PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Especialização em Direito da Proteção e Uso de Dados

Sandra Buth Zanon

PROGRAMA DE GOVERNANÇA DE DADOS E SUA IMPORTÂNCIA PARA A ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Belo Horizonte
2021

Sandra Buth Zanon

PROGRAMA DE GOVERNANÇA DE DADOS E SUA IMPORTÂNCIA PARA A ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Trabalho de Conclusão de Curso de Especialização em Direito da Proteção e Uso de Dados como requisito parcial à obtenção do título de especialista.

Belo Horizonte

2021

1 INTRODUÇÃO

A evolução tecnológica vem garantindo um rápido desenvolvimento da sociedade que se transforma a cada dia, à medida que surgem novos meios de comunicação e aumenta a capacidade de processamento de dados digitais. A ampliação do acesso da população aos meios de comunicação e à Internet também contribui para a globalização e consequente maior disseminação de informações.

Nesse contexto, surge a problemática do uso indevido de dados pessoais e a consequente necessidade de tutelar o direito à intimidade e à privacidade das pessoas, cada vez mais expostas na rede mundial de computadores. Assim, em 2018 foi promulgada a Lei Geral de Proteção de Dados Pessoais (LGPD), plenamente em vigor, tendo como principal objetivo a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

O presente estudo objetiva analisar a estrutura mínima que um programa de governança de dados deve ter para que uma instituição, seja ela pública ou privada, esteja em conformidade com a LGPD, garantindo segurança aos dados pessoais dos titulares, o que também impactará positivamente sua competitividade e sua reputação. Para tanto, analisou-se o contexto em que se desenvolveu a necessidade de tutela dos dados pessoais com culminância na publicação da LGPD no Brasil, seus fundamentos e princípios. Foi elaborado a partir de uma pesquisa qualitativa e exploratória em referências bibliográficas produzidas por pesquisadores, profissionais e organizações empenhados no estudo dos impactos das novas normativas de privacidade e proteção de dados pessoais na vida das pessoas e das instituições, no contexto do mundo hiperconectado em que vive a sociedade contemporânea.

Ao final, considerando que as pessoas jurídicas de direito público, no desempenho de sua finalidade pública, apresentam particularidades no tratamento de dados pessoais, bem como também devem atender a outros normativos, tais como aqueles voltados à transparência pública, propõe-se uma análise da convergência da LGPD e da Lei de Acesso à Informação (LAI) e reflexão dos aspectos vagos no contexto da preservação histórica de documentos públicos que contenham dados pessoais.

2 O DESENVOLVIMENTO DOS DIREITOS DA PERSONALIDADE NA SOCIEDADE CONTEMPORÂNEA

Atualmente a sociedade está estruturada em torno da rede mundial de computadores performando atividades econômicas, educativas, culturais e políticas. Essa amplitude da internet[1] acaba por envolver toda a sociedade, seja em seus negócios, seja em sua vida privada. Esse envolvimento cada vez maior das pessoas na dimensão virtual é o que leva ao compartilhamento de infinita quantidade de dados, informações, ideias, convicções etc. através das redes que circundam e envolvem o mundo atual. De acordo com Castells (2003, p. 5) “uma rede é um conjunto de nós interconectados. A formação de redes é uma prática humana muito antiga, mas as redes ganharam vida nova em nosso tempo transformando-se em redes de informação energizadas pela Internet.”

O desenvolvimento amplo e acelerado das tecnologias da informação e da Internet é o que tem garantido a digitalização dos negócios e a virtualização das relações humanas. No âmbito público, por exemplo, a prestação de serviços públicos mais eficientes e direcionados aos anseios da sociedade requer o uso cada vez maior de tecnologias da informação que proporcionarão mais capacidade de processamento de dados. Estar na rede tem suas vantagens, assim como usufruir dos benefícios do *machine learnig*, dos *big datas* e da inteligência artificial, por exemplo. Contudo, o desenrolar das atividades no mundo virtual, com as formas de ser e de fazer se alterando constantemente, aos poucos vem revelando que também pode haver desvantagens. O crescente monitoramento das pessoas com o fim de segurança e a captação excessiva de dados pessoais com o fim de personalização e melhoria da qualidade de oferecimento de produtos e serviços, por exemplo, são atividades cujos fins, na teoria, justificariam a coleta de dados pessoais. Na prática, porém, não raro observa-se um abuso de finalidade e desrespeito à boa-fé quando esses dados pessoais são tratados e usados para outros fins, que afrontam a dignidade da pessoa humana, tais como o controle, a manipulação e o comércio não autorizado de dados pessoais.

> O volume de dados cresce de forma exponencial com a evolução e sofisticação da rede mundial de computadores e de suas aplicações. Todo o potencial de conhecimento obtido com a coleta, o processamento, o armazenamento e a análise dos dados pode ser utilizado a favor da

> sociedade. Por outro lado, os dados podem ser utilizados: pelos governos, para o controle do cidadão e com objetivos políticos; ou pelas organizações privadas, para direcionar um determinado padrão de consumo. (AZAMBUJA; GRANVILLE; SARMENTO, 2019, p.14).

Neste cenário, ganham o palco as discussões sobre os limites da vida privada. O conceito de privacidade entendido como o "direito a ser deixado só" foi assim concebido por Warren e Brandeis (1890 apud Doneda, 2006) no final do século XIX. No entanto, a preocupação com a tutela da privacidade e intimidade da pessoa natural ganhou outros contornos na sociedade contemporânea. Na era digital, a privacidade e a intimidade são violadas pelo compartilhamento de dados pessoais em rede, aquela concepção individualista de privacidade precisou evoluir para atender a realidade do mundo atual, superando o pretérito direito de ficar só para passar a ser entendido como o direito do indivíduo de controle sobre o uso de seus dados pessoais, também conhecido como autodeterminação informativa[2]. Colombo e Facchini Neto (2019) deixam evidente a relação entre a necessidade de proteção dos dados pessoais para garantir a privacidade nos dias atuais, dizendo:

> O mundo virtual permite a potencialização das violações que atingem o bom nome, a imagem, a privacidade, a identidade social das pessoas, a exposição de dados pessoais sensíveis […] em razão da sua assombrosa capacidade de difusão, em escala assustadoramente gigantesca. Assim, não só o meio digital permite a violação de alguns direitos fundamentais da pessoa, como também propicia uma replicação inimaginável dos danos. (COLOMBO; FACCHINI NETO, 2019, p. 10).

A dignidade da pessoa humana é fundamento da Constituição da República Federativa do Brasil (CRFB), de 5 de outubro de 1988, e dela decorrem direitos fundamentais como a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas e a garantia do direito de propriedade (BRASIL, 2016).

Da dignidade da pessoa humana também decorrem os direitos humanos e os direitos da personalidade, garantidos através de arcabouço jurídico específico, tais como o Código Civil e normas de direito público. Há consenso de que os direitos da personalidade são amplos, vista sua dimensão na proteção da condição humana. Abordando a evolução histórica dos direitos de personalidade, Colombo e Facchini Neto (2019) apontam que:

> Eles não surgiram "prontos" e acabados. Ao contrário, foram frutos de intensas e prolongadas lutas sociais, sofrendo uma evolução ao longo do tempo. E tal evolução está longe de estar acabada, pois à medida que a

> civilização avança, novos valores e novos problemas, derivados muitas vezes dos impactos tecnológicos na vida privada, outros direitos de personalidade vão surgindo. (COLOMBO; FACCHINI NETO, 2019, p. 5).

De acordo com o que assevera Castells (2003), de que a Internet se constitui em tecnologia suscetível de ser alterada como resultado das interações que ocorrem entre essa tecnologia e a sociedade, vislumbram-se novas possibilidades nas atividades humanas num futuro não muito distante, impulsionadas pelo uso da internet e pelas inovações tecnológicas. O *big data* e o *machine learning*, por exemplo, se constituem em sistemas de automação que já são utilizados para auxiliar no desenvolvimento do trabalho humano ou mesmo para substituir os humanos na realização de atividades, conferindo-lhes maior agilidade e eficiência, por sua capacidade de processamento na análise de grandes volumes de dados e até mesmo, capacidade de aprendizagem. A inteligência artificial ganha cada vez mais espaço na sociedade, vez que promete facilitar a vida das pessoas e otimizar os negócios, públicos e privados (MEDINA; MARTINS, 2020).

A transferência de conhecimento às máquinas, no entanto, não pode ser feita sem a transferência de dados. Os dados, por sua vez, assim como a informação, possuem valor econômico. Os dados pessoais, especificamente, também representam valores éticos e morais e sua exposição pode ser prejudicial aos titulares dos dados. Nesse contexto, tornou-se imprescindível rever e incrementar os institutos jurídicos vigentes para prever as novas relações da sociedade contemporânea, protegendo os direitos de todos os envolvidos, especialmente no que se refere às formas apropriadas e legítimas de tratamento de dados pessoais. Questões como os limites no uso da Internet e no uso de dados pessoais tiveram que ser mais amplamente legisladas, resultando em normativos como o Marco Civil da Internet (MCI) e a Lei Geral de Proteção de Dados Pessoais (LGPD).

3 OS NORMATIVOS DE PROTEÇÃO DE DADOS PESSOAIS: MCI E LGPD

A evolução da sociedade, conforme referido, trouxe a necessidade de especificar mais e melhor o uso da internet e o tratamento dos dados pessoais, a fim de garantir a proteção da dignidade da pessoa humana e de sua privacidade, mesmo que ela esteja interagindo nas redes sociais e compartilhando informações íntimas. Foi assim que se desenvolveu o Marco Civil da Internet (MCI) e a Lei Geral de Proteção de Dados Pessoais (LGPD), principais normativos atuais no Brasil que disciplinam a matéria.

O MCI, lei 12.965, de 23 de abril de 2014, tem como objetivo estabelecer "princípios, garantias, direitos e deveres para o uso da Internet no Brasil." (BRASIL, 2014). É sustentado por três pilares básicos: a privacidade dos usuários; a liberdade de expressão; e a neutralidade da rede. Neste sentido, o MCI tem importante papel na regulação da tutela dos dados pessoais frente ao direito de liberdade de expressão (BRASIL, 2014). Esse equilíbrio é de extrema importância para a preservação da memória nacional, especialmente quando se trata de arquivos públicos.

O desenvolvimento das leis de proteção de dados pessoais já se estende por cinquenta anos no cenário mundial e, de acordo com Viktor Mayer-Scönberger (1997 apud Doneda, 2011) é caracterizado por quatro gerações de leis. Na primeira geração, durante a década de 1970, a preocupação acerca do uso de dados pessoais estava voltada apenas aos limites técnicos a serem impostos ao seu tratamento, por conta da capacidade de processamento dos computadores. Somente em meados da década de 1980, na Europa, começou-se a desenvolver a noção de controle sobre o uso dos dados pessoais por parte dos titulares (DONEDA, 2011).

No Brasil, embora de forma esparsa, a preocupação com a privacidade e a proteção dos dados pessoais já existia antes da LGPD, estando capitulada em normativos como a Constituição da República Federativa do Brasil (CRFB), de 5 de outubro de 1988, o Código de Defesa do Consumidor (CDC), o Código Civil (CC), o Marco Civil da Internet (MCI), entre outros. Contudo, pode-se dizer que a LGPD é o primeiro normativo a dispor sobre o tema de forma autônoma, estabelecendo mecanismos instrumentais para viabilizar a tutela de direitos. É fruto de debates públicos que iniciaram em 2010 e projetos de lei que tramitaram no Congresso

Nacional na sequência. Está baseada nos objetivos e princípios do Regulamento Geral sobre a Proteção de Dados (GDPR - *General Data Protection Regulation*) instituído pelo Regulamento n. 2016/679, do Parlamento Europeu e do Conselho da União Europeia. De acordo com Bezerra (2019), o GDPR é um modelo internacional a ser seguido:

> Vista por muitos, como a mais completa legislação de proteção de dados do mundo a aplicabilidade do GDPR não está restrita apenas aos dados de pessoas naturais localizadas no âmbito da União Europeia, e sim, a todo o fluxo de dados existente entre os países membros e os demais países ao redor do mundo, que possuem pontos de contato com o mercado europeu. Sua abrangência, amplitude legislativa e maturidade conceitual tornam-no um verdadeiro um modelo mundial em que diversos países, inclusive o Brasil, têm se espelhado na busca de padrões normativos uniformes para a proteção de dados pessoais. (BEZERRA, 2019, p. 11).

O GDPR se tornou um modelo internacional de proteção de dados pessoais não apenas por comportar um sistema atualizado, adequado às necessidades da sociedade contemporânea, mas também porque entre seus princípios está a previsão de transferência de dados pessoais apenas com países que prezem pela proteção de dados pessoais, afetando, assim, as relações econômicas, políticas e sociais. A LGPD, portanto, é o normativo que assegurará a livre circulação de dados entre o Brasil e a União Europeia.

A LGPD foi publicada em 14 de agosto de 2018, lei n. 13.709. Sua promulgação veio suprir a necessidade de tutelar o direito de controle dos titulares sobre o uso de seus dados pessoais. Para Souza e Silva (2019),

> [...] a LGPD não inova na atribuição de direitos ao titular de dados pessoais, visto que apenas reproduz conteúdos que já eram atribuídos de longa data ao direito à privacidade. Em vez disso, consagra medidas e procedimentos que podem ser adotados pelo titular de dados ou que devem ser implementados pelo agente de tratamento, com vistas a efetivar a tutela da privacidade e, mais do que isso, mensurar a extensão da tutela desse direito. (SOUZA; SILVA, 2019, p. 10).

O objetivo, bem como os fundamentos e os princípios da LGPD estão claramente expressos no 1º e 2º artigos da lei. “Proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”, através de dispositivos “sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado”, constitui-se no objetivo da lei, fundamentado “no respeito à privacidade; na

autodeterminação informativa; na liberdade de expressão, de informação, de comunicação e de opinião; na inviolabilidade da intimidade, da honra e da imagem; no desenvolvimento econômico e tecnológico e a inovação; na livre iniciativa, na livre concorrência e na defesa do consumidor; e nos direitos humanos, no livre desenvolvimento da personalidade, na dignidade e no exercício da cidadania pelas pessoas naturais." (BRASIL, 2018). A lei apresenta, no artigo 6, rol exemplificativo dos princípios que dão suporte ao seu objetivo e fundamentos, a saber, boa-fé; finalidade, adequação, necessidade; livre acesso aos dados pelos titulares; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e responsabilização e prestação de contas (BRASIL, 2018).

De acordo com a LGPD, dado pessoal é "informação relacionada a pessoa natural identificada ou identificável." (BRASIL, 2018). A lei é mais exata quando conceitua o dado pessoal sensível, especificando os casos no inciso II do artigo 5. No entanto, a exposição de dados pessoais, considerados sensíveis ou não, pode trazer prejuízos ao titular de dados. Essa impressão é corroborada pelo Ministério Público Federal (2019):

> [...] entre os dados pessoais encontram-se os dados sensíveis, informações que, se conhecidas e processadas, prestam-se a uma potencial utilização discriminatória ou lesiva, particularmente mais intensa e que apresenta maiores riscos potenciais que a média. Exemplos: dados sobre raça, credo político, religioso, opções sexuais, histórico médico, dados genéticos. A análise de dados sensíveis apresenta elevado potencial lesivo aos titulares. Mas mesmo dados não considerados sensíveis, submetidos a tratamento, podem levar à discriminação. (BRASIL, 2019, p. 57).

Na consecução do objetivo e atentando aos fundamentos, a LGPD se aplica às pessoas naturais e ao tratamento de dados realizados por qualquer meio, por pessoa natural ou jurídica, seja *online* ou *off-line*, do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional, de acordo com o disposto no artigo 3 (BRASIL, 2018). O artigo 7 prevê que o tratamento de dados pessoais poderá ser realizado mediante o fornecimento de consentimento pelo titular, que poderá ser expresso, informado, voluntário e por escrito ou por meios comparáveis, bem como as

situações em que o consentimento é dispensado. (BRASIL, 2018). Por fim, ressalta-se que os direitos previstos na LGPD não são absolutos, especialmente diante do interesse público, estando previstos os casos em que não será aplicada ao tratamento de dados pessoais no artigo 4.

4 PROGRAMA DE GOVERNANÇA DE DADOS EM CONFORMIDADE COM A LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD) prevê em seu artigo 50 a formulação de regras e a adoção de boas práticas de governança para o tratamento de dados pessoais. Neste sentido, entende-se que somente a partir do estabelecimento de uma política de proteção de dados pessoais e privacidade, os controladores e operadores poderão assegurar o cumprimento das normas de proteção de dados pessoais, bem como os titulares de dados terão garantido o direito de controle sobre seus dados pessoais (BRASIL, 2018).

De acordo com a LGPD, a política de proteção de dados pessoais e privacidade deve considerar, entre outras coisas, “a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.” (BRASIL, 2018). Para a consecução da política de proteção de dados pessoais e privacidade, a lei prevê a implementação de um programa de governança em privacidade com estrutura mínima, bem como a publicação e atualização contínua das boas práticas e de governança de dados (BRASIL, 2018).

Neste sentido, é essencial que a política de proteção de dados pessoais e privacidade esteja integrada e alinhada à governança corporativa das instituições. A governança corporativa está apoiada em quatro pilares, a saber, transparência, equidade, prestação de contas e responsabilidade e, segundo Valadares (2020, p. 133), denota a adoção de ações éticas e postura íntegra da instituição, através de “um conjunto de práticas que visam preservar a organização e gerar valores”. Entre essas práticas, aponta-se o desenvolvimento de um Programa de Governança de Dados (PGD) como forma efetiva de comprovar a capacidade da instituição de resguardar todos os aspectos da LGPD e demonstrar sua conformidade com a lei. Além disso, o desenvolvimento do PGD se constitui em mecanismo importante de *accountability*[3] e de *compliance*[4].

Outrossim, o tratamento de dados pessoais vem agregar políticas como as de segurança da informação e de gestão da informação, tornando-as coadjuvantes. Quer dizer, a política de proteção de dados e privacidade irá impactar outras políticas da instituição, que deverão ser melhoradas e adequadas, a fim de alcançar seu objetivo.

Sob esse aspecto torna-se essencial a reflexão sobre os dados pessoais que as instituições tratam, a começar pela análise do que coletam. A finalidade de tratamento de dados pessoais, princípio essencial da LGPD, talvez seja o “guia” para conduzir a aplicação coerente da lei: para quê os dados pessoais são necessários? Quais dados pessoais são necessários? A qual tratamento os dados pessoais precisam ser submetidos? Responder essas questões significa estabelecer uma base a ser seguida para a adequação da instituição à nova lei.

O saneamento da coleta de dados à razão do mínimo necessário é a medida que contribuirá para a eficácia da política com reflexos positivos na segurança da informação (por reduzir a possibilidade de incidentes com dados pessoais) e na gestão da informação (menos dados pessoais em documentos com valor histórico). Isso implica em repensar a elaboração de formulários e os procedimentos de trabalho, a fim de coletar e movimentar os dados pessoais o menos possível e retê-los pelo menor tempo necessário a fim de atender a finalidade de seu tratamento. Ainda, caso os documentos resultantes das funções e atividades da instituição tenham valor histórico, essa medida garante que somente dados pessoais imprescindíveis para a história social estarão registrados e serão divulgados.

Não há, ainda, uma metodologia consagrada para desenvolver programas voltados à governança de dados pessoais. Contudo, o Governo Federal publicou recentemente um guia para a elaboração de programa de governança em privacidade para órgãos públicos, elaborado pelo Ministério da Economia, do qual se depreende que um PGD influencia os processos de tomada de decisão da instituição e, portanto, deve estar alinhado à estratégia institucional, vez que esta visa o aprimoramento contínuo das ações de controle da instituição, considerando os riscos e com foco no desempenho (BRASIL, 2020).

A esse respeito, Valadares (2020) atenta que

> [...] não existe uma receita de bolo a ser seguida igualmente por todas as empresas. Cada uma deve buscar o seu caminho, e implementar as medidas que forem adequadas à sua realidade, pois que o mais importante é a criação de uma cultura de proteção de dados e segurança da informação, ou seja, entender a importância desse direito e o quanto ele diz respeito a todos nós. (VALADARES, 2020, p. 126).

Neste sentido, será abordada em sequência a estrutura mínima para o estabelecimento do PGD, sabendo que o melhor caminho está focado na mudança

de cultura que visa incorporar conceitos como *privacy by design*[5] e *privacy by default*[6] que denotam uma preocupação com a privacidade desde a concepção dos produtos ou serviços e adoção das melhores práticas orientadas à privacidade dos dados, respectivamente.

No que tange às fases do PGD, deve incluir avaliação inicial ou preliminar do cenário de privacidade e proteção de dados atual da instituição, indicação do encarregado pelo tratamento de dados e plano de conscientização e capacitação; inventário de dados pessoais tratados e diagnóstico detalhado das funções e atividades, aspectos de segurança e gestão da informação e mapeamento dos riscos; programa estratégico de atuação para governança de dados pessoais, incluindo mecanismos de gestão e levantamento de indicadores de gestão e de controle e elaboração de políticas; na sequência é necessário definir o plano de implementação propriamente dito de execução das ações necessárias para a adequação, incluindo a definição de papéis e responsabilidades, cronograma e custos; por fim, é imprescindível estabelecer monitoramento contínuo, a fim de garantir a eficácia do PGD, acompanhando os indicadores e avaliando a necessidade de atuações corretivas ou de melhoria.

4.1 Avaliação inicial e conscientização

Para definir os contornos do PGD é necessário, inicialmente, identificar se já existem regulamentos ou práticas na instituição voltadas para a privacidade e proteção de dados pessoais, os interessados, os pontos positivos e os pontos a serem melhorados para adequação à LGPD, incluindo as lacunas legais existentes. Isso possibilitará visualizar claramente e de forma estratégica os objetivos a serem traçados no escopo de tutelar a privacidade e os resultados que se pretende alcançar.

Ainda nesta fase, a LGPD requer, expressamente, nos artigos 5, 23 e 41, a designação de encarregado pelo tratamento de dados pessoais. O encarregado é um profissional indicado pelo controlador e operador, preferencialmente com conhecimentos jurídicos e de informática, que irá atuar como canal de comunicação entre o controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD)[7]. Suas atividades consistem em: aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da autoridade nacional e adotar providências; orientar os funcionários e os contratados

da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (BRASIL, 2018). Neste sentido, o envolvimento do encarregado em todas as fases do PGD é de extrema importância para o sucesso de sua atuação.

Não menos importante é a conscientização dos envolvidos no tratamento de dados na instituição, vez que está diretamente relacionada com a mudança cultural que se espera com a implementação do PGD. Uma boa forma de começar é promovendo campanhas de divulgação das novas lei e políticas de proteção de dados pessoais e privacidade e seus impactos nas atividades institucionais e ações de capacitação para comunicar e alinhar as ações do PGD.

4.2 Inventário de dados pessoais e diagnóstico

O passo seguinte é a realização do inventário de dados pessoais tratados pela instituição. Para tanto, é necessário o mapeamento dos dados pessoais para identificar o que é coletado, em função de quais atividades, e a que tipo de tratamento estão sujeitos. Em conjunto com o diagnóstico detalhado das funções e atividades, dos aspectos de segurança e de gestão da informação e do mapeamento dos riscos, o inventário de dados pessoais é imprescindível para que se definam as melhores estratégias de atuação para o alcance dos resultados pretendidos com o PGD, demonstrando o comprometimento da instituição na adoção dos processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais.

O mapeamento de riscos é importante à medida que incidentes de segurança em proteção de dados pessoais podem significar grandes prejuízos à instituição e lesar o direito de privacidade do titular de dados. No âmbito do PGD importa definir mecanismos adequados de gestão de riscos que realmente contribuam para o alcance dos seus objetivos com segurança. A elaboração de uma matriz de riscos que analise possíveis impactos *versus* probabilidade de ocorrência, é uma prática comum e permite identificar as vulnerabilidades a que a proteção de dados está sujeita e atuar na definição de estratégias para sua mitigação. De acordo com o Instituto Brasileiro de Governança Corporativa (2019) uma adequada gestão de riscos é imprescindível:

> [...] uma abordagem omissa ou inadequada pode custar caro, dadas as potenciais perdas que expõem a empresa. Em última instância, ela tem potencial para comprometer a sustentabilidade da organização e a confiabilidade da informação sob sua responsabilidade. (INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA, 2019, p. 9).

A gestão de riscos na área de proteção de dados pessoais encontra fundamentos nas normas da família ISO/IEC 27.000 que versam sobre o Sistema de Gestão de Segurança da Informação (SGSI), vez que alcançam toda espécie de dados digitais ou sistemas informatizados de gestão da informação.

A LGPD, em seu artigo 50, prevê a existência de mecanismos de mitigação de riscos e, em seu artigo 5, a existência do relatório de impacto à proteção de dados pessoais, o qual poderá ser solicitado pela ANPD. Além disso, prevê em seu artigo 44 que, na ocorrência de vulnerabilidades que afetam a segurança dos dados pessoais, caso as operações de tratamento não estejam apoiadas, entre outras coisas, na gestão de riscos, podem ser consideradas irregulares (BRASIL, 2018).

4.3 Programa estratégico de atuação para governança de dados pessoais

Nesta fase são definidas as práticas a serem adotadas para a adequação dos processos e produtos/serviços da instituição à LGPD, bem como os controles a serem implementados para monitorar o alcance dos resultados. Neste sentido, envolve a elaboração de políticas e procedimentos e a publicação de normativos voltados para o tratamento de dados pessoais na instituição e a garantia dos direitos dos titulares de dados, o desenvolvimento de mecanismos de gestão (projetos). De acordo com a LGPD, o controlador é responsável por estabelecer as bases legais para o tratamento, determinando o motivo e a finalidade, bem como avaliar e organizar a gestão de tratamento de dados pessoais da instituição para conduzi-la à conformidade legal.

É necessário definir e comunicar claramente na instituição quem são os controladores, os operadores, o encarregado e os titulares de dados, bem como as responsabilidades e os direitos e deveres de cada um (BRASIL, 2018). Além disso, nesta fase a transparência também deve ser contemplada. Isso implica a elaboração e publicação de termos de uso e política de privacidade para que os titulares de dados

tenham conhecimento sobre a forma como seus dados pessoais são tratados pela instituição.

4.4 Plano de implementação

Esta fase se constitui essencialmente no desenvolvimento dos projetos necessários à consecução dos objetivos do PGD, especialmente o planejamento das ações para adequação dos processos de trabalho e produtos e serviços oferecidos pela instituição a uma cultura de proteção de dados pessoais. Através dos projetos será possível planejar, organizar e gerenciar os recursos necessários, dentro de limites estabelecidos pelos interesses e necessidades da instituição, os quais serão definidos em escopo, cronograma, orçamento e resultados esperados.

Os projetos devem ser conduzidos de modo que contemplem o gerenciamento do ciclo de vida total da integralidade de dados pessoais tratados, em conformidade com a política de proteção de dados pessoais e privacidade instituída e procedimentos estabelecidos no PGD. Dentre os objetivos de todos os projetos deve estar o atendimento dos ditames legais e a garantia dos direitos dos titulares de dados.

4.5 Monitoramento contínuo

O monitoramento é contínuo e, por isso mesmo, não se trata de uma fase em particular, mas sim uma atividade que percorre todas as demais fases desde o início do PGD. Seus principais objetivos estão relacionados à eficácia do PGD, à *accountability* e ao *compliance*.

O monitoramento é realizado a partir de indicadores de desempenho, da comunicação dos resultados e da avaliação periódica do projeto e implica em atuações corretivas ou de melhoria e até em novos treinamentos. A utilização de um plano de monitoramento e avaliação é altamente requerida para esta fase, com o objetivo de acompanhar em detalhes o progresso do PGD em relação aos indicadores de desempenho e os riscos mapeados. As ameaças identificadas devem ser devidamente gerenciadas e mitigadas, bem como os incidentes de segurança.

As atividades de monitoramento e controle no âmbito das instituições públicas é assunto ainda mais delicado, visto estar o Poder Público sujeito a legislações que visam o combate à corrupção. Neste contexto, o conceito de *compliance* adquire

grande valor, por representar a adoção de práticas voltadas para o combate de violações à legislação e de atos de corrupção, com foco na garantia da prestação de serviços pautados na ética, na transparência e na sustentabilidade. Por seu caráter estratégico, o *compliance* deve se voltar também ao PGD, visando garantir a conformidade com a LGPD e outros institutos jurídicos e normativos legais que abordam o tema da privacidade e proteção de dados, a depender da área de atuação da instituição.

A não conformidade implica, entre outras coisas, a responsabilidade civil, presente sempre que há obrigação de fazer ou não fazer algo ou de suportar sanções legais ou penalidades, de acordo com o previsto no Código Civil (BRASIL, 2002). O mesmo instituto prevê ainda que o empregador responda pela reparação civil dos atos praticados por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele. No âmbito público, o Estado não está isento da responsabilidade civil, conforme previsto na Constituição de 1988, “as pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.” (BRASIL, 2016). Assim, a não conformidade pode custar caro, - inclusive aos cofres públicos - e não apenas em termos financeiros, mas também de reputação. Além disso, a análise da responsabilidade civil das instituições mostra a importância de iniciar o PGD com a capacitação dos envolvidos, isto é, de todos aqueles que irão atuar como controladores e operadores dos dados pessoais tratados pela instituição.

5 PROTEÇÃO DE DADOS FRENTE O ACESSO À INFORMAÇÃO

No que tange o Poder Público, há particularidades na aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD), definidas por sua finalidade pública. Neste sentido, a lei dispõe, no artigo 4, sobre as exceções para sua incidência na Administração Pública, a saber, quando os dados são tratados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação ou repressão de infrações penais. Além disso, o artigo 7 prevê as hipóteses em que os dados pessoais podem ser tratados pelas instituições públicas independente de consentimento, a saber, “para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.” (BRASIL, 2018).

O artigo 23 da lei, ao abordar o tratamento de dados pessoais pelas pessoas jurídicas de direito público, menciona expressamente que “deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.” (BRASIL, 2018). Ainda assim, o Poder Público não está isento de informar as hipóteses em que o tratamento de dados é realizado, nem de responder questionamentos da Autoridade Nacional de Proteção de Dados (ANPD), nem tampouco de observar todos os demais princípios e requisitos da lei para o tratamento de dados pessoais.

Entende-se que a consecução de políticas públicas é essencial à manutenção do Estado e, portanto, não há como se furtar do equacionamento entre interesses públicos e privados. A esse respeito, MacNeil (2019) conclui:

> Concede-se, geralmente, que o princípio de liberdade de informação, ou o “direito de saber” do público, constitui uma restrição legítima do direito do indivíduo à privacidade. O interesse público em uma cidadania informada e em um governo responsável requer que, quando o direito do indivíduo à privacidade se torna um impedimento ao direito de saber do público, o primeiro deve ceder lugar ao último. (MACNEIL, 2019, p. 20).

Para além dos usos primários dos dados e informações tratados pelas instituições públicas, há que se mencionar o fato de que a história política, social e econômica de um povo tem como fonte principal os arquivos públicos, local para

onde os documentos são recolhidos após cumprirem os objetivos primeiros para os quais foram criados e acumulados. Na LGPD, a custódia de documentos históricos que contenham dados pessoais pelos arquivos públicos não é abordada diretamente. O Regulamento Geral sobre a Proteção de Dados (GDPR), por sua vez, em suas Considerações 158 e 160, respectivamente, refere os documentos históricos:

> Quando os dados pessoais são tratados para fins arquivísticos, o presente Regulamento deverá ser também aplicável, à exceção dos casos de pessoas falecidas [...]. Quando os dados pessoais são tratados para fins de investigação histórica, o presente Regulamento deveria ser igualmente aplicável. Deveria incluir, também, as pesquisas históricas e as genealógicas, tendo em mente que o presente Regulamento não deverá ser aplicável a pessoas falecidas. (MACNEIL, 2019, p. 12-13).

A função dos arquivos é servir aos interesses sociais disponibilizando fontes de informação primárias, isto é, conjuntos de documentos íntegros, autênticos e confiáveis. Para compreender a função dos arquivos públicos e qual deveria ser seu posicionamento frente à aparente dialética entre o direito à privacidade e o de acesso à informação, toma-se como base o disposto na Lei de Arquivos, lei n. 8.159, de 8 de janeiro de 1991, segundo a qual "arquivos públicos são os conjuntos de documentos produzidos e recebidos, no exercício de suas atividades, por órgãos públicos de âmbito federal, estadual, do Distrito Federal e municipal em decorrência de suas funções administrativas, legislativas e judiciárias." (BRASIL, 1991). A lei prevê ainda que os documentos públicos que possuem valor histórico, probatório e informativo são de guarda permanente, motivo pelo qual devem ser definitivamente preservados. E também que "todos têm direito a receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo ou geral, contidas em documentos de arquivos, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado, bem como à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas." (BRASIL, 1991).

Passando para a análise da Lei de Acesso à informação (LAI), lei n. 12.527, de 18 de novembro de 2011, até este ponto, percebe-se que está alinhada com Lei de Arquivos. Porém, a LAI traz elementos novos a fim de cumprir seu objetivo de regulação do acesso à informação. Para tanto, prevê em seu artigo 31 a restrição de acesso às informações pessoais, relativas à intimidade, vida privada, honra e ima-

gem, por no máximo 100 anos, prazo após o qual os documentos considerados de valor histórico poderão ser tornados públicos. Durante esse prazo de restrição, de acordo com a LAI, documentos com informações pessoais custodiados nos arquivos públicos "poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem" e que a responsabilização pelo uso indevido dos dados pessoais será daquele que obtiver o acesso (BRASIL, 2011).

Além da LAI, a exigência de publicidade dos atos da Administração Pública também está prevista na Constituição de 1988 e em outros normativos específicos, como aqueles voltados à gestão fiscal pública. Segundo o Ministério Público Federal, não obstante as diretrizes de transparência pública terem sido abarcadas pelo ordenamento jurídico brasileiro, a abertura de dados no país ainda é pequena e insatisfatória para atender as diretrizes de disponibilização de informações previstas na LAI (BRASIL, 2019).

Para Souza e Silva (2019) a LGPD estabelece remédios legais para a tutela de um direito, o de privacidade, e a correta interpretação da lei é necessária para evitar a confusão entre remédios e direitos, sob pena dos mecanismos instrumentais (remédios) voltados a viabilizar a tutela de direitos (privacidade) e a mensurar a extensão dessa tutela, se tornarem situações jurídicas subjetivas próprias e autônomas, isto é, interpretadas como poderes absolutos. Neste sentido, ao abordar o tema da preservação de documentos públicos históricos é necessário cuidar dos interesses dos titulares de dados pessoais, de sua privacidade, sem descuidar de outros direitos relevantes. Para tanto, eventualmente, haverá casos concretos de interesses de titulares de dados que merecerão análise particular.

Percebe-se que a preocupação com a privacidade nos arquivos já existia antes da LGPD, no entanto, a lei trouxe um aprofundamento do conceito de privacidade e livre desenvolvimento da personalidade e, com ela, uma preocupação antes inexistente nos arquivos com a divulgação de dados pessoais, mesmo que fosse apenas o nome da pessoa. A pergunta é, até onde vai o dever do Estado de transparência e onde está o limite para a divulgação de dados pessoais? Talvez a resposta para esse questionamento esteja no princípio da finalidade de realização do tratamento para propósitos legítimos, isto é, se existir uma necessidade social ou estiverem em jogo outros direitos, a situação deve ser analisada e proporcionalmente equacionada. Não é à toa que a boa-fé figura ao lado dos princípios na LGPD.

A abordagem proposta do aparente impasse entre LAI e LGPD no âmbito dos arquivos públicos traz apenas algumas reflexões que merecem ser amplamente discutidas. Certo é que os responsáveis pela gestão pública deverão decidir sobre as medidas mais apropriadas para equacionar os direitos de privacidade e de transparência pública, alinhado à política de proteção de dados pessoais e privacidade e ao PGD instituído. Além disso, as decisões também deverão estar pautadas em orientações a serem emanadas da ANPD.

6 CONCLUSÃO

A preocupação atual com a privacidade no Brasil e no mundo encontra fundamento no avanço tecnológico, visto que, sem o potencial de processamento das tecnologias da informação e da inteligência artificial, outrora, era muito difícil a compilação, manipulação e compartilhamento de dados pessoais. Abdicar das tecnologias da informação na sociedade contemporânea, que tem no cerne de sua evolução justamente o desenvolvimento tecnológico, não é uma opção. Tornou-se, portanto, imprescindível, a atualização dos ordenamentos jurídico e legal, a fim de regular as novas relações decorrentes do avanço que se experimenta.

A publicação da Lei Geral de Proteção de Dados Pessoais (LGPD) evidenciou a necessidade de regulação do uso dos dados pessoais como forma de proteção da dignidade da pessoa humana e, mais especificamente, dos direitos fundamentais, compreendidos os da personalidade. Neste cenário, é premente a adaptação das instituições, públicas e privadas, às normas de proteção de dados.

O estudo demonstrou que a adequação é necessária e que ela inicia uma “nova era” para as instituições no que tange a forma de lidarem com os dados pessoais. Demonstrou ainda que, para a conformidade com a lei, é essencial a implementação de uma política de proteção de dados pessoais e privacidade e de um Programa de Governança de Dados (PGD), os quais delinearão o caminho a ser trilhado pela instituição. Não obstante a implementação de boas práticas, a necessidade de proteção de dados pessoais requer, em primeiro lugar, uma reflexão sobre os dados que as instituições têm tratado, a fim de se tornarem mais comprometidas com a garantia dos direitos da personalidade, coletando e compartilhando apenas o estritamente necessário.

Entender cada uma das fases do PGD é fundamental para gerenciar com eficiência e eficácia o tratamento de dados pessoais numa visão integrada e alinhada com as demais práticas da instituição, das quais o PGD pode se beneficiar, tais como a governança corporativa, o planejamento estratégico, a gestão de riscos e as ferramentas de *compliance* e *acountability*. Essa integração e co-atuação garantirá a adequação à LGPD, bem como trará outas vantagens à instituição, como o aprimoramento das demais políticas vigentes, melhora da imagem institucional e vantagem competitiva.

Por fim, num contexto de governança corporativa, *compliance* e *acountability*, a harmonização do direito de proteção de dados com o direito de acesso à informação no Poder Público é uma questão que não pode ser esquecida, vez que ainda demanda discussões e orientações mais específicas. Neste sentido, a análise dos pontos de convergência dos principais normativos vigentes, bem como dos aspectos vagos, levou à apresentação de pontos para reflexão sobre sua necessária interseção para garantir a preservação histórica legítima de documentos públicos, mesmo que contenham dados pessoais, sem descuidar do alinhamento à política de proteção de dados pessoais e privacidade e ao PGD instituídos.

---

[1] A ideia da Internet, inicialmente denominada Arpanet, surgiu entre as décadas de 1950 e 1970 com um objetivo de estratégia militar, durante a Guerra Fria. Somente na década de 1980 seu uso alcançou também objetivos científicos e acadêmicos e, finalmente, a partir da década de 1990, descobriu-se na internet uma excelente ferramenta também para fins comerciais. No Brasil, a primeira vez que se estabeleceu conexão com a rede mundial de computadores foi em 1988 (ALMEIDA, 2019).

[2] Autodeterminação informativa consiste no poder do indivíduo de determinar e controlar a utilização de seus dados pessoais. Está relacionada ao direito fundamental ao livre desenvolvimento da personalidade e permite que o indivíduo se realize enquanto pessoa, na medida em que decide como irá exercer seus direitos ou, até mesmo, se abster de exercê-los (ALMEIDA, 2019).

[3] *Accountability* é um dos pilares da governança corporativa e pressupõe que a "prestação de contas deve ser feita de forma clara, concisa e tempestiva, cabendo ao agente proceder com diligência e assumir a responsabilidade por seus atos e omissões." (PIMENTA; NOGUEIRA; FONSECA, 2020, p. 189-190).

[4] *Compliance* envolve "a execução de um grande conjunto de processos e atividades de controle, fundamentados em diretrizes…, para atender as necessidades da "Governança Corporativa" no cumprimento de suas missões, bem como, no atendimento das melhores práticas de mercado, das determinações de regulação e principalmente dos requerimentos legais, no cumprimento das Leis e Regulamentos nacionais e internacionais." (PEREZ; BRIZOTI, 2016, p. 8).

[5] *Privacy by design*, traduzido significa "privacidade desde a concepção". Trata-se de conceito inicialmente introduzido pelo GDPR e "significa que todas as etapas do processo de desenvolvimento de um produto ou serviço de uma empresa devem ter a privacidade em primeiro lugar. Ou seja, o conceito de privacidade deve estar totalmente embutido no projeto, e não se aplica à iniciativas onde a privacidade é discutida somente na fase final." (DANTAS, 2019).

[6] *Privacy by default*, traduzido significa "privacidade por padrão". Trata-se de conceito inicialmente introduzido pelo GDPR e "significa que um produto ou serviço, ao ser lançado no mercado, deve vir com as configurações de privacidade no modo mais restrito possível por padrão, e o usuário deve liberar acesso à coleta de mais informações caso julgue necessário." (DANTAS, 2019).

[7] A Autoridade Nacional de Proteção de Dados, órgão da administração pública federal, integrante da Presidência da República, está prevista no artigo 50-A da LGPD e possui autonomia técnica e decisória. De acordo com Bezerra (2019) "A Autoridade Nacional de Proteção de Dados é essencial

para a aplicabilidade das normas de proteção de dados pessoais e sua função é efetivar a tutela da privacidade enquanto propicia segurança jurídica na interpretação e aplicação da Lei.” (BEZERRA, 2019, p. 64).

REFERÊNCIAS

ALMEIDA, D. E. V. **Shadow profiles e a privacidade na internet**: a coleta de dados pessoais de usuários e não usuários das redes sociais. Porto Alegre: Editora Fi, 2019. *E-book*. Disponível em: https://www.editorafi.org/541daniel. Acesso em: 23 jul. 2021.

AZAMBUJA, A. J. G. de; GRANVILLE, L. Z.; SARMENTO, A. G. M. A privacidade, a segurança da informação e a proteção de dados no Big Data. **Parcerias Estratégicas**, Brasília, DF, v. 24, n. 48, p. 9-32, jan./jun. 2019. Disponível em: http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/914/831. Acesso em: 27 jul. 2021.

BEZERRA, M. R. B. Autoridade nacional de proteção de dados pessoais: a importância do modelo institucional independente para a efetividade da lei. **Caderno Virtual [do] Instituto Brasiliense de Direito Público**, Brasília, DF, v. 2, n. 44, abr./jun. 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3828. Acesso em: 5 ago. 2021.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 jul. 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. Brasília, DF: Presidência da República, [2014]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 4 ago. 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. Brasília, DF: Presidência da República, [2011]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 23 jul. 2021.

BRASIL. **Lei n. 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Brasília, DF: Presidência da República, [2002]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 4 ago. 2021.

BRASIL. **Lei n. 8.159, de 8 de janeiro de 1991.** Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Brasília, DF: Presidência da República, [1991]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8159.htm. Acesso em: 4 ago. 2021.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em:

http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 29 jul. 2021.

BRASIL. Ministério da Economia. **Guia de elaboração de programa de governança em privacidade.** Brasília, DF: Ministério da economia, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_governanca_privacidade.pdf. Acesso em: 5 ago. 2021.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 3. S**istema brasileiro de proteção e acesso a dados pessoais**: análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados. Brasília, DF: Ministério Público Federal, 2019. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr3/documentos-e-publicacoes/roteiros-de-atuacao/sistema-brasileiro-de-protecao-e-acesso-a-dados-pessoais-volume-3. Acesso em: 27 jul. 2021.

CASTELLS, M. **A galáxia da internet: reflexões sobre a internet os negócios e a sociedade**. Tradução de Maria Luiza X. de A. Borges. Revisão técnica Paulo Vaz. Rio de Janeiro: Jorge Zahar, 2003.

COLOMBO, C.; FACCHINI NETO, E. Violação dos direitos de personalidade no meio ambiente digital: a influência da jurisprudência europeia na fixação da jurisdição/competência dos tribunais brasileiros. **Civilistica.com**, Rio de Janeiro-RJ, v. 8, n. 1, p. 1-25, 28 abr. 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/400. Acesso em: 4 de ago. 2021.

CONTROLADORIA-GERAL DA UNIÃO. **A OGP**. Brasília, DF, 2021. Disponível em: https://www.gov.br/cgu/pt-br/governo-aberto/a-ogp. Acesso em: 21 jul. 2021.

DANTAS, H. LGPD: O que é Privacy by Design e Privacy by Default. **Advogatech**. [s.l.] 15 jun. 2019. Disponível em: https://www.advogatech.com.br/blog/@HenriqueDantas/lgpd-o-que-e-privacy-by-design-e-privacy-by-default-vc4zyjv. Acesso em 30 de julho de 2021.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 5 ago. 2021.

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

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. Papéis e responsabilidades do conselho na gestão de riscos cibernéticos. São Paulo, SP: IBGC Orienta, 2019. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2020/02/papeis-e-responsabilidades-do-conselho-na-gestao-de-riscos-ciberneticos.pdf. Acesso em: 3 ago. 2021.

MACNEIL, H. **Sem consentimento**: a ética na divulgação de informações pessoais em arquivos públicos. Tradução de Shirley Carvalhêdo Franco e Mônica Tenaglia. Belo Horizonte: Editora UFMG, 2019.

MEDINA, J. M. G.; MARTINS, J. P. N. do. A era da inteligência artificial: As máquinas poderão tomar decisões judiciais? **Revista dos Tribunais**, [s.l.], vol. 1020/2020, p. 311-338, out. 2020. Disponível em: https://www.thomsonreuters.com.br/content/dam/openweb/documents/pdf/Brazil/revistas-especializadas/rtdoc-27-10-2020-12-20-pm-1.pdf. Acesso em: 4 ago. 2021.

NOGUEIRA, F. A. C. e M. Governança corporativa e conformidade nas startups. *In:* PIMENTA, E. G.; NOGUEIRA, F. A. C. e M.; FONSECA, M. L. da (Orgs.). **Legal Talks** – Startups à luz do direito brasileiro. Belo Horizonte: Editora Expert, 2020. p. 187-209. *E-book*. Disponível em: https://experteditora.com.br/legal-talks-startups-a-luz-do-direito-brasileiro/. Acesso em: 5 ago. 2021.

PERES, J. R.; BRIZOTI, N. **UPDATE** – Guia COMPLIANCE – Fundamentos. São Paulo: Câmara do Livro, 2016. *E-book*. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/12/e-BooK-1-COMPLIANCE-Fundamentos.pdf. Acesso em 29 de julho de 2021.

SOUZA, E. N. de; SILVA, R. da G. Tutela da pessoa humana na lei geral de proteção de dados pessoais: entre a atribuição de direitos e a enunciação de remédios. **Pensar Revista de Ciências Jurídicas**, Fortaleza, CE, v. 24, n. 3, p. 1-22, jul./set. 2019. Disponível em: https://periodicos.unifor.br/rpen/article/view/9407. Acesso em: 5 ago. 2021.

UNIÃO EUROPEIA. **Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Bruxelas, 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 5 ago. 2021.

VALADARES, H. de C. F. Proteção dos dados e Startups. *In:* PIMENTA, E. G.; NOGUEIRA, F. A. C. e M.; FONSECA, M. L. da (Orgs.). **Legal Talks** – Startups à luz do direito brasileiro. Belo Horizonte: Editora Expert, 2020. p. 115-151. *E-book*. Disponível em: https://experteditora.com.br/legal-talks-startups-a-luz-do-direito-brasileiro/. Acesso em: 5 ago. 2021.