RICI Revista Ibero-Americana de Ciência da Informação

ISSN 1983-5213

Arquivos públicos: a proteção de dados diante do acesso à informação

Sandra Buth Zanon
Tribunal Regional Eleitoral de Santa Catarina, Florianópolis, SC, Brasil
sandrazanon@gmail.com

DOI: https://doi.org/10.26512/rici.v15.n2.2022.40678

Recebido/Recibido/Received: 2021-11-07
Aceitado/Aceptado/Accepted: 2022-07-11

ARTIGOS

Resumo
Este artigo apresenta uma discussão teórica sobre o contexto de desenvolvimento da necessidade de tutela dos dados pessoais com culminância na publicação da Lei Geral de Proteção de Dados no Brasil e como a privacidade pode ser garantida pelos arquivos públicos, ao tempo em que estes também cumprem sua função de preservar e difundir a memória da sociedade, servindo aos interesses sociais e garantindo o direito de acesso à informação previsto na Lei de Acesso à Informação. Tem como base uma pesquisa bibliográfica e documental, de caráter analítico e descritivo. Conclui que, para a conformidade com a lei, é essencial a implementação de uma política de privacidade, a qual irá impactar a gestão da informação que, por sua vez, precisa ser adequada para garantir a harmonização do direito de proteção de dados com o direito de acesso à informação, especialmente quando se trata de documentos públicos permanentes. A partir do estudo realizado, apresenta medidas para contribuir com as decisões dos responsáveis visando a solução do aparente impasse entre as normas jurídicas de privacidade e transparência no âmbito dos arquivos públicos.
Palavras-chave: Documento público permanente. Privacidade. Transparência. Lei Geral de Proteção de Dados. Lei de Acesso à Informação.

Public archives: data protection in front of information access
Abstract
This paper presents a theoretical discussion about the context of the development of the need to protect personal data culminating in the publication of the General Data Protection Law in Brazil and how privacy can be guaranteed by public archives, while they also fulfill their function of preserving and disseminating the memory of society, serving social interests and ensuring the right of information access predicted in the Access to Information Law. It is based on a bibliographic and documentary research, of analytical and descriptive character. It concludes that, for compliance with the law, the implementation of a privacy policy is essential, which will impact the management of information that, in turn, needs to be adequate to ensure the harmonization of the right to data protection with the right of access to information, especially when it comes to permanent public documents. From the study carried out, it presents measures to contribute to the decisions of those responsible for resolving the apparent impasse between the legal norms of privacy and transparency in the context of public archives.
Keywords: Permanent public document. Privacy. Transparency. General Data Protection Law. Access to Information Law.

Archivos públicos: la protección de los datos ante el acceso a la información
Resumen
Este artículo presenta una discusión teórica sobre el contexto de desarrollo de la necesidad de tutela de los datos personales, que culminó con la publicación de la Ley General de Protección de Datos en Brasil y como la privacidad puede ser garantizada por los archivos públicos, mientras también cumplen su función de preservar y difundir la memoria de la sociedad, sirviendo a los intereses sociales y garantizando el

derecho de acceso a la información previsto en la Ley de Acceso a la Información. Tiene como base una investigación bibliográfica y documental, de carácter analítico y descriptivo. Concluye que, para la conformidad con la ley, es esencial la implementación de una política de privacidad, la cual impactará la gestión de la información que, a su vez, necesita ser adecuada para garantir la armonización del derecho de protección de datos con el derecho de acceso a la información, especialmente cuando se trata de documentos públicos permanentes. A partir del estudio realizado, presenta medidas para contribuir con las decisiones de los responsables buscando la solución del aparente impasse entre las normas jurídicas de privacidad y transparencia en el ámbito de los archivos públicos.
Palabras clave: Documento público permanente. Privacidad. Transparencia. Ley General de Protección de Datos. Ley de Acceso a la Información.

1 Introdução

O avanço tecnológico 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 necessidade de tutelar o direito à intimidade e à privacidade das pessoas, cada vez mais expostas na rede mundial de computadores. Assim, em 14 de agosto de 2018 foi promulgada no Brasil a lei nº 13.709, conhecida como a *Lei Geral de Proteção de Dados Pessoais* (LGPD), plenamente em vigor desde agosto de 2021, 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 artigo pretende analisar 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. Além disso, propõe-se uma análise da convergência da LGPD e da lei nº 12.527, de 18 de novembro de 2011, conhecida como a *Lei de Acesso à Informação* (LAI), e os aspectos não abrangidos por tais normas jurídicas no contexto de preservação de documentos públicos. Assim, cabe o seguinte questionamento: até onde vai o dever do Estado de conferir transparência e onde está o limite para a divulgação de dados pessoais? Buscou-se uma resposta que vislumbre formas possíveis de viabilizar a transparência pública ao tempo em que se garanta o direito de privacidade, considerando as novas regras para tratamento de dados pessoais.

Foi elaborado a partir de uma pesquisa bibliográfica e documental, de caráter analítico e descritivo, observando-se as questões colocadas 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.

2 O desenvolvimento dos direitos da personalidade na sociedade contemporânea

A sociedade atual, em quase todas as suas atividades econômicas, culturais, sociais, políticas e até na vida privada, é permeada pela rede mundial de computadores, conhecida como internet[1]. Essa imersão cada vez maior de instituições e pessoas no ambiente virtual leva ao compartilhamento de infinita quantidade de dados, informações, ideias, etc.

O desenvolvimento amplo e acelerado das tecnologias da informação e da internet tem garantido a digitalização dos negócios e a virtualização das relações humanas. No âmbito público, por exemplo, a prestação de serviços mais eficientes e direcionada aos anseios da sociedade requer o uso cada vez maior de tecnologias da informação que proporcionarão maior capacidade de processamento de dados. Estar na rede tem suas vantagens, assim como usufruir dos benefícios do *machine learning*, 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 a finalidade de obter segurança, e a captação excessiva de dados pessoais com a justificativa de personalização e melhoria da qualidade de oferecimento de produtos e serviços, por exemplo, são atividades que, na teoria, legitimariam a coleta de dados pessoais. Na prática, porém, não raro observa-se um abuso de finalidade e desrespeito à boa-fé quando esses dados são tratados e usados de modo a afrontar a dignidade da pessoa humana, sendo utilizados no controle, na manipulação e no comércio não autorizado de dados pessoais, como exemplificam Azambuja, Granville e Sarmento (2019):

> 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).

Em tal 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

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).

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, vez que esses direitos são violados pelo compartilhamento de dados pessoais em rede. Esta mudança ocasionada pela era digital levou à evolução da concepção individualista de privacidade, 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 a garantia da 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 Federal (CF), de 5 de outubro de 1988, e dela decorrem direitos essenciais 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[3]. Há consenso de que os direitos da personalidade são amplos, visto

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"Encara-se o Direito, regulando as atividades ou os interesses do homem, considerado como um ser individual, para integrar todas as regras atinentes a estes mesmos interesses, na ordem do Direito Privado. Enquanto que, quando se toma o homem como um elemento da sociedade e se exige a solidariedade para com todos os outros homens e respeito às instituições constituídas, as normas reguladoras de todas essas atividades, sejam do homem ou das instituições políticas, enfeixam-se no Direito Público... São considerados, *v.g.*, como Direito Privado o Direito Civil, o Direito Comercial e o Direito Agrário". O Direito Público, por sua vez, compreende o "conjunto de leis, elaboradas para regularem os interesses de ordem coletiva, ou seja, precipuamente, a organização das instituições políticas de um país, as relações dos Poderes Públicos entre si, e destes com os elementos particulares, não quando encarregados isoladamente, mas como membros da coletividade, e na defesa dos interesses da sociedade... Mostra-se numa dupla face: Interno e Externo. No Externo compreende o Direito Internacional Público em suas várias manifestações. No Interno, constituindo-se do Direito Constitucional, Direito Administrativo, Direito Penal, Direito Processual, Direito Internacional Privado, tem aplicações dentro de seus limites territoriais, salvo as exceções que admitam sua extraterritorialidade" (SILVA, 2014, p. 484 e 485).

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

Atualmente, o MCI e a LGPD são dois normativos vigentes no Brasil que disciplinam de modo específico a matéria da proteção da dignidade da pessoa humana e a sua privacidade.

O MCI, promulgado pela lei nº 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.

A promulgação da LGPD, sob o nº 13.709, em 2018, 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 conteúdo 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, os fundamentos e os princípios da LGPD estão claramente expressos nos artigos 1º e 2º 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 (BRASIL, 2018). Esta se fundamenta “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 na 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 6º, rol exemplificativo dos princípios que dão suporte aos seus fundamentos e objetivo, 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 5º. 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 (BRASIL, 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 *on-line* 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 3º (BRASIL, 2018). O artigo 7º 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 4º.

Importante atentar que os dados anonimizados não são considerados dados pessoais de acordo com a lei, a menos que sua reversão seja possível. A anonimização consiste na utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Dados pessoais pseudo anonimizados, por sua vez, estão sujeitos à lei. Apesar dos dados também perderem a possibilidade de associação, direta ou indireta, a um indivíduo, na pseudo anonimização, diferente da anonimização, os dados suprimidos são mantidos separadamente pelo controlador em ambiente controlado e seguro (BRASIL, 2018).

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 do MCI e da LGPD, estando capitulada em normativos como a Constituição Federal (CF), o *Código de Defesa do Consumidor* (CDC) e o *Código Civil* (CC), 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 em sequência. Está baseada nos objetivos e princípios do Regulamento Geral sobre a Proteção de Dados (GDPR - *General Data Protection Regulation*) instituído pelo Regulamento nº 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 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 entre 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.

4 Programa de governança em privacidade para a conformidade com a LGPD

A 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). 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 de governança de dados (BRASIL, 2018).

A execução das ações voltadas para o estabelecimento do programa de governança em privacidade na instituição também alcança os arquivos públicos, que não estão isentos de rever suas práticas de difusão em razão das novas diretrizes voltadas à tutela da privacidade, apesar de a LGPD não ter abordado diretamente a custódia de documentos permanentes que contenham dados pessoais pelos arquivos públicos. Não obstante, destacam-se aspectos

importantes do programa de governança em privacidade para uma adequada gestão da informação, com harmonização do direito de proteção de dados e do direito de acesso à informação.

O primeiro aspecto requer uma reflexão sobre como as instituições tratam os dados pessoais, a começar pela análise do que coletam. A finalidade do tratamento de dados pessoais, princípio essencial da LGPD, talvez seja o "guia" para conduzir a aplicação coerente da lei. Diante deste princípio, alguns questionamentos são oportunos: os dados pessoais são necessários para quê? Quais dados pessoais serão realmente utilizados? A qual tratamento os dados pessoais precisam ser submetidos? Responder essas questões significa estabelecer uma base a ser seguida para a adequação das instituições à nova lei.

O saneamento da coleta de dados à razão do mínimo necessário é uma medida que contribuirá para a eficácia da política de proteção de dados pessoais e privacidade com reflexos positivos na segurança da informação e na gestão da informação. 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 à finalidade de seu tratamento.

Além disso, entende-se que o melhor caminho para o desenvolvimento do programa de governança em privacidade está focado na mudança de cultura que visa incorporar conceitos como *privacy by design*[4] e *privacy by default*[5], que denotam, respectivamente, uma preocupação com a privacidade desde a concepção dos produtos ou serviços e a adoção das melhores práticas orientadas à privacidade dos dados.

Apresenta-se, na sequência, uma reflexão acerca dos limites entre o privado e o público, na perspectiva dos arquivos públicos, os quais estão comprometidos também com a transparência pública e a memória social.

5 Proteção de dados diante do acesso à informação: LGPD x LAI

No que tange ao Poder Público, há particularidades na aplicação da LGPD, definidas por sua finalidade pública. Neste sentido, a lei dispõe, no artigo 4º, sobre as exceções para sua

4*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).

5*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).

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 7º prevê as hipóteses em que os dados pessoais podem ser tratados pelas instituições públicas independentemente 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) ou 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 de dados e informações tratados pelas instituições públicas, há que se mencionar o fato de que a história política, social e econômica da sociedade tem como fonte de informação importante os arquivos públicos, locais para onde os documentos permanentes são recolhidos após cumprirem os objetivos primeiros para os quais foram criados e acumulados. Na LGPD, conforme anteriormente referido, a custódia de documentos permanentes que contenham dados pessoais pelos arquivos públicos não é abordada diretamente. O GDPR, por sua vez, em suas Considerações 158 e 160, refere-se aos documentos permanentes:

> [Consideração de número 158] Quando os dados pessoais são tratados para fins de arquivo, o presente regulamento deverá ser também aplicável, tendo em mente que não deverá ser aplicável a pessoas falecidas. (GDPR, 2016).
>
> [Consideração de número 160] Quando os dados pessoais sejam tratados para fins de investigação histórica, o presente regulamento deverá ser

> também aplicável. Deverá também incluir-se nesse âmbito a investigação histórica e a investigação para fins genealógicos, tendo em mente que o presente regulamento não deverá ser aplicável a pessoas falecidas. (GDPR, 2016).

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 ao aparente impasse entre o direito à privacidade e o de acesso à informação, toma-se como base o disposto na Lei de Arquivos, lei nº 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 LAI, sob o nº 12.527, de 2011, até este ponto, percebe-se que está alinhada com a *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 imagem, 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" (BRASIL, 2011). A mesma lei prevê que a responsabilização pelo uso indevido dos dados pessoais será daquele que obtiver o acesso, bem como que a restrição a esses dados não poderá ser invocada em ações voltadas para a recuperação de fatos históricos de maior relevância.

Além da LAI, a exigência de publicidade dos atos da Administração Pública também está prevista na Constituição Federal de 1988 e em outros normativos específicos, como aqueles voltados à gestão fiscal pública. Não obstante as diretrizes de transparência pública terem sido

abarcadas pelo ordenamento jurídico brasileiro, segundo o Ministério Público Federal a abertura de dados no país ainda é pequena e insatisfatória para atender as diretrizes de disponibilização de informações previstas na LAI (BRASIL, 2019). Sousa (2019) conclui que o direito de acesso à informação é a base das democracias contemporâneas, bem como elemento essencial para a evolução política e social do mundo, afirmando que:

> [...] a promoção do acesso à informação é indispensável para a concretização da participação dos cidadãos na vida pública, resguardando o seu direito de controlar e vigiar as ações e decisões de seus governos eleitos representativamente (SOUSA, 2019, p. 61).

Barros *et al*. (2019) corroboram esta afirmação e acrescentam que o Estado tem o dever de fornecer mecanismos que facilitem, de forma eficiente, o acesso à informação.

Neste contexto, percebe-se que a preocupação com o acesso à informação nos arquivos, inclusive visando à proteção da privacidade, já existia mesmo antes da LAI e da LGPD, no entanto, essas leis aprofundaram os conceitos de transparência pública, de privacidade e de livre desenvolvimento da personalidade, respectivamente. A LGPD, por sua vez, fez emergir uma preocupação antes inexistente nos arquivos com a divulgação de dados pessoais, mesmo que fosse apenas o nome da pessoa. A pergunta é: onde está o limite entre o privado e o público?

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. Para Matos e Ruzyk (2020) a necessidade de compreensão harmonizada da LAI e da LGPD é inegável, assim como o fato da segunda ter encoberto, em alguma medida, a regra da publicidade das informações estabelecida pela primeira. Sabendo que tanto a privacidade como o direito à informação estão assegurados constitucionalmente no Brasil, para os autores, inexiste entre esses direitos qualquer hierarquia ou juízo de prevalência, sendo papel do legislador assegurar o exercício de ambos. Neste sentido, consideram que esses direitos devem ser conjugados e, em situações-limite, de colisão, ponderados, vez que direitos fundamentais não se interpretam restritivamente. Sugerem que "a chave hermenêutica para uma possível harmonização dos direitos fundamentais em jogo pode ser um conceito de interesse público, vinculado, ele próprio, a direitos fundamentais" (MATOS e RUZYK, 2020, p. 205). Bento (2020) concorda com essa linha de pensamento afirmando:

> De um modo geral, a técnica jurídica empregada nessa avaliação chama-se ponderação de direitos e consiste em um teste de dano e interesse público. Trata-se de sopesar o interesse público na transparência contra o interesse na proteção da privacidade e da autodeterminação informativa dos titulares dos dados (BENTO, 2020, p. 184).

Não se pode esquecer o motivo pelo qual a sociedade contemporânea necessitou regular juridicamente os limites para o tratamento de dados pessoais, fazendo evoluir o conceito de privacidade relacionado ao direito de ficar só para uma abordagem de autodeterminação informativa. Isso se deve ao desenvolvimento e uso massivo das tecnologias da informação e da internet que proporcionaram, entre outras coisas, grande poder de processamento e cruzamento de dados e difusão de informações, o que pode levar a resultados desastrosos para a intimidade e a vida privada. Este fato deve estar na base de qualquer abordagem arquivística que venha a ser definida acerca da proteção de dados pessoais contidos em documentos públicos.

Zimmerman (1983 *apud* MACNEIL, 2019, p. 44), sugere que uma lei de privacidade na sociedade da informação só pode ser justa se seu foco estiver na "identificação das trocas de informações que justifiquem proteção na origem" e não no simples fato de a informação ter sido divulgada, caminho "tortuoso", segundo o mesmo autor, que vem sendo adotado pelas leis de privacidade. Como exemplo, analisa-se a questão relacionada à divulgação de dados pessoais de servidores públicos contidos em documentos oficiais produzidos no exercício de suas funções públicas. Está expresso no artigo 3º da LGPD que a mesma deve ser aplicada quando "a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços" (BRASIL, 2018). Ora, o servidor público, no desempenho de suas funções, é considerado controlador e operador, o que afasta a necessidade de tratamento de seus dados. Entende-se que os dados pessoais de servidores estão sujeitos à lei apenas quando figurarem em documentos pessoais, mesmo nas suas relações com o ente público a que servem, vez que, no caso de interesses particulares, o servidor deixa de ser controlador/operador e passa a ser o sujeito cujos dados serão tratados. Doneda (2011, p. 93) afirma que a informação pessoal, para ser tratada à luz da LGPD, deve "possuir um vínculo objetivo com uma pessoa, revelando algo sobre ela". Esse vínculo, segundo o autor, é de extrema importância para afastar "outras categorias de informações que, embora também possam ter alguma relação com uma pessoa, não seriam propriamente informações pessoais". No mesmo sentido, a lei de privacidade canadense, conforme MacNeil (2019), também não submete informações pessoais de servidores públicos e demais colaboradores das instituições públicas atuando em suas funções públicas.

A internet é, atualmente, a extensão dos arquivos, vez que se constitui em ferramenta utilizada para promover a difusão dos documentos permanentes. Justamente por seu poder de potencializar a difusão de informações, surgiram outros mecanismos para garantir a tutela da

privacidade na rede - tais como o direito ao esquecimento[6] - que, no entanto, precisam ser invocados com cautela. O direito ao esquecimento guarda relação com a questão da proteção de dados e merece um estudo aprofundado, não podendo, *a priori*, ser utilizado como regra para requerer a exclusão de dados e informações de valor histórico-social da rede, sob pena de fragilizar outros direitos, como a liberdade de expressão e informação e a livre manifestação do pensamento.

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 de os 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. "Torna-se possível, assim, não apenas uma compreensão mais minuciosa acerca do funcionamento de tais instrumentos, mas também um controle valorativo eficaz do exercício dessas prerrogativas pelo titular de dados pessoais" (SOUZA; SILVA, 2019, p. 13). Neste sentido, ao abordar o tema da preservação de documentos públicos permanentes 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.

As discussões atuais acerca da problemática da preservação de documentos públicos permanentes contendo dados pessoais mostram que estudiosos e profissionais dos arquivos tendem à ideia de que a passagem do tempo distribui o valor dos direitos em questão, na seguinte medida: quanto mais o tempo passa, mais relevância ganha o direito de acesso à informação em detrimento ao direito de proteção de dados. Essa interpretação pode estar correta se considerarmos que tanto na lei de privacidade da União Europeia como na do Canadá está previsto que não estão sujeitas à proteção informações de pessoas falecidas, o que, quase sempre, denota a passagem do tempo. Brown (1981 apud MACNEIL, 2019) corrobora essa interpretação dizendo:

> [...] o princípio da passagem do tempo 'pressupõe que as razões e a indicação de negar o acesso diminuem ao longo do tempo. Ou, por outras palavras, o interesse público em permitir o acesso aos documentos governamentais aumenta ao longo do tempo (BROWN, 1981 apud MACNEIL, 2019, p. 126).

6 O fundamento do direito ao esquecimento está na facilidade de difusão da informação através da internet. "No ordenamento jurídico brasileiro tem-se o enunciado 531 do STJ, que dispõe que a tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento. Evidente que já se tem uma base para o direito ao esquecimento. Por mais que qualquer informação na rede seja perene, é dado aos usuários o direito de serem literalmente esquecidos pela rede, através da exclusão de seus dados" (ALMEIDA, 2019, p. 81).

Neste sentido, MacNeil (2019) sugere que documentos de valor permanente contendo dados pessoais poderiam ser protegidos por um prazo de restrição de acesso adequado para atender aos interesses particulares antes de sua divulgação pública.

As orientações do Conselho Internacional de Arquivos (ICA - International Council on Archives) são base para práticas que se observam no cenário internacional no intuito de harmonizar os interesses públicos e privados da informação, tais como, desenvolver uma política de acesso, acordar restrições de acesso na ocasião da transferência de documentos aos arquivos e controlar o acesso a documentos públicos permanentes com restrição (CONSELHO INTERNACIONAL DE ARQUIVOS, 2014). O ICA enfatiza em suas orientações a necessidade de divulgação da existência de restrições de acesso a determinados conjuntos documentais, quando houver. Também orienta o registro das restrições nos instrumentos de pesquisa dos arquivos, prevendo que até mesmo os documentos restritos devem ser descritos, com a respectiva pseudo anonimização. O princípio 5 estabelece que "arquivos são disponibilizados em condições de acesso igualitárias e justas", porém pedidos de acesso a documentos com restrição dependem da elegibilidade do solicitante. O princípio 8, por sua vez, dispõe que "pedidos de acesso são processados sem discriminação com base na raça, sexo, religião, crença ou condição social dos solicitantes" e que um pedido de acesso a documento restrito resulta em revisão imediata das restrições pelos responsáveis dos arquivos (CONSELHO INTERNACIONAL DE ARQUIVOS, 2014).

A dependência da autorização de acesso a documento restrito a uma análise particular do pedido, tendo como base principalmente sua legitimidade, é considerada uma problemática por alguns autores. Segundo MacNeil (2019), essa prática é considerada legítima e tem a vantagem de contribuir para a sensibilização dos pesquisadores para a necessidade de proteção da privacidade; no entanto, o autor também registra os perigos que essa prática pode fomentar, como a discriminação, o elitismo e a antidemocracia. Barros *et al.* (2019) também concluem, em suas análises comparativas entre LAI e LGPD, que essas leis, inevitavelmente, possuem pontos de encontro e desencontro, resultando num acesso condicional relacionado a diversos fatores, tais como "a intenção de quem quer acessar tais documentos, o teor dos dados ou informações pessoais registradas nesses documentos e, ainda, qual instrumento legal vai fundamentar o acesso ou a restrição de acesso" (BARROS *et al*., 2019, p. 37).

A preservação e difusão de documentos públicos permanentes que contenham dados pessoais ainda demanda discussões e orientações mais específicas. Contudo, o estudo demonstrou que há convergência entre a LGPD e a LAI. Assim, para contribuir com as discussões que trarão luz sobre o aparente impasse entre a LAI e a LGPD, no âmbito dos arquivos públicos, sugerem-se medidas para alicerçar as decisões dos responsáveis, entendendo que as decisões

também devem estar pautadas em orientações a serem emanadas da ANPD. Na avaliação dos tipos documentais produzidos e recebidos pelas instituições públicas deverá ser considerada, além do valor testemunhal, probatório e informativo, a existência de dados pessoais nos documentos que justifiquem um prazo de guarda intermediário mais longo antes de seu recolhimento, a fim de garantir a restrição de acesso mínima necessária em função dos dados pessoais neles contidos. Também é importante formular fundamentação consistente para justificar o interesse público de cada tipo documental recolhido ao arquivo permanente contendo dados pessoais, bem como considerar a obtenção de termo de concessão por parte do titular dos dados tornando manifestamente públicos os documentos permanentes que contenham seus dados pessoais. A pseudo anonimização dos dados pessoais contidos em documentos públicos permanentes deve ser considerada para a difusão na internet. Neste caso, o acesso local aos originais poderia ser concedido ao pesquisador, após o prazo de restrição a que estiverem sujeitos os documentos, sem possibilidade de reprodução. Um último recurso poderia ser a assinatura de um termo de responsabilidade pelo pesquisador que acessar dados pessoais contidos em documentos públicos permanentes, conforme sugere MacNeil (2019). Por fim, e em consonância com o programa de governança em privacidade, políticas de acesso a documentos públicos permanentes devem ser elaboradas e amplamente difundidas pelos arquivos, com informações claras sobre as restrições existentes, conforme sugere Schwaitzer (2020).

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 e reprodutibilidade das tecnologias da informação e da inteligência artificial, outrora, não se realizava com tanta qualidade, rapidez e na escala em que se realiza nos dias de hoje a compilação, a manipulação e o compartilhamento de dados pessoais. Abdicar das tecnologias da informação na sociedade contemporânea, que tem no cerne do seu desenvolvimento justamente a inovação tecnológica, não é uma opção. Tornou-se, portanto, imprescindível, a atualização do ordenamento jurídico, a fim de regular as novas relações decorrentes desse avanço.

A promulgação da LGPD, em 2018, 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 às normas de proteção de dados.

Este estudo demonstrou que para a conformidade com a lei é essencial a implementação de uma política de privacidade. Não obstante a implementação de boas

práticas, a necessidade de proteção de dados pessoais requer, em primeiro lugar, uma reflexão sobre o tratamento dos dados pelas instituições, a fim de as mesmas se tornarem mais comprometidas com a garantia dos direitos da personalidade, coletando e compartilhando apenas o estritamente necessário. Na consecução da política, o programa de governança em privacidade impactará também a gestão da informação, a qual requer as adequações necessárias para uma efetiva harmonização do direito de proteção de dados com o direito de acesso à informação, especialmente no âmbito dos arquivos públicos.

A preservação e a difusão de documentos públicos permanentes que contenham dados pessoais ainda demanda discussões e orientações mais específicas. Logo, a análise dos pontos de convergência dos principais normativos vigentes sobre privacidade e transparência, bem como dos aspectos não abrangidos por essas normas jurídicas no contexto de preservação de documentos públicos, levou à reflexão sobre sua necessária interseção, com apresentação de medidas adequadas para equacionar o direito de proteção de dados diante do acesso à informação nos arquivos, imprescindível para garantir a preservação legítima de documentos públicos permanentes que contenham dados pessoais.

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.

BARROS, G. da S.; SILVA, L. dos S.; SCHMIDT, C. Documentos públicos e dados pessoais: o acesso sob a ótica da lei geral de proteção de dados pessoais e da lei de acesso à informação. **Revista do Arquivo**, São Paulo, v. 5, n. 9, p. 22-39, outubro de 2019. Disponível em: <http://www.arquivoestado.sp.gov.br/revista_do_arquivo/09/artigo_01.php#inicio_artigo>. Acesso em: 10 mar. 2022.

BENTO, L. V. Critérios de ponderação entre o direito de acesso a informações públicas e o direito à proteção de dados pessoais: lições a partir do modelo espanhol. **Revista da CGU/Controladoria Geral da União**, Brasília, DF, v. 12, n. 22, p. 184 a 195, jul.-dez. 2020. Disponível em: <https://revista.cgu.gov.br/Revista_da_CGU/article/view/173>. Acesso em: 11 mar. 2022.

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. Constituição (1988). Constituição da República Federativa do Brasil de 1988. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 5 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 29 jul. 2021.

BRASIL. Lei nº 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. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 18 nov. 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 23 jul. 2021.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 4 ago. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 15 ago. 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 18 jul. 2021.

BRASIL. Lei nº 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 9 jan. 1991. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8159.htm>. Acesso em: 4 ago. 2021.

BRASIL. Ministério Público Federal. **Sistema 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, 2019, 85 p. 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 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, v. 8, n. 1, p. 1-25, 28 abr. 2019. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/400>. Acesso em: 4 ago. 2021.

CONSELHO INTERNACIONAL DE ARQUIVOS. Comitê de Boas Práticas e Normas. Grupo de Trabalho sobre Acesso. **Princípios de acesso aos arquivos: orientação técnica para gestão de arquivos com restrições.** Tradução de Silvia Ninita de Moura Estevão e Vitor Manoel Marques da Fonseca. Rio de Janeiro: Arquivo Nacional, 2014. Disponível em:

<https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/principios_acesso_arquivos.pdf>. Acesso em: 13 mar. 2022.

DANTAS, H. LGPD: **O que é Privacy by Design e Privacy by Default.** [S.l.]: Advogatech, 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 jul. 2021.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, [S.l.], 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.

MACNEIL, H. **Sem consentimento: a ética na divulgação de informações pessoais em arquivos públicos.** Belo Horizonte: Editora UFMG, 2019.

MATOS, A. C. H.; RUZYK, C. E. P. Diálogos entre a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação. In: TEPEDINO, G.; FRAZÃO, A.; OLIVA, M. D. (Coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2 ed. São Paulo: Thomson Reuters Brasil, 2020. p. 195-215.

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.], v. 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 (Org.). **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.

SCHWAITZER, L. de B. da S. LGPD e acervos históricos: impactos e perspectivas. **Archeion Online Revista de Arquivologia da UFPB**, João Pessoa, v. 8, n. 2, p. 36 a 51, out-dez 2020. Disponível em: <https://periodicos.ufpb.br/index.php/archeion/article/view/57020>. Acesso em: 11 mar. 2022.

SILVA, De P. e. **Vocabulário Jurídico.** Atualizadores Nagib Slaibi Filho e Priscila Pereira Vasques Gomes. 31 ed. Rio de Janeiro: Forense, 2014.

SOUSA, A. G. de. Arquivo, democracia e acesso à informação pública: breve panorama da experiência internacional. **Revista do Arquivo**, São Paulo, v. 5, n. 9, p. 60 a 71, outubro de 2019. Disponível em: <http://www.arquivoestado.sp.gov.br/revista_do_arquivo/09/artigo_04.php#inicio_artigo>. Acesso em: 10 mar. 2022.

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, 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.

UNIÂO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation). **Jornal Oficial da União Europeia**, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 12 mar. 2022.

VALADARES, H. de C. F. Proteção dos dados e Startups. In: PIMENTA, E. G.; NOGUEIRA, F. A. C. e M.; FONSECA, M. L. da (Org.). **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.