UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE DIREITO PROF. JACY DE ASSIS

CAROLINA VILELA DE SOUZA

COMPLIANCE DIGITAL: PRIVACIDADE E PROTEÇÃO DE DADOS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS E OS DESAFIOS DE IMPLEMENTAÇÃO

UBERLÂNDIA
2022

CAROLINA VILELA DE SOUZA

COMPLIANCE DIGITAL: PRIVACIDADE E PROTEÇÃO DE DADOS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS E OS DESAFIOS DE IMPLEMENTAÇÃO

Trabalho Conclusão de Curso apresentada à Graduação em Direito da Universidade Federal de Uberlândia como requisito para a obtenção do título de bacharel em Direito.

Orientador: Dr. Almir Garcia Fernandes

UBERLÂNDIA

2022

CAROLINA VILELA DE SOUZA

COMPLIANCE DIGITAL: PRIVACIDADE E PROTEÇÃO DE DADOS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS E OS DESAFIOS DE IMPLEMENTAÇÃO

Trabalho de Conclusão de Curso apresentado como exigência parcial para a obtenção do título de bacharel em Direito à Universidade Federal de Uberlândia (MG) pela banca examinadora formada por:

Aprovada em: 24 de março de 2022.

_____

Professor orientador – Dr. Almir Garcia Fernandes
Universidade Federal de Uberlândia, MG

_____

Professora examinadora Dra. Shilei Silmara de Freitas Mello
Universidade Federal de Uberlândia, MG

_____

Mestranda examinadora Sthéfane Alves Vasconcelos
Universidade Federal de Uberlândia, MG

Compliance digital: privacidade e proteção de dados à luz da Lei Geral de Proteção de Dados e os desafios de implementação

Carolina Vilela de Souza[1]
Dr. Almir Garcia Fernandes[2]

RESUMO

O presente estudo objetiva verificar se a regulamentação do tema apresentada pela Lei Geral de Proteção de Dados (LGPD) tem se mostrado suficiente para salvaguardar o direito fundamental à privacidade em tempos em que a evolução tecnológica caminha a largos passos e como as normas de *compliance* podem auxiliar as empresas a cumprir as determinações da novel legislação. Para tanto, explica o tratamento jurídico dispensado aos dados pessoais dos cidadãos no Brasil em tempos de massificação de dados; expõe os novos paradigmas que redefinem a privacidade e a proteção de dados pessoais na era da evolução tecnológica; e discute os princípios previstos no art. 6º da LGPD e sua importância para projetos de implementação de um programa da *privacy compliance.* Como metodologia foi empregada a pesquisa teórico-dogmática, tendo em vista que foi realizada uma revisão de literatura em doutrinas e legislações com o intuito de responder ao problema de pesquisa delineado permitindo concluir que não existem soluções preterminadas para que a *accountability* seja devidamente tratada pelas organizações, mas, certamente, a boa inter-relação entre *accountability*, alinhamento e adaptabilidade é um fator que poderá representar o sucesso ou o fracasso de um programa de *privacy compliance*.

Palavras-chave: Privacidade. Proteção de Dados. Lei Geral de Proteção de Dados. Compliance digital.

---

[1] Graduanda em Direito pela Universidade Federal de Uberlândia.

[2] Doutor em Direito Comercial pela Pontifícia Universidade Católica de São Paulo, PUC-SP, Mestre em Direito pela Universidade de Franca, Especialista em Direito Processual Civil pela Universidade Federal de Uberlândia, graduado em Direito pela Universidade Federal de Uberlândia. Professor da Faculdade de Direito da Universidade Federal de Uberlândia

ABSTRACT

The present study aims to verify whether the regulation of the subject presented by the General Data Protection Law (call of LGPD in brazilian translate) has been sufficient to safeguard the fundamental right to privacy in times when technological evolution is taking large steps and also to assess how compliance standards they can help companies to comply with the requirements of the new legislation. Therefore, it explains the legal treatment given to the personal data of citizens in Brazil in times of mass data; exposes the new paradigms that redefine the privacy and protection of personal data in the era of technological evolution; and discusses the principles foreseen in the art. 6 of the LGPD and its importance for projects to implement a privacy compliance program. Theoretical-dogmatic research was used as a methodology, considering that a literature review on doctrines and legislation was carried out in order to answer the outlined research problem, allowing the conclusion that there are no pre-terminated solutions for accountability to be properly addressed by organizations, but, certainly, the good interrelationship between accountability, alignment and adaptability is a factor that can represent the success or failure of a privacy compliance program.

Keywords*: Privacy. Data Protection. General Data Protection Law. Digital compliance*

SUMÁRIO

INTRODUÇÃO

O risco pode ser definido de várias maneiras, e conforme Salles Júnior et al. (2010), em geral se relaciona com a incerteza, consiste na probabilidade de ocorrência de um determinado evento e seus impactos resultantes.

A partir da década de 1990, entre todos os tipos de riscos passíveis de mapeamento, observou-se um crescimento da preocupação relativa às ameaças cibernéticas, ou seja, tudo aquilo relacionado a questões que envolvem o uso de sistemas informatizados, o que fez surgir a necessidade de uma cultura de gestão de risco na Tecnologia da Informação (TI). A partir disso, tornou-se notório o fortalecimento e aperfeiçoamento dos diversos processos de governança implementados para gerenciar melhor este risco (CABRAL; CAPRINO, 2015). E é neste sentido que começa a ser adotada, como melhor prática, a segurança da informação e consequentemente a segurança cibernética e a proteção de dados.

Ante a realidade exposta, o problema principal que norteou esta pesquisa foi a busca de respostas para o seguinte questionamento: o cumprimento de um *Compliance* Digital – de planos e políticas resguardados pela LGPD - é suficiente para preservar o direito à proteção dos dados nas relações consumeristas?

Frente ao questionamento proposto, o presente estudo objetiva verificar, com base nas doutrinas, legislação e jurisprudências se a proteção trazida pela LGPD se mostra suficiente para resguardar o direito à proteção de dados.

Com o fim de complementar a análise da proteção legislativa indicada na LGPD também se faz de suma importância apontar os novos paradigmas que redefinem a privacidade e a proteção de dados pessoais na era da evolução tecnológica; investigar o posicionamento jurisprudencial a respeito das violações à proteção de dados pessoais antes e após o advento da Lei n.13.709/2018; pesquisar se o *compliance* digital é uma alternativa eficiente na prática das tutelas legais inerentes; e apresentar possíveis alternativas e soluções ante as práticas abusivas e aos vazamentos e usos indevidos de dados, visando sustentar a análise presente neste estudo.

Não se pode negar que a rede mundial de computadores propiciou a aproximação virtual dos indivíduos, modificando a forma pela qual as pessoas (naturais e jurídicas) se relacionam. No entanto, pela perspectiva jurídica –

notadamente, quanto à proteção de dados em escala mundial – percebe-se que esta evolução tecnológica, não veio acompanhada da respectiva evolução jurídica que permita identificar e punir de forma adequada aqueles que atentam contra a honra, privacidade e dignidade de outrem.

Apesar do Brasil fazer parte da Rede Ibero-Americana de Proteção de Dados (RIPD), a legislação sobre essa proteção ainda é incipiente, bem como a cultura jurídica do país ainda está mais voltada para a discussão das políticas públicas relativas ao mínimo existencial, porque grande parte da população ainda carece de tais condições. Porém, não é de menos importância a proteção de outros direitos fundamentais, a exemplo daqueles que dizem respeito à privacidade, principalmente porque a informação tornou-se um bem de valor econômico incomensurável para determinadas instituições públicas ou privadas, uma riqueza primordial da sociedade.

Entende-se que as novas tecnologias transformaram as relações sociais e, assim como já ocorre em outras áreas da ciência, o Direito precisa examiná-las com o objetivo de assegurar o seu desenvolvimento (especialmente econômico) sem violar as garantias individuais e coletivas dos cidadãos.

Com vistas a alcançar o objetivo proposto neste artigo foi empregada a pesquisa teórico-dogmática, fundamentada em uma revisão de literatura em doutrinas e legislações com o intuito de responder ao problema apresentado com vistas a encontrar uma solução para mitigar o conflito que se formou em torno do direito à privacidade e o direito à informação.

1. Evolução legal até a normatização da lei geral de proteção de dados

Historicamente a proteção de dados tem sido tema de discussão e tentativas de normatização há algum tempo. Conforme Marcacini (2016) contextualiza, um dos objetos de razoável discussão foi o projeto de lei voltado a regular a tecnologia como meio, que resultou na Lei nº 11.419/2006 e tratou-se de norma de amplitude mais restrita, ao se considerar as múltiplas relações entre o Direito e as novas tecnologias, já que o projeto focava apenas na informatização processual.

Muitas idas e vindas precederam o arcabouço da Lei Geral de Proteção de Dados Pessoais (LGPD), Pinheiro (2021) destaca que, apesar da sua criação e história remeter ao ano de 2010, ocasião em que o Ministério da Justiça disponibilizou uma minuta de um Anteprojeto de Lei de Proteção de Dados, colocando-o em consulta pública, toda euforia relacionada surgimento da Lei Geral de Proteção de Dados Pessoais (LGPD) somente tomou destaque em 2018.

Ainda conforme a autora afirma em sua obra, a consulta pública durou quatro meses, recebeu opiniões de diversos entes da sociedade e "em 2012, com clara inspiração na consulta pública, foi protocolado o PL nº 4.060 que dispunha sobre o tratamento de dados pessoais e dava outras providências". Pinheiro conclui que o projeto, somente teve andamento em 2013 quando Edward Snowden revelou irregularidades e práticas de vigilância em escala global empreendidas pela Agência Nacional de Segurança ("NSA").

O referido escândalo acabou possibilitando uma maior celeridade na tramitação de projetos que envolviam o assunto, pelos motivos que Marcacini esclarece,

> "Tal fato acelerou o trâmite do projeto de lei, enquanto este ainda se encontrava na Câmara dos Deputados. A Presidência da República solicitou a aplicação de regime de urgência constitucional para apreciação do projeto, motivada pelas revelações trazidas à luz por Edward Snowden. Divulgou-se que a própria Presidência da República de nosso país teria sido foco de espionagens mediante interceptação de suas comunicações telefônicas e eletrônicas, e a indignação que isso causou em nossa então governante resultou na aplicação do regime de urgência ao projeto de lei sobre o Marco Civil." (MARCACINI, 2016, p.22).

Para Pinheiro (2021, p.144), o tema "proteção de dados" não teve grandes novidades em 2013, somente ganhando fôlego em 2015 quando o Ministério da Justiça disponibilizou a segunda rodada de consultas públicas sobre o anteprojeto da lei de proteção de dados, após a qual, o anteprojeto foi consolidado e então protocolado na Câmara dos Deputados, ocasião em que recebeu nº 5.276/2016, considerado mais célere, amplo e melhor redigido que o antecessor, de nº 4.060/2012.

Segundo as notícias da época, após acordos entre Câmara e Senado no que se referia a precedência e substituibilidade entre os PLs nº 5.276/2016 e nº 4.060/2012, após apensação, eles foram colocados em pauta no plenário da

Câmara e foram aprovados por unanimidade e seguindo para o Senado recebeu o nº 53/2018.

Como Pinheiro (2021, p.145-146) ainda elucida, na comissão, o texto foi aprovado e recebeu requerimento de urgência para ser incluído em pauta para votação, e no dia 10 de julho, depois de fortes pressões da sociedade civil, o projeto foi pautado e aprovado por unanimidade, sendo encaminhado para a sanção presidencial, o que ocorreu em 14 de agosto de 2018, sofrendo algumas alterações no ano de 2019 por meio da Lei 13.853[3].

O país, por fim, logrou êxito no tema, e a partir de então havia regulamentação voltada para a proteção de dados. Porém o foco da LGPD se via puramente direcionado aos direitos ligados as pessoas físicas, deixando um vazio legal no que se trata das informações coletivas ou empresariais[4]. Por meio deste histórico, foi possível compreender o processo de conquista da proteção de dados, e como algumas situações influenciaram esse processo sendo possível avançar para a exploração de algumas de suas possíveis aplicações práticas.

2. A Lei nº 13.709/2018 – Lei Geral de Proteção de Dados seus princípios e aplicações práticas

O tema da proteção dos dados pessoais se depara com novos desafios diuturnamente. Exemplificativamente, a questão do *big data*, o problema do direito ao esquecimento, o "consentimento" do cidadão em disponibilizar informações relevantes em sites de redes sociais, cujos provedores "praticamente sabem o que pensamos" (FERGUSON, 2015, p. 6).

Assim, o avanço tecnológico, além de trazer vários benefícios para a sociedade, também apresenta preocupações. A inserção de dados pessoais na rede, o posterior desejo de torná-los indisponíveis, bem como as novas formas como

[3] Em 27 de dezembro de 2018, foi editada a Medida Provisória n° 869, publicada no Diário Oficial da União no dia seguinte, que promoveu alterações no texto sancionado e criou a ANPD. A MP foi votada no ano seguinte, tendo sido convertida em lei, recebendo o número 13.853/19.

[4] Não que estes não gozem de proteção legal, no entanto são outros diplomas que serão os responsáveis por isso, tais como a lei de propriedade industrial (9.279/96), lei do software (9.609/98), lei de direitos autorais (9.610/98), entre outras.

tais informações são utilizadas, acenderam a discussão sobre o direito dos usuários terem a sua privacidade protegida, além dos seus dados pessoais.

Cada dia mais o acesso a dados pessoais contendo informações sensíveis do indivíduo não depende do acesso ao seu *smartphone* ou dispositivo pessoal, mas pode ser obtido através do consentimento de provedores considerados como "terceiros" nesta relação (no direito norte-americano conhecido por *third-party providers*), o que na prática representa um controle cada vez menor de seus dados pessoais (FERGUSON, 2015).

Com a finalidade de cobrir a ausência de controle, a LGPD foi estruturada em dez capítulos, sendo composta por sessenta e cinco artigos. Entre eles, o art. 6º da referida Lei é o responsável por listar importantes princípios[5] que devem nortear a aplicação da lei, sob a observância da boa-fé. Mais do que isso, os princípios previstos no art. 6º são de grande importância também para projetos de implementação de um programa de *privacy compliance*.

Como um dos primeiros princípios elencados no referido art. 6º, a finalidade refere-se à realização do tratamento servindo a propósitos legítimos, específicos e informados ao titular, sem que seja possível o tratamento posterior de maneira incompatível com essas finalidades[6] (SOMBRA, 2019).

Considera-se o princípio da finalidade um dos mais importantes, já que a própria lei repete a expressão por trinta vezes, ligando-a inicialmente ao consentimento ("para uma finalidade determinada"; art. 5º, XII) e também a outros princípios (adequação, necessidade por duas vezes e qualidade, incisos II, III e V todos do art. 6º).

Este é o princípio que dará claro direcionamento ao titular do que será feito com seus dados e tem grande importância prática na medida em que pretende impedir tratamentos de dados à revelia do titular (SOMBRA, 2019).

Quanto aos propósitos legítimos, trata-se de atividades permeadas pela legalidade, bons costumes e boa-fé. É o atuar no sentido diametralmente oposto de atividades ilícitas, de má-fé (CRESPO, 2019).

---

[5] Art. 6º: I – finalidade; II - adequação; III - necessidade; IV - livre acesso; V - qualidade dos dados; VI - transparência; VII - segurança; VIII - prevenção; IX - não discriminação; X - responsabilização e prestação de contas.

[6] Também mencionado nos artigos 7º, § 5º, 8º, §§ 4º e 6º, 10, 11, I, 13, 14, § 1º, 26, caput, e § 1º, 33, VIII, além de ser previsto no General Data Protection Regulation (GDPR) no considerando 39 e no art. 5º item 1(b).

Ainda, merece destaque o princípio da adequação que se refere à compatibilidade do tratamento com as finalidades informadas ao titular, conforme o contexto do tratamento (PINHEIRO, 2018).

A adequação nada mais é que a correlação das finalidades do tratamento de dados com o contexto do tratamento, evitando desvirtuação. É, assim, o vínculo lógico de pertinência entre a finalidade objetivada do modo que foi informada ao titular dos dados (SOMBRA, 2019).

Há, aqui, uma clara necessidade de observação da finalidade objetivada, o que foi transmitido ao titular dos dados e como efetivamente ocorre o tratamento dos dados.

Na sequência tem-se o princípio da necessidade, que indica a limitação do tratamento de dados pessoais ao mínimo necessário para que suas finalidades sejam realizadas, com abrangência dos dados pertinentes, não excessivos e, especialmente proporcionais em relação às finalidades do tratamento de dados. Com isso, modifica-se a lógica de mercado existente até o momento de que tudo se pode fazer com os dados coletados. Passa-se a um cenário de somente tratar dados que se mostrem indispensáveis para que o objetivo a princípio almejado seja atingido (CRESPO, 2019).

Pretende-se que, com o princípio do livre acesso permitir que o titular de dados exerça um seu direito: o de ter acesso aos dados tratados pelo controlador. E isso deve ser feito de modo facilitado, sem obstáculos ou impedimentos, para a totalidade dos dados constantes nos registros do controlador (PENNA, 2020). Está, portanto, relacionado ao artigo 9º, que indica quais são os direitos do titular de dados, como saber qual a finalidade do tratamento, a duração, dados do controlador, com quem seus dados são compartilhados, etc.

A qualidade dos dados fornece aos titulares a garantia de exatidão, clareza, relevância e atualização dos dados, consoante a necessidade e para que a finalidade de seu tratamento seja cumprida. Tal princípio impõe que os dados pessoais sejam tratados na sua melhor forma, sendo corretos, exatos, atualizados, conforme a necessidade e para que atinja a finalidade pretendida. É, assim, um aspecto essencial para o tratamento, mas que depende de outros princípios, tais como a necessidade e a finalidade, em especial (CRESPO, 2019).

Já o princípio da transparência é outra diretriz essencial num projeto de LGPD, já que fazer com que o tratamento seja claro, preciso, sem obscuridades é fundamental (PINHEIRO, 2018). Sem transparência, não se pode proceder a qualquer tipo de tratamento, exceto os resguardados pelos sigilos comercial e industrial.

A transparência é tão importante que a LGPD declara que o consentimento será nulo se as informações transmitidas ao titular forem enganosas ou abusivas (SOMBRA, 2019).

Também se exige transparência para tratamentos especialmente feitos com base no legítimo interesse (art. 10, § 2º) e quando os dados forem de crianças e adolescentes (art. 14, § 6º).

O princípio da segurança é o que impõe que os agentes de tratamento busquem sempre utilizar as medidas técnicas e administrativas disponíveis para proteger os dados pessoais de tratamentos ilícitos, sejam eles autorizados ou não, causando sua destruição, perda, alteração, comunicação, difusão. O foco aqui é evitar os chamados vazamentos de dados ou *data breaches*, sejam eles causados por ataques direcionados a isso ou mesmo decorrentes de negligências praticadas pelos agentes de tratamentos (TEPEDINO; FRAZÃO; OLIVA, 2020).

A prevenção é um princípio que complementa ao princípio da segurança, impondo que os agentes de tratamento adotem as medidas necessárias para prevenir que danos ocorram em razão do tratamento de dados pessoais. É mais amplo que a segurança porque deveria ser interpretado como atividades não necessariamente técnicas, mas de governança e preparo para gestão de crises (GUILHERME, 2021).

Não é mera reiteração do princípio da segurança, estando, assim, relacionado com outras atividades não técnicas para impedir os dados aos titulares dos dados, o que pode incluir, mas não se limita a prover treinamentos, simular crises, ter planos de respostas a incidentes etc.

O princípio da não discriminação refere-se à impossibilidade de realização do tratamento de dados com finalidades discriminatórias, ilícitas ou abusivas e uma das grandes preocupações da LGPD é evitar que os titulares de dados sejam discriminados a partir do tratamento de seus dados pessoais, bem como lhes sejam impostas situações claras de abuso ou ilicitude (CRESPO, 2019), portanto, a lei não

se refere apenas à atuação em clara oposição, mas, também, ao tratamento baseado em abusividade, embora não haja uma definição legal do que possa representar esse abuso.

O último princípio previsto no art. 6º tem grande importância prática para os projetos de LGPD. É um direcionamento de que não basta cumprir com as exigências legais, mas que é preciso, acima de tudo, ser capaz de demonstrar que isso é feito de forma eficaz. A responsabilização e a prestação de contas é a demonstração, por parte do agente, que foram adotadas medidas capazes de comprovar que foram observadas e cumpridas as normas de proteção de dados pessoais, bem como a eficácia dessas medidas[7].

Além disso, o art. 42 da LGPD traz as hipóteses de responsabilização dos agentes de tratamentos quando causarem danos patrimoniais, morais, individuais ou coletivos, em razão do tratamento de dados que realizarem. Já as exclusões de responsabilidade são limitadas à demonstração de que não fizeram o tratamento, que o dano aconteceu em razão de culpa exclusiva da vítima ou situação que se enquadre nos termos do art. 43, “embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados”. Isso só se poderá demonstrar, se houver boas práticas de governança, de *compliance* e de *accountability*. Sem estas, a exclusão da responsabilidade muito dificilmente será declarada.

Vale ressaltar que embora viva-se em um mundo onde tudo tem nascido em ambientes digitais, não se ignora que ainda há registros em variados outros tipos de repositórios, muitos em papel. A LGPD não faz qualquer distinção sobre o repositório onde se encontram os dados pessoais, sendo plenamente aplicável inclusive, a tudo o que estiver registrado em papéis (CRESPO, 2019).

Na atualidade, a importância - ou até mesmo indispensabilidade - da *internet* requer a adequação de direitos e garantias do cidadão ao ambiente cibernético, entre os quais se destaca a privacidade. Os conceitos de privacidade e de proteção de dados pessoais na *internet* possuem muitos aspectos, resultado das várias possibilidades de uso desse instrumento, o que cria um desafio legal para a correta tutela dos interesses dos indivíduos.

[7] Também previsto no art. 146 do GDPR.

Fortes (2016, p.183) estabelece quatro direitos-base a título de direitos de privacidade na Internet (originalmente, *Internet Privacy Rights*): “o direito de navegar pela Internet [sic] com privacidade; o direito de monitorar quem monitora; o direito de deletar os dados pessoais; o direito a uma identidade online”. Sendo o direito à privacidade corolário da dignidade humana e um direito fundamental de primeira dimensão, sua tutela de modo adequado é elemento indispensável em um Estado democrático de direito.

Longhi (2017) salienta que a privacidade na Internet é um pressuposto de um sistema democrático deliberativo por dois grandes motivos. O primeiro diz respeito à guarida dos dados pessoais como forma de evitar hierarquizações e discriminações com base em informações pessoais. O segundo, a restrição da autonomia privada do indivíduo frente ao abuso de poderes públicos e privados quando detentores de informações pessoais.

Mas estes não são os únicos problemas jurídicos em torno da proteção da privacidade dos cidadãos em um sistema democrático. O primeiro deles é o da sua abrangência. Isto porque, há, no ocidente, dois grandes sistemas que se dedicam à guarnecer a privacidade: liberdade e dignidade. O da liberdade, oriundo dos países da *common law*, tutela a privacidade como uma espécie de liberdade pública abrangente, que justifica a não intervenção de terceiros na esfera de decisão do indivíduo. Já a privacidade como dignidade é uma característica dos países da tradição jurídica continental, restringindo-se à proteção da intimidade e vida privada dos indivíduos (DONEDA, 2006).

Restringindo-se às TICs, leciona Rodotà (2008) que o direito à privacidade hoje ganha novos contornos, dando margem à existência de um direito autônomo dele decorrente, a proteção dos dados pessoais. Embora ambas façam alusão à proteção da dignidade humana, os dados pessoais tutelam um bem jurídico diverso da intimidade. Enquanto um cuida do “corpo físico” o outro cuida do “corpo eletrônico”. Ou seja, os dados, quando analisados e disponibilizados em conjunto, permitem que se formem perfis a serviço tanto do mercado como do Estado. Algo que põe em risco todos os outros direitos e garantias fundamentais.

3. O consentimento dos titulares de dados como objeto primordial da proteção de dados

Inicialmente, a LGPD, define no inc. XII do art. 5º que consentimento é definido como a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, em seguida em seu art. 7º, a LGPD ressalta que o tratamento de dados pessoais somente poderá ser mediante o fornecimento de consentimento pelo titular. Fica clara a intrínseca relação entre o consentimento e a efetiva aplicação da lei no campo prático, tal importância dada pela lei outorga ao titular dos dados, o poder sobre suas próprias informações.

No mesmo sentido, Ruaro (2015) explica que, a autodeterminação informativa é a possibilidade de um indivíduo, titular de determinado dado, exigir a forma como eles devem ser tratados ou que não sejam tratados. Dito de outra forma é a capacidade, possibilidade e liberdade que as pessoas têm para decidir sobre o tratamento de seus dados, e se desejarem, interromper este tratamento.

E ainda, Rodotà (2008) acentua que, esse direito considera ilegítima toda coleta de informações pessoais que for realizada sem um prévio conhecimento e explícito consentimento do interessado. Esse direito consiste em que determinadas informações coletadas sobre uma determinada pessoa não devem circular fora da instituição pública ou privada que tenha coletado essas informações originalmente para certa finalidade.

Segundo a previsão dos Incs. VI e VII do art. 7º da Lei 12.965/2014, tal direito encontra-se alicerçado em dispositivos que: 1) veda o fornecimento a terceiros de registros de conexão e de acesso a aplicações de Internet, exceto mediante consentimento livre, expresso e informado; 2) exige clareza e completude das informações sobre a coleta, uso, tratamento e proteção de seus dados pessoais; e 3) que apenas poderão ser empregados para as finalidades que fundamentaram sua coleta.

Como se viu, a LGPD prevê expressamente que a autodeterminação informativa é um dos fundamentos da disciplina da proteção de dados pessoais. O objetivo legal é atribuir à pessoa, o direito de saber o que é feito com as informações pessoais e decidir se autoriza ou não a utilização para fim diverso da que foi obtida.

Porém, uma questão essencial que surge com tudo isso está centrada na forma como esse controle deverá ser exercido a fim de assegurar o direito à proteção de dados. Tal resposta ultrapassa a questão jurídica, pois está adstrita à gestão de políticas públicas da qual o direito já regulou, e para que este direito possa ter efetividade este representa mais um desafio que deverá ser transposto. Assim, no mesmo sentido que a engenharia informática é capaz de criar inteligências artificiais para tratar informações, a criação de ferramentas para que o indivíduo possa ter esse conhecimento e manifeste seu consentimento pode ser simples de ser desenvolvido e posto à disposição da pessoa que for alvo dessa situação.

Nether (2018) explica que historicamente, assim como os regimes absolutistas foram dando lugar a regimes democráticos, em diversos países no mundo, esse direito à autodeterminação informativa está sendo reconhecido gradativamente pelos sistemas jurídicos, e se consolidando como resultante da afirmação constante da necessidade de regimes democráticos.

Como se vê, no Brasil está em fase inicial ou embrionária, tendo em vista a fase que se encontra a recente vigência da Lei, mas esse direito, como derivante do direito fundamental à proteção dos dados pessoais, está se tornando imprescindível nos dias atuais. Diante disso, pode-se constatar que os dados pessoais precisam ter um significado e valor diferentes, bem como mais abrangentes de quando foi incluso no rol de direitos fundamentais na década de 1980, quando da promulgação da CRFB/1988.

4. Os avanços tecnológicos e a segurança de informação

De acordo com a literatura especializada, a era da informação está relacionada aos avanços tecnológicos da comunicação e da informação no campo digital, a partir dos anos 70, com a invenção do computador, da internet e dos cabos de fibra óptica. Tem por base o processo e a dinâmica da comunicação *online*, por meio de redes, adquirindo um poder multidimensional, estabelecido de acordo com os interesses e os valores dos diferentes usuários (CASTELLS, 2005).

Brancher, Kujawski e Castellano (2019) vão além ao afirmarem que a revolução tecnológica digital promoveu a corrosão das fronteiras da intimidade, na qual o devassamento da vida privada se tornou mais agudo e inquietante. Ele avalia que essa revolução, muitas vezes, avança desprovida de diretrizes morais, o que acarreta uma deformação progressiva dos direitos fundamentais numa escala cada vez maior de assédio.

Castells (2005), criador do conceito de sociedade em rede, esclarece que estamos conectados a grupos de pessoas com interesses distintos e com acesso ilimitado, o que podemos compreender como redes. Basicamente, estas são estruturas abertas, integrativas e dinâmicas, com capacidade de expansão ilimitada, onde pessoas compartilham os mesmos códigos de comunicação para acessarem ou compartilharem suas informações.

A sociedade em rede é também uma sociedade complexa, contingente, com inúmeras possibilidades de escolhas, pautada pela revolução dos meios de comunicação em massa e em tempo real com futuro incerto e inseguro, cujos indivíduos estão cada vez mais vulneráveis aos riscos, o que levou Beck (2011) a cunhar a expressão “sociedade de risco”.

O mundo da “Era da *internet*” é um mundo agitado, acelerado, prenhe de novas possibilidades, de novas liberdades. É um tempo de otimismo e geração de riqueza. Um mundo tomado pela exigência de informação de todos a todos: pelos cidadãos diante de governos que se quer mais transparentes; de patrões a empregados, que se quer atualizados. E de seu centro nervoso, quiçá mais nervoso que o de outras Eras, se fazem decorrências mil (ROBERTO, 2010).

Este elevado crescimento da *internet*, levou ao aumento substancial de dados estruturados e não estruturados, bem como ao compartilhamento deles levando alguns autores, a exemplo de Mèlo (2019) a afirmarem que estamos na era do *big data*, que nada mais é, que uma era marcada pela intensa produção e fluxo de dados.

Através da *Web* qualquer pessoa com conhecimentos mínimos de informática pode acessar e divulgar conteúdo na rede em tempo real, sem intermediários. Os próprios usuários podem desenvolvê-la e aprimorá-la.

A partir do surgimento de dispositivos que viabilizam que usuários se comuniquem na *internet*, eleva o número de pessoas conectadas. O advento da

rede sem fio fez crescer a quantidade de pessoas acessando a *internet* (SILVA, 2017). As facilidades de pacotes de serviços ofertadas pelos provedores atualmente a um valor reduzido e com alta velocidade motivou mais pessoas a acessarem a Internet, seus inúmeros benefícios e também dissabores o que leva à necessidade de se investir em segurança da informação.

Primeiramente, a aplicação do termo segurança da informação está relacionada a uma abordagem abrangente, que se baseia em diversos pilares e vem de muitos caminhos diferentes, independente do meio onde os dados estão armazenados ou são transmitidos. Inclusive, pode-se entender que é a preservação da confidencialidade, integridade e disponibilidade da informação, conforme norma ISO 27001 (BIONI, 2019).

Já por segurança cibernética pode-se entender que seja referente às informações que estejam em meios digitais, conforme definições presentes na ISO 27032 que, além de elencar a definição de segurança cibernética, define também o que é o espaço cibernético:

> Espaço Cibernético: ambiente complexo resultante da interação de pessoas, software e serviços na Internet por dispositivos de tecnologia e redes conectadas a ele, ao qual não existe em qualquer forma física.
> Segurança Cibernética (*Cyber Security*): preservação da confidencialidade, integridade e disponibilidade das informações no Espaço Cibernético (MÈLO, 2019, p. 63).

Segundo Mèlo (2019), ainda se está no processo de aprender como trazer segurança para o *cyberspace*. Para ele, antes do termo cibersegurança estar na moda, o foco era segurança computacional, ou seja, tudo estava relacionado à Tecnologia da Informação.

Atualmente, a humanidade subsiste em uma sociedade tecnológica, permeada por uma infinidade de ameaças e vulnerabilidades e preocupações com a proteção do patrimônio digital, ou seja, aquele que está em ativos intangíveis, passou a ter uma relevância cada vez maior (BIONI, 2019). Tudo isso fica mais evidente quando se percebe o quanto a operação de uma empresa e a sociedade em si podem ser afetadas caso se perca o sinal de conexão de internet ou o forte impacto dos danos resultantes de um vazamento de informações.

Tudo isso, gera um fomento na necessidade de maior proteção nas organizações e instituições que lidam com esse risco, sendo possível por meio de

ações que demandam investimentos em políticas, em tecnologia, em processos e melhores práticas, aliados a campanhas de conscientização e campanhas que promovem a educação em segurança digital, já que, lacunas nos esclarecimentos deixam dúvidas e abrem as portas para a judicialização da matéria.

A LGPD pode ser usada como ferramenta prática na proteção dos dados, pois, mais que cumprir a lei é necessário ter meios para comprovar que todo o tratamento de dados é praticado adequadamente. Dessa forma, o agente de tratamento de dados deverá demonstrar ter adotado procedimentos autorizados e exigidos pela lei, mas, acima de tudo, ser capaz de comprovar sua eficaz implementação na organização. Isso é importante, pois, mesmo que sua ação seja imbuída de boa-fé, se não houver meios para se demonstrar esse intuito, de nada valerá perante autoridades de fiscalização ou em demandas administrativas e judiciais para, de alguma forma, atenuar sua responsabilidade.

Vale ressaltar, além disso, que, embora viva-se em um mundo onde tudo tem nascido em ambientes digitais, não se ignora que ainda há registros em variados outros tipos de repositórios, muitos em papel. A LGPD não faz qualquer distinção sobre o repositório onde se encontram os dados pessoais, sendo plenamente aplicável, inclusive, a tudo o que estiver registrado em papéis (CRESPO, 2019).

Houve também a minimização de violações legais e éticas, com o surgimento da *General Data Protection Regulation* (GDPR) que trouxe o conceito de *accountability* para a proteção de dados e, na legislação brasileira, foi denominado princípio da responsabilização e da prestação de contas, impõe mais do que o cumprimento da lei, havendo a obrigação de se adotar medidas para que seja possível comprovar a efetivação da implementação de um programa de *privacy compliance* na organização. Desta forma, cabe ao agente de tratamento de dados fazer tudo o que for possível para cumprir as obrigações legais.

Ainda destacam-se as práticas de *Privacy by Design,* que se tratam essencialmente de um método de planejamento e estrutura de padrão de segurança, a fim de propiciar maior eficiência e controle efetivo na proteção dos dados. Serve, pois, para garantir o uso ético dos dados no limite do consentimento do usuário no que tange a circulação de dados nos meios de comunicação tecnológicos consumeristas.

Assim, finaliza-se com a percepção de que toda evolução econômica apenas se justifica se estiver afinada com os axiomas mais expressivos do sentimento jurídico atual – no âmbito interno e comparado – de promoção e proteção da pessoa, seus valores e direitos essenciais, no qual se inclui, inevitavelmente, a nova faceta da privacidade, qual seja, a tutela dos dados pessoais.

5. Segurança e boas práticas no relacionamento com os dados pessoais – aplicação de *compliance* digital

Catapultados pela pandemia, avança-se (por necessidade) na jornada da transformação digital e na desmaterialização das relações. Atualmente, a sobrevivência dos negócios e a própria existência do homem em sociedade nunca foram tão dependentes de sistemas (e seus algoritmos), cada vez mais conectados e distribuídos (GUILHERME, 2021).

Seja do trabalho cada vez mais remoto, passando pelo ensino, expandindo sem fronteiras, ao atendimento médico virtual em qualquer local do mundo, depende-se cada vez mais dos sistemas que conectam e suportam as atividades humanas (alguns decidem pelas pessoas também).

Excelentes padrões estão disponíveis para aplicação pelas empresas, em especial, o conjunto ISO 27.001, 27.005, 27.032 e 27.701 e o *framework* desenvolvido pelo Instituto Nacional de Padrões e Tecnologia dos EUA (NIST), denominado *Cybersecurity Framework*.

Com tudo isso, pode-se afirmar que o tema cibersegurança não é apenas mais um indicador de conformidade baseado nas boas práticas de mercado (em especial, a ABNT NBR ISO/IEC 27032:2015) ou em uma nova necessidade de atender exigências legais, sejam elas de um setor regulado como o financeiro, mercado de capitais, saúde ou mesmo para assegurar a privacidade das pessoas. Cibersegurança é uma necessidade, e ela nunca foi tão necessária como nos dias atuais.

Nos últimos anos, a importância da segurança cibernética está diretamente vinculada à necessidade de se aperfeiçoar os mecanismos de controle para prevenção dos riscos cibernéticos. Isso exige um planejamento específico que

salvaguarde a segurança e a legitimidade para tratar as ameaças e aplicar metodologias de defesa dentro da previsão legal (SILVEIRA, 2017).

A criação de novas normas governamentais de cibersegurança e de padrões legislativos comuns apresentados por Organizações Internacionais buscam estabelecer o consenso entre os países e os diversos setores estratégicos, sobretudo, infraestruturas críticas. Porém, tendo em vista a complexidade de aplicação das normas e amplitude do assunto, por vezes apenas a existência das regras pode não ser suficiente para garantir as boas práticas no relacionamento com os dados pessoais. Daí então, surgem meios para auxiliar as organizações e os órgãos de fiscalização, como a *accountability* e *compliance*.

Accountability[8] é um termo bastante comum na língua inglesa, sem tradução exata para o vernáculo. É comumente traduzido como responsabilidade das organizações e seus membros pelas atividades que praticam. É uma prestação de contas sobre o que fazem, como fazem e os efeitos destas ações, mas não em termos numéricos e sim com foco num viés de desempenho relativo à governança (CRESPO, 2019).

O *accountability* é a responsabilização e prestação de contas como elementos a serem concretizados para demonstrar a conformidade com a lei (PENNA, 2020).

O conceito de *accountability* foi bastante estendido com o tempo, com divisões materiais e de alcance sobre sua aplicação. No entanto, aqui assume-se o conceito como a possibilidade de responsabilizar agente públicos ou privados em razão das suas atividades.

O *General Data Protection Regulation* (GDPR) trouxe o conceito de *accountability* para a proteção de dados e, na legislação brasileira, está insculpido no art. 6º, X, e foi denominado princípio da responsabilização e da prestação de contas.

Como dito alhures, é por este princípio que se impõe mais do que o cumprimento da lei, havendo a obrigação de se adotar medidas para que seja possível comprovar a efetivação da implementação de um programa de *privacy compliance* na organização. Desta forma, cabe ao agente de tratamento de dados

[8] *Accountability* origina-se de *accomptare* (do latim, tomar em conta), derivado de *computare* (computar) que, por sua vez, deriva de *putare* (calcular). É uma extensão da terminologia usada em empréstimos financeiros.

fazer tudo o que for possível para cumprir as obrigações legais (TEPEDINO; FRAZÃO; OLIVA, 2020).

Os elementos concretos que podem personificar a existência de responsabilidade pelo tratamento de dados pessoais podem ser demonstrados pela existência de políticas, normativas e procedimentos, pela existência de controles internos, pelo constante monitoramento para evitar falhas e para impedir sua reincidência. Também pode ser enxergados através da existência de procedimentos de auditoria, dos registros das atividades processantes (art. 37 da LGPD), dos registros da atuação independente de um encarregado de proteção de dados (art. 41 da LGPD), da realização de *assessments* e relatórios de impacto (art. 38), de registros de incidentes de segurança (art. 48 da LGPD) e de violação de dados, além de treinamentos e planos de respostas a incidentes. Isso tudo pode ser extraído do art. 50 da LGPD[9], que trata dos programas de *privacy compliance* e das boas práticas nacionais e internacionais de um robusto programa de *compliance*.

Todo este rol, quando posto em prática, tenderá a evitar que existam punições em patamares altos, já que no juízo de gravidade de uma violação deverão ser levadas em conta as medidas técnicas adotadas (art. 48, § 3º, c.c. art. 50 da LGPD).

Como resumo, o dever de responsabilidade ou *accountability* imporá às organizações que, além de alterar suas rotinas em fluxos de tratamentos de dados pessoais, providenciem a estruturação de um verdadeiro programa de *compliance* com foco nos dados pessoais, de modo a demonstrar efetivamente sua implementação por meio de registros robustos e coerentes de atividades voltadas à proteção de dados pessoais (TEPEDINO; FRAZÃO; OLIVA, 2020).

Os desafios, portanto, vão muito além de seguir normas previstas em lei, passando pela necessidade de ter uma forte organização interna, desenhar processos, treinar pessoas, classificar informações e saber quais devem ser preservadas, por quanto tempo, quais devem ser descartadas e como isso é realizado, bem como estruturar as atividades para atender às diversas entidades que

[9] Art. 50 - 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 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.

poderão fiscalizar as atividades de tratamento de dados pessoais, como também desenhar e implementar formas de atendimento aos direitos dos titulares de dados pessoais.

Estes pontos supracomentados podem não exaurir tudo o que é preciso fazer para se proporcionar elementos de *accountability*, mas, certamente, já são desafios grandes o suficiente para trazer dificuldades de implementação pela grande maioria das organizações.

Em razão da necessidade de identificar o que priorizar e quais controles aplicar de modo prático, pois não é raro encontrar controles genéricos ou em um nível elevado de aplicação nas boas práticas supramencionadas, observa-se a crescente aplicação do *framework* do *Center for Internet Security* (CIS) (MÈLO, 2019). Por meio de um guia de implementação criado pelo CIS, o responsável pela segurança consegue trilhar o seu plano de ação com a identificação do porte de sua empresa (pequena, média e grande) e dos controles necessários para implementar, divididos em básicos, fundamentais e organizacionais (BIONI, 2019).

A necessidade de estabelecer padrões mínimos de segurança e aplicá-los (realmente) na prática torna-se necessário para todos, seja a pessoa, um usuário do sistema, uma empresa ou o governo (SILVEIRA, 2017).

Claro que não se pode exigir perfeição nem nada que esteja em absoluta desproporcionalidade com os recursos financeiros e técnicos disponíveis. Mas é preciso providenciar uma estrutura de governança corporativa que garanta o cumprimento das normas de proteção de dados e que disponibilize um conjunto de documentos que podem provar que estas obrigações estão realmente sendo satisfeitas. Diante disso, surgem desafios para colocar em prática todos esses conceitos, assunto que será discutido no próximo capítulo.

Patrícia Peck (2021) orienta que é fundamental criar um programa de *compliance* digital, com *risk assessment*, planos de respostas a incidentes, treinamentos e comunicação, *due diligence* de terceiros, e que tudo isso deve ser analisado considerando o ramo do negócio ou empresa e a maturidade da governança dos dados pessoais.

Apesar de o *Compliance* Digital não ser obrigatório tal proposta é desejável. Contudo, existem limitações a sua aplicação quando se considera, por exemplo, seus custos de implementação e as dificuldades que podem ser enfrentadas pelas

micro e pequenas empresas. Diante disso, é importante que seja avaliada a relação custo-benefício desse projeto.

Segundo Zilli (2021), se adequar à LGPD pode gerar um custo alto para as empresas, pois a lei é extensa e complicada, contém obrigações muitas vezes consideradas ambíguas que ao primeiro contato pode ser de difícil interpretação. Essas complexidades na lei acabam por se tornar um grande desafio para as empresas sobretudo para as pequenas e médias. Ainda segundo o autor:

> "Na Europa alguns estudos indicam que o valor médio pago para um profissional da gira em torno de 70 mil euros por ano. No Brasil a média salarial de um DPO gira em torno de R$ 10.000,00 a R$ 21,5 mil. Isso faz que muitas empresas principalmente as PMes (pequenas e médias empresas) sofram para entrar em conformidade com a Lei de proteção de dados, pois muitas tem uma realidade financeira muita abaixo do que as grandes organizações." (Zilli, 2021, p.25)

Considerando todas as limitações, tanto de custos quanto de qualificação de mão-de-obra para executar uma boa gestão de proteção de dados, se torna importante discutir as alternativas possíveis para tornar essa realidade acessível às empresas de porte menor, e tais alternativas podem ser extraídas de perspectivas criadas pela própria lei, através do controlador.

Pelo inc. VI do art.5º, a LGPD define que o controlador é pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Tendo em vista as funções do controlador, o art. 50 da referida Lei, permite que os controladores e operadores formulem regras de boas práticas e de governança relacionadas ao tratamento de dados pessoais. Diante disso, cria-se uma nova perspectiva para a ME/EPP, permitindo a aplicação das exigências impostas pela legislação de forma paralela ao *Compliance* Digital, devendo sem prejuízo a legalidade do assunto.

Dentre as possibilidades estão 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. Isso quer dizer que os controladores e operadores teriam a liberdade de estabelecer normas próprias para a governança e colocar em prática seus próprios regimes e procedimentos voltados a garantia da proteção de dados tratados naquele local.

Outrossim, a lei permite que essas figuras controlem suas normas de segurança, e coordenar os padrões técnicos e obrigações específicas para os

diversos envolvidos no tratamento dos dados. Poderão também se incumbir das ações educativas e dos mecanismos internos de supervisão e de mitigação de riscos por conta própria, tendo seu próprio sistema de controle e gestão o que cria alternativas para a simplificação da aplicação da lei.

A ainda em seu art.50, a referida lei permite que tal idealização de regras seja feita individualmente ou por meio de associações, no qual é possível se extrair que, a empresa poderia contar com o apoio de organizações ou profissionais especializados em direito digital, podendo ser analisada a possibilidade de se terceirizar a gestão dos dados, caso os custos e a gestão dos processos pudessem se tornar mais administráveis para empresas de porte pequeno, ressaltando, novamente, a relevância de se avaliar os custos e riscos de se fazer uma gestão interna própria ou não.

Ademais, em um futuro próximo, seria possível considerar um ordenamento jurídico pelo direito ao tratamento diferenciado às ME/EPPs no que se refere à gestão de dados, nos moldes do que se vê hoje na Lei 123/2006 e suas alterações, principalmente no que concerne à fiscalização pela ANPD. Sendo este um tópico a ser analisado em novos estudos conduzidos futuramente sobre o tema.

CONCLUSÃO

Vive-se atualmente em uma sociedade rede. Como a internet não tem fronteiras, nas relações digitais, o limite da liberdade do indivíduo e dos negócios é a ética. Todos da rede têm o mesmo poder tanto para agir de forma protetiva como de forma destrutiva, e, portanto, o dever de praticar segurança da informação. Por isso, a importância de fomentar uma cultura de cibersegurança.

Trata-se, a princípio de uma mudança cultural, que deve efetivar-se através de investimentos em capacitação e aperfeiçoamento técnico com vistas a identificar e apontar os impactos socioeconômicos e os métodos para que a mudança esteja em conformidade com as regras. Esta mudança cultural consiste em um trabalho educativo para que todos tenham conhecimento da forma como funciona: riscos, direitos, limites e responsabilidades.

Juntamente com as soluções tecnológicas e revisões de contratos, a capacitação das equipes está entre os pilares que devem nortear o planejamento das instituições.

Para que a legislação possa realmente se mostrar mais efetiva, é necessário que o usuário seja conscientizado, especialmente quanto à sua função de implementar as melhores práticas de segurança digital. Por este motivo, as próprias leis estão trazendo consigo o dever de realizar campanhas de conscientização.

Isso é observado na Resolução 4658/2018, artigo 3º, que prevê sobre o mínimo que uma política de segurança cibernética precisa contemplar e traz ainda em seu art. 4º a previsão de que política de segurança cibernética deve ser informada aos funcionários e às empresas que prestam serviços a terceiros, valendo-se de linguagem clara, acessível, adequadamente detalhada e compatível com a sensibilidade das informações e funções desempenhadas, além do dever que as instituições têm de divulgar ao público um resumo contendo ao menos as diretrizes gerais da política de segurança cibernética (artigo 5º).

Do mesmo modo ocorre quando comparado à LGPD, que também traz previsões similares nos artigos 6º, 9º, 14 e 50.

Isto posto tem-se que um programa de *privacy compliance* de sucesso é bastante complexo de se conseguir. O time de proteção de dados precisa acompanhar as mudanças regulatórias e estatutárias, analisar ameaças internas e externas, se relacionar com diversos *stakeholders*, prover à alta liderança as informações estratégicas para manutenção e desenvolvimento do programa de proteção de dados, entre outras tantas atividades. Vê-se que se trata de um jogo coletivo, não de disputas individuais.

Um dos itens essenciais para se obter sucesso num programa de *privacy compliance* é o alinhamento com os objetivos dos negócios. Mas esta é apenas uma faceta de alinhamento, já que ele precisa existir, também, para os aspectos regulatórios e dos *stakeholders*. Um grande desafio aqui é equilibrar todas essas facetas de alinhamento, já que, se atendida apenas uma delas, a tendência será o fracasso.

Accountability é outro desafio, uma vez que a responsabilidade pelo tratamento de dados não se esvai com a construção de um programa de *privacy compliance* e com o apontamento de um encarregado ou DPO. É necessário muito

mais do que isso: alta direção e demais níveis de colaboradores precisam atuar não só com palavras, mas dar exemplos concretos de que atuam com boa-fé e diligência no que diz respeito aos dados pessoais tratados pela organização. Para este atendimento, é essencial haver ótima comunicação interna e treinamentos frequentes.

Por fim, adaptabilidade é outro desafio, visto que está relacionado a mudanças. Algumas podem levar muito tempo; outras muito pouco para acontecer. A recente pandemia foi um significativo fator de mudanças, muitas, inclusive, relacionadas ao tratamento de dados pessoais em razão da necessidade de atuar em *home office*. Mas a adaptabilidade depende de outros fatores, como desafios regulatórios (com mais normas regulando a proteção de dados no país e no mundo), bem como os desafios impostos pelo desenvolvimento tecnológico.

Evidentemente não há uma fórmula mágica e pronta para que a *accountability* seja devidamente tratada pelas organizações, mas, certamente, a boa inter-relação entre *accountability*, alinhamento e adaptabilidade é um fator que poderá representar o sucesso ou o fracasso de um programa de *privacy compliance*.

REFERÊNCIAS

BECK, Ulrick. **Sociedade de risco**: rumo a uma outra modernidade. 2. ed. Tradução de Sebastião Nascimento. São Paulo: Editora 34, 2011.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2020.

BRANCHER, Paulo Marcos Rodrigues; KUJAWSKI, Fábio Ferreira; CASTELLANO, Ana Carolina Heringer Costa. Princípios gerais de proteção de dados pessoais: uma análise dos princípios elencados no art. 6 da Lei nº 13.709/2018 (LGPD). In: BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Cláudia (Coords.). **Proteção de dados pessoais no Brasil**: uma nova visão a partir da Lei nº 13.709/2018. Belo Horizonte: Forum, 2019. p. 63-70.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 25 mar. 2021.

CABRAL, Carlos; CAPRINO, Willian. **Trilhas da Segurança da Informação.** Rio de Janeiro: Brasport. 2015.

CASTELLS, Manuel. A sociedade em rede: do conhecimento à política. In: CASTELLS, Manuel; CARDOSO, Gustavo. (Orgs.). **A sociedade em rede**: do conhecimento à acção política. Belém: Imprensa Nacional, 2005, p. 19.

CRESPO, Marcelo Xavier de Freitas. Compliance Digital. In: CRESPO, Marcelo Xavier de Freitas. **Governança, Compliance e Cidadania**. 2. ed. São Paulo: Revista dos Tribunais, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

FERGUSON, Andrew Guthrie. Big Data and Predictive Reasonable Suspicion. **Univesity of Pensylvania Law Review**, v. 163, n. 327, January, 2015.

FORTES, Vinícius Borges. **Os Direitos de Privacidade e a Proteção de Dados Pessoais na Internet**. Rio de Janeiro: Lumen Juris, 2016.

GUILHERME, Luiz Fernando do Vale de Almeida. **Manual de Proteção de Dados**: LGPD comentada. São Paulo: Almedina, 2021.

LONGHI, João Victor Rozatti. **Processo Legislativo Interativo**. Curitiba: Juruá Editora, 2017.

MARCACINI, Augusto Tavares Rosa. **Aspectos fundamentais do Marco Civil da Internet**: Lei no 12.965/2014. São Paulo: Edição do Autor, 2016.

MÈLO, Augusto. **Proteção de Dados Pessoais na Era da Informação**. Curitiba: Juruá Editora, 2019.

NETHER, Nicholas Augustus de Barcellos. **Proteção de Dados dos Usuários de Aplicativos**. Curitiba: Juruá Editora, 2018.

PENNA, Thomaz Murta e. Proteção de Dados vs *blockchain*: o armazenamento *off-chain* como garantia de direitos dos titulares de dados pessoais no Brasil. In: PEDROSA, Clara Bonaparte. Direito e Tecnologia: discussões para o século XXI. Belo Horizonte: Legal Hackers, 2020. p. 131-158.

PINHEIRO, Patrícia Peck. **Direito Digital.** 6 ed. São Paulo: Saraiva, 2016.

_____. **Direito Digital aplicado 4.0**. 1 Ed. 2021. São Paulo: Revista dos Tribunais, 2021.

_____. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

ROBERTO, Wilson Furtado. **Dano Transnacional e Internet**. Curitiba: Juruá Editora, 2010.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden. Privacidade e autodeterminação informativa: obstáculos ao estado de vigilância? **Arquivo Jurídico**, Teresina – PI, v.2, n.1, p.41-60, Jan./Jun., 2015.

SALLES JR., Carlos Alberto Corrêa; SOLER, Alonso Mazini; VALLE, José Angelo Santos do; RABECHINI JR., Roque. Gerenciamento de riscos em projetos. 2ª. Ed. Rio de Janeiro: Editoria FGV, 2010.

SILVA, Alexandre Assunção. **Sigilo das Comunicações na Internet**. Curitiba: Juruá Editora, 2017.

SILVEIRA, Sérgio Amadeo da. **Tudo sobre tod@s:** redes digitais, privacidade e venda de dados pessoais. São Paulo: Edições Sesc São Paulo, 2017.

SOMBRA, Thiago Luiz Santos. **Fundamentos da regulação da privacidade de proteção de dados:** pluralismo jurídico e transparência em perspectiva. São Paulo: Revista dos Tribunais, 2019.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro**. 2. ed. São Paulo: Revista dos Tribunais, 2020.

ZILLI, Felipe. **Os Desafios para as Empresas Diante a Adequação a Regulamentação a Lei 13.709/2018**. Curitiba, 2021. 60 p. Monografia (Bacharelado em Direito) - Centro Universitário Curitiba. Documento eletrônico. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/18637