ser claro, objetivo e pertinente à realidade da empresa. Por mais bonito que o texto possa parecer, ele precisa ter um significado alinhado aos valores e às necessidades da organização.
- Canais de comunicação: não basta criar um código, ele tem que ser colocado em prática. Para isso, devem ser criados e divulgados canais de denúncias e análise de situações. Esses canais precisam ser abertos tanto para o público interno (colaboradores) quanto para o externo (clientes e fornecedores). Essencial que todos tomem conhecimento sobre as diretrizes e ter o apoio da alta administração.
- Capacitação de colaboradores: todos os funcionários devem estar conscientes das responsabilidades de seus atos. Mas acima de tudo, eles devem de fato aderir ao Programa de *Compliance*. Para isso, podem ser feitos treinamentos periódicos, campanhas de conscientização e de comunicação interna.
- Monitoramento do funcionamento do Programa: monitorar o funcionamento de cada um dos pilares do Programa de *Compliance*. Não basta colocá-los em pé, é preciso acompanhar a operação e testar cada um dos componentes do programa, constantemente, para ter certeza sobre sua efetividade.
- Avaliação e correção de problemas: as soluções não devem considerar apenas os casos isolados, mas sim o contexto que possibilitou tais ocorrências. Ou seja, um Programa de *Compliance* não se trata de um simples paliativo. Tem como principal objetivo propor mudanças permanentes na conduta dos membros da empresa (LEC, 2021).

O modelo apresenta um novo ponto de vista sobre as operações, ajudando a garantir o sucesso contínuo das iniciativas de gerenciamento de riscos, e é aplicável a qualquer organização – não importando seu tamanho ou complexidade. Mesmo em empresas em que não haja uma estrutura ou sistema formal de gerenciamento de riscos, o modelo de Três Linhas de Defesa pode melhorar a clareza dos riscos e controles e ajudar a aumentar a eficácia dos sistemas de gerenciamento de riscos (ASSI, 2018, p. 58).

5 GOVERNANÇA, BOAS PRÁTICAS E SANÇÕES

Governança Corporativa é uma estrutura com um conjunto de processos, políticas e regulamentos internos que permite que a organização regule a maneira como ela é administrada e controlada. Governança lida com conflitos. A Governança Corporativa decorre da globalização, do crescimento das empresas e da regulamentação do funcionamento das mesmas (como normas de agências reguladoras: Anatel, CVM, etc.). Um dos pilares da Governança Corporativa é o "conflito agência", ou seja, o conflito de interesses entre a propriedade difundida e a divergência entre os dirigentes da empresa.

Por isso, a Governança Corporativa visa a estabelecer critérios e estruturar diretrizes para a tomada de decisão, otimizar o desempenho para proteger os interesses e buscar informação técnica do caso, usando as habilidades e experiências pertinentes de cada área, sempre alinhados com o interesse empresarial. É importante, também, que a empresa crie uma cultura de riscos ("apetite a risco") para que estruture um gerenciamento efetivo de riscos operacionais e estratégicos, não somente para identificá-los e administrá-los, mas para otimização de capital, fornecer maior proteção aos acionistas e atrair investimentos. Desde a *Lei Sarbanes-Oxley* (2002), que tem por objetivo criar mecanismos de auditoria e de segurança para mitigar

riscos aos negócios empresariais, estimulou as empresas a divulgar mais sobre sua abordagem de governança corporativa.[1] Ribeiro Neto e Famá (2021) definem a importância dos papéis da alta administração:

> A importância da Governança Corporativa não se concentra apenas em disciplinar as relações entre as diversas áreas de uma organização ou com partes externas. O conselho de administração deve ser órgão máximo da empresa, responsável pela definição dos objetivos e estratégias que serão implementadas pela administração executiva. O conselho deve ser independente, isto é, a maioria de seus membros deve ser externa à organização. Cabe ao conselho também o papel de fiscal da gestão. Além de ressaltar a importância do conselho de administração na gestão, os princípios de governança também versam sobre as atribuições da diretoria executiva, da auditoria externa e princípios de ética, entre outros. Assim, a implementação das boas práticas de Governança Corporativa possibilita uma gestão mais profissionalizada e transparente, diminuindo a assimetria informacional, procurando convergir os interesses de todas as partes relacionadas, buscando maximizar a criação de valor na empresa (2021).

A ferramenta normalmente utilizada para direcionar a efetivação da Governança Corporativa é o Coso (*Committee of Sponsoring Organization of the Treadway Comission*), *framework* integrado para ajudar empresas a avaliar e aperfeiçoar seus sistemas e controles internos. O modelo de controles internos do Coso tem uma seção devotada aos objetivos de controle para o Conselho de Administração, que tem como objetivo fornecer diretrizes no estabelecimento de uma efetiva prática de governança para o Conselho. Há uma outra ferramenta que orienta processos de governança e gestão de TI chamada Cobit (*Control Objectives for Information and Related Technology*). Seu foco principal é a governança de TI, mas pode ser utilizada em Governança Corporativa, pois tem como principal objetivo gerar valor para a empresa e seus processos.

Com referência a Boas Práticas e Governança na LGPD, destaca-se, em seus artigos 50 e 51, que os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular. O controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá criar programa de governança em privacidade contendo os requisitos mínimos, conforme descritos nas alíneas do inciso I do parágrafo 2º, artigo 50. É importante lembrar, também, que a nova lei das Estatais, Lei nº 13.303/2016, dispõe sobre exigências às regras de governança corporativa, prática de gestão de risco e de controle interno no estatuto das empresas pública e de economia mista. Ainda, estipula que o estatuto social destas deverá prever a possibilidade da área de *compliance* se reportar diretamente ao Conselho de Administração em situações em que se suspeite do envolvimento do diretor-presidente em irregularidades ou quando este se furtar à obrigação de adotar medidas necessárias em relação à situação a ele relatada.

[1] O Instituto Brasileiro de Governança Corporativa (IBGC) define os seguintes princípios básicos como boas práticas de Governança: Transparência – consiste no desejo de disponibilizar para as partes interessadas as informações que sejam de seu interesse e não apenas aquelas impostas por disposições de leis ou regulamentos. Não deve se restringir ao desempenho econômico-financeiro, contemplando também os demais fatores (inclusive intangíveis) que norteiam a ação gerencial e que condizem à preservação e à otimização do valor da organização. Equidade – caracteriza-se pelo tratamento justo e isonômico de todos os sócios e demais partes interessadas (*stakeholders*), levando em consideração seus direitos, deveres, necessidades, interesses e expectativas. Prestação de Contas (*accountability*) – os agentes de governança devem prestar contas de sua atuação de modo claro, conciso, compreensível e tempestivo, assumindo integralmente as consequências de seus atos e omissões e atuando com diligência e responsabilidade no âmbito dos seus papéis. Responsabilidade Corporativa – os agentes de governança devem zelar pela viabilidade econômico-financeira das organizações, reduzir as externalidades negativas de seus negócios e suas operações e aumentar as positivas, levando em consideração, no seu modelo de negócios, os diversos capitais (financeiro, manufaturado, intelectual, humano, social, ambiental, reputacional, etc.) no curto, médio e longo prazos.

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. A preocupação da Governança Corporativa é, portanto, criar um conjunto eficiente de mecanismos, tanto de incentivos quanto de monitoramento, a fim de assegurar que o comportamento dos administradores esteja sempre alinhado com o melhor interesse da empresa (IBGC, 2021).

6 DAS PENALIDADES

A LGPD prevê, em seu Capítulo VIII, sanções administrativas a serem aplicadas de acordo com cada caso concreto pela autoridade competente, assegurados ampla defesa, contraditório e direito de recurso. As sanções englobam advertência, multa diária ou multa simples de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, limitada, no total, a R$ 50.000.000,00 por infração; além da publicização da infração, do bloqueio dos dados pessoais, suspensão e proibição do exercício de atividade de tratamento de dados e até aplicação de sanções da Lei 8.078/1990 (CDC). O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos. Observa-se que os vazamentos individuais ou os acessos não autorizados conforme a LGPD, poderão ser objeto de conciliação direta entre controlador e titular; no entanto, caso não haja acordo, o controlador estará sujeito à aplicação das devidas penalidades.

Nesta linha de pensamento, entendemos que o gestor empresarial deve utilizar uma robusta Governança Corporativa e ética empresarial em seus negócios não somente para cumprir com o previsto na referida legislação, mas também para empreender rentabilidade, competitividade, crescimento e sustentabilidade.

7 CONSIDERAÇÕES FINAIS

Destaca-se que a LGPD protege dois tipos de informação: os dados pessoais e os dados sensíveis. A lei exige que o tratamento desses dados seja feito com transparência, qualidade e segurança, que normalmente poderá ser por meio de políticas de privacidade ou de termos de uso, e devem estes serem aceitos expressamente pelo titular.

Hoje, os termos de uso disponibilizados no meio digital são longos, cansativos e complexos. São feitos para não serem lidos. O usuário apenas aceita, sem lê-los e não sabe como serão tratados esses dados e qual o uso que será feito deles. O maior desafio é garantir o tratamento adequado e a segurança no uso e armazenamento dos dados, e que não sejam acessados por pessoas não autorizadas, principalmente os dados sensíveis. Daí a preocupação com a privacidade e controles eficazes para a segurança da informação. Deve-se, também, considerar fazer uma análise de risco, justificar a finalidade do legítimo interesse em coletar e armazenar determinadas informações. Para isso, será necessária adaptação pelas empresas de seus termos de uso e de suas políticas de privacidade. Em razão das infrações cometidas às normas previstas na LGPD, são a responsabilização por danos e sanções administrativas aplicáveis pela autoridade nacional.

Lembra-se que a LGPD é importante para o Brasil poder se adequar às exigências previstas na GDPR, pois uma das exigências do GDPR é que outro país esteja apto às suas regras, principalmente se envolver dados europeus.

Neste sentido, perguntamos se com a nova legislação de proteção de dados os Programas de *Compliance* das empresas nacionais conseguirão atender às exigências desta lei de forma segura e eficaz. As normas corporativas, adequadas para um certo momento, podem se tornar obsoletas e devem ser mudadas. O *Compliance* nasce num ambiente de regulação, e para um Programa de *Compliance* efetivo é imprescindível o envolvimento da alta direção e a devida utilização de mecanismos tecnológicos de proteção de dados. Ainda, é importante a cooperação das empresas com os organismos internacionais para o cumprimento da legislação externa no tratamento extraterritorial de dados.

As empresas deverão procurar mais transparência no tratamento, pois a pessoa natural, titular dos dados, terá maior controle sobre suas informações pessoais (revogação, correção, exclusão, etc.) e deverá atentar-se para as penalidades aplicadas pelo descumprimento da norma. A primeira providência é conhecer o princípio constitucional do direito à privacidade, que pode conduzir o Programa de *Compliance* ao emprego mais consistente a assertivo do uso e tratamento dos dados pessoais. É preciso associar o direito à privacidade ao direito à finalidade do uso e coleta de dados e contemplar em sua estrutura como se dará a gestão e tratamento desses dados e, estando, assim, em conformidade com o exigido na lei. O Programa de *Compliance* não é somente estar em conformidade com leis, regulamentos internos e externos e políticas. É um conjunto de disciplinas, uma estrutura cíclica, um processo reiterado, para fazer cumprir todas as diretrizes estabelecidas, buscando melhorias contínuas. Deve incluir critérios e ações baseados em melhores

práticas, proceder com a formalização dos documentos corporativos (códigos de conduta e de ética, normas, políticas e procedimentos internos) com as demais áreas de empresa, procurar a rápida identificação das irregularidades e monitoramento dos riscos e proceder com a devida resposta as não conformidades com as leis e regulamentos e políticas internas (sanções, remediação e melhoria de modelos e práticas), sempre relacionando-se com o negócio corporativo para evitar danos à imagem e à reputação da empresa.

Ressaltamos que este *compliance* será reforçado com a presença da Autoridade Nacional de Proteção de Dados – ANPD –, órgão que deverá fiscalizar o cumprimento da lei pelas empresas nacionais e que poderá solucionar conflitos evitando demandas na via judicial. A ANPD também é de extrema importância para poder manter padrões estipulados na lei e, assim, garantir o atendimento dos direitos do cidadão e a segurança jurídica.

É preciso lembrar que a liderança das empresas tem papel importante para que o Programa de *Compliance* e a própria Governança Corporativa sejam efetivos, principalmente na conscientização e engajamento de seus colaboradores no direcionamento às responsabilidades éticas, legais e sociais definidos pela empresa, uma vez que os diferentes comportamentos resultam em maneira diversa pela qual o indivíduo se relaciona. Todos os colaboradores da empresa devem entender que toda norma é uma diretriz obrigatória que resulta em sanção em caso de desvio de conduta. Além disso, todos devem estar alinhados com a cultura da empresa. Algumas iniciativas podem ajudar a organização a instituir um programa efetivo, por exemplo, certificação ISO 19600 (normas técnicas de *compliance*) ou Selo Pró-Ética, que tem por objetivo construir um ambiente de integridade e de prevenção de atos contra a corrupção.

O tratamento de dados na LGPD terá grande implicação nas empresas brasileiras, pois elas deverão adaptar seus procedimentos e políticas internas às exigências da nova lei, bem como conhecer suas vulnerabilidades e redesenhar seus sistemas de segurança em detrimento destas exigências. Um Programa de *Compliance* eficaz, acompanhado de sistema seguro de proteção de dados, é a forma ideal de conciliar as exigências da lei entre as empresas nacionais e os titulares de dados, bem como no mercado.

8 REFERÊNCIAS

ABEMD. Associação Brasileira de Marketing de Dados. *Relatório proteção de dados.* Disponível em: https://abemd.org.br/interno/Relatorio-Protecao-de-Dados-231017.pdf. Acesso em: 23 mar. 2021.

ASSI, Marcos *Compliance:* como implementar. Colaboração Roberta Volpato Hanoff. São Paulo: Trevisan, 2018.

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

BRASIL. Constituição da República Federativa do Brasil de 1988. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 13 fev. 2021.

BRASIL. Decreto 8.420, de 18 de março de 2015. Regulamenta a Lei n. 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: 18 mar. 2021

BRASIL. Decreto n. 8.771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8771.htm. Acesso em: 20 jan. 2021.

BRASIL. Lei n. 6.015, de 31 de dezembro de 1973. Dispõe sobre os registros públicos, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L6015compilada.htm. Acesso em: 21 mar. 2021.

BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8078.htm. Acesso em: 13 mar. 2021.

BRASIL. Lei n. 8.935, de 18 de novembro de 1994. Regulamenta o art. 236 da Constituição Federal, dispondo sobre serviços notariais e de registro. (Lei dos cartórios). Disponível em: http://www.planalto.gov.br/CCivil_03/LEIS/L8935.htm. Acesso em: 21 mar. 2021.

BRASIL. Lei n. 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm. Acesso em: 15 fev. 2021.

BRASIL. Lei n. 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 18 mar. 2021.

BRASIL. Lei n. 12.846, de 1º 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: 18 mar. 2021.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 jan. 2021.

BRASIL. Lei n. 13.303, de 30 de junho de 2016. Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13303.htm. Acesso em: 18 mar. 2021.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018a. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 5 fev. 2021.

BRASIL. Lei n. 13.853/2019, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 27 mar. 2021.

BRASIL. Medida Provisória n. 869, de 27 de dezembro de 2018b. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 5 fev. 2021.

CGI. Comitê Gestor da Internet. *O CGI.br e o marco civil da internet*. Disponível em: https://www.cgi.br/publicacao/o-cgi-br-e-o-marco-civil-da-internet/. Acesso em: 12 mar. 2021.

DAVENPORT, Thomas H.; PRUSAK, Laurence. *Conhecimento empresarial.* Trad. Lenke Peres. Rio de Janeiro: Campus; São Paulo: Publifolha, 1999.

IBGC. Instituto Brasileiro de Governança Corporativa. *Governança corporativa:* princípios básicos. Disponível em: https://www.ibgc.org.br/governanca/governanca-corporativa/principios-basicos. Acesso em: 25 fev. 2021.

LEC. Legal Ethics Compliance. *Saiba como implementar um programa de compliance na empresa.* Disponível em: http://www.lecnews.com.br/blog/saiba-como-implementar-um-programa-de-compliance-na-empresa/. Acesso em: 26 mar. 2021.

RIBEIRO NETO, Ramon Martinez; FAMÁ, Rubens. *A importância da governança corporativa na gestão das empresas brasileiras.* Disponível em: http://www.ibgc.org.br/biblioteca/download/RIBEIRONETO,RM_sd_Importancia...mon.pdf. Acesso em: 25 mar. 2021.

PINHEIRO, Patrícia Peck. *Proteção de dados pessoais:* comentários à lei 13.709/2018 (LGPD). São Paulo: Saraiva, 2018.

STJ. Recurso Especial Nº 1.653.152. Relatora: Ministra Nancy Andrighi. DJ: 10/10/2017. *Jusbrasil.* Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/511208501/recurso-especial-resp-1653152-sp-2016-0309793-0/relatorio-e-voto-511208530?ref=juris-tabs. Acesso em: 23 mar. 2021.

STF. *Respostas a perguntas frequentes.* Disponível em: http://www.stf.jus.br/portal/cms/verTexto.asp?servico=centralDoCidadaoAcessoInformacao. Acesso em: 12 mar. 2021.

TEMER, Michel. *Elementos de direito constitucional.* 15. ed. rev. amp. São Paulo: Malheiros Editores, 1999.

TRT. Recurso Ordinário Nr. 0010599-39.2014.5.03.0053. Relator: Rogério Valle Ferreira. DJ: 26/5/2015. *Jusbrasil.* 2015. Disponível em: https://www.jusbrasil.com.br/topicos/38282431/processo-n-0010599-3920145030053-do-trt-3. Acesso em: 23 mar. 2021.