Gerenciamento dos dados pessoais em arquivos

Uma perspectiva centrada no indivíduo com base na LGPD

Personal data managing in archives: a human centered perspective based on the Brazilian General Data Protection Law / Gestión de datos personales en archivos: una perspectiva centrada en el ser humano basada en la Ley Brasileña de Protección General de Datos

José Augusto Bagatini
Mestrando em Ciência da Informação na Universidade Estadual Paulista Júlio de Mesquita Filho (Unesp), Brasil.
jose.bagatini@unesp.br

José Augusto Chaves Guimarães
Doutor em Ciências da Comunicação pela Universidade de São Paulo (USP) e livre-docente em Análise Documentária pela Unesp. Professor titular do Departamento de Ciência da Informação da Unesp, Brasil.
chaves.guimaraes@unesp.br

Ricardo César Gonçalves Sant'Ana
Doutor em Ciência da Informação e livre-docente em Sistemas de Informações Gerenciais pela Unesp, Brasil.
ricardo.santana@unesp.br

RESUMO

Com a expansão da internet, fez-se necessária a construção de *frameworks* jurídicos que versem sobre a proteção dos dados pessoais. No Brasil, tem-se a lei n. 13.709, de 14 de agosto de 2018. À vista disso, apresentam-se aqui abordagens que subsidiam o fazer arquivístico relativo a dados dessa natureza.

Palavras-chave: *ciclo de vida dos dados*, *dados pessoais*; *privacidade*; *ética*; LGPD.

ABSTRACT

After the expansion of the internet, it was necessary to build legal frameworks that deal with the protection of personal data. In Brazil, there is the law n. 13.709, of August 14, 2018. In view of this, we present here, approaches that subsidize archival processes related to data of this nature.

Keywords: *data life cycle*; *personal data*; *privacy*; *ethic*; LGPD.

RESUMEN

Con la expansión de la internet, fue necesario construir marcos legales que se ocupen de la protección de datos personales. En Brasil, existe la ley n. 13.709, del 14 de agosto de 2018. En vista de esto, presentamos aquí enfoques que subsidian el trabajo de archivo relativo a datos de esta naturaleza.

Palabras clave: *ciclo de vida de los datos*; *datos personales*; *privacidad*; *ética*; LGPD.

Introdução

Com o surgimento, na década de 1960, da Arpanet (Advanced Research Projects Agency Network), desenvolvida por engenheiros da agência de projetos de pesquisa avançada do Departamento de Defesa dos Estados Unidos (Darpa) para impedir a tomada ou destruição do sistema estadunidense de comunicação, teve início uma rede de comunicação horizontal global, composta por milhares de computadores autônomos abrindo caminho para a internet que, quatro décadas após, ultrapassou trezentos milhões de usuários (Castells, 2009). Esse crescimento exponencial e contínuo é objeto do relatório *Digital 2019: global digital overview*, produzido pela We Are Social e Hootsuite, que apresenta uma análise do desenvolvimento da internet nos últimos anos e da maneira que vem sendo usada pela população global. Segundo a publicação, o número de usuários de internet no mundo saltou de quase 2,5 milhões em 2014 para cerca de 4,4 milhões em 2019, o que representa uma penetração de 57%, ou seja, mais da metade da população global se conecta à rede mundial de computadores (Hootsuite; We Are Social, 2019). Especificamente no Brasil, em janeiro de 2020, cerca de 150 milhões de pessoas utilizaram diariamente a internet. Entre os anos de 2018 e 2019, o Brasil foi o décimo país em que a internet mais cresceu, houve um aumento de 7,2%, o que representa quase dez milhões de pessoas; já entre os anos de 2019 e 2020, o número de usuários cresceu 6%, ou seja, 8,5 milhões de pessoas adquiriram o direito de acesso à rede mundial de computadores. Atualmente, a penetração da internet em solo brasileiro é de 71% da população total do país (Kemp, 2020).

Nesse cenário, ainda, é necessário avaliar o crescimento da internet móvel, essencial em diversos aspectos cotidianos, em um tipo de conexão, fornecida por empresas de telefonia, diretamente atrelada à expansão de dispositivos inteligentes, tais como *smartphones* e *wearables* – pulseiras, relógios, anéis etc. inteligentes. Em 2014 o uso da internet móvel, em termos mundiais, representava 26% do tempo total gasto na internet, passando a 48% em 2019, em uma média diária de seis horas e 42 minutos. Nesse contexto, o Brasil registra uma média diária de nove horas e 29 minutos, ocupando, assim, o segundo lugar no *ranking* mundial, ultrapassado apenas pelas Filipinas (Hootsuite; We Are Social, 2019).

Boa parte desse tempo conectado à internet é gasto em redes sociais on-line, havendo assim uma média global diária de duas horas e 16 minutos, enquanto no Brasil a média é de três horas e 34 minutos, ficando somente atrás das Filipinas (Hootsuite; We Are Social, 2019). Nesse contexto, especial destaque merece o uso das redes sociais, como Instagram, Facebook, Twitter, acessíveis

a 45% da população global. No Brasil, esse índice sobe para 65% da população, com especial destaque para o fato de que, de 2018 para 2019, essas redes angariaram mais de dez milhões de novos usuários (Hootsuite; We Are Social, 2019).

O uso de soluções informatizadas em rede, que se expandiu de forma acelerada e acrítica, possibilitou ao cidadão contemporâneo realizar quase todas as suas tarefas cotidianas de forma conectada – ler notícias, agendar atendimento em repartições públicas, conectar-se com amigos, assistir a filmes e fazer compras on-line. Mais recentemente, com a disseminação dos *smartphones* e dispositivos *wearables*, a produção de dados se intensificou e passou a abranger aspectos mais privados de um indivíduo. Assim, a simples locomoção com um *smartphone* no bolso, ou vestindo um relógio inteligente, pode gerar dados como a quantidade de passos, o caminho percorrido, a frequência cardíaca, a altura, o peso e os locais frequentados.

Essa trilha de dados sobre uma pessoa foi batizada por Westin (1967) como *data shadow*. Segundo Saulles (2015), esses conjuntos de dados podem ser divididos em estruturados e não estruturados, o primeiro originado a partir de transações em que uma das partes é a instituição que coleta os dados, como na compra e venda de uma mercadoria, enquanto o segundo grupo diz respeito a dados produzidos a partir de outros tipos de interação, como e-mails, telefonemas, publicações em redes sociais etc.

Esses dados são objeto de delimitação conceitual em fontes normativas. Assim, a legislação da União Europeia (GDPR) define dados pessoais como

> informação relativa a uma pessoa singular identificada ou identificável. [...] É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização [...] ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular. (European Parliament; Council of the European Union, 2016)

A lei canadense (Pipeda), de forma mais abrangente, define informação pessoal como "qualquer informação factual ou subjetiva, registrada ou não, sobre um indivíduo identificável (Canadá, 2000, tradução nossa). Por sua vez, o relatório produzido pelo World Economic Forum refere-se a

> dados (e metadados) criados por e sobre uma pessoa, compreendendo: dados voluntários: criados e explicitamente compartilhados por indivíduos, exemplo os perfis

> de redes sociais; dados observados: capturados por gravação de ações de um indivíduo, exemplo os dados de localização ao usar celulares; e dados inferidos: dados sobre um indivíduo baseado em análise de terceiros, exemplo o *score* financeiro. (World Economic Forum, 2011, tradução nossa)

No âmbito brasileiro, a lei n. 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais no Brasil, define dados pessoais como "informação relacionada à pessoa natural identificada ou identificável" (Brasil, 2018). O documento vai além ao definir dado pessoal sensível como sendo aquele que trata "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, saúde, vida sexual, genética ou biometria, quando vinculado à pessoa natural" (Brasil, 2018).

É fato que esses dados passaram por um processo de *commoditização*, tornando-se, assim, insumo para diversas atividades econômicas, aspecto destacado por Bauman e Lyon (2012), ao referirem-se àquilo que denominam economia da privacidade, a qual é composta por empresas que possuem seus modelos de negócios voltados à vigilância e que orientam seus negócios e produtos para a coleta e processamento de dados pessoais, estabelecendo uma faceta do capitalismo que se fundamenta no enfraquecimento do direito à privacidade. E é a partir disso que Mayer-Schonberger (2011) afirma que a erosão da privacidade individual é um dos principais desafios a ser enfrentado na contemporaneidade, uma vez que a trilha de ações coletadas torna-se cada vez mais abrangente, registrada e mantida indefinidamente em uma memória digital que pertence a companhias e governos.

Para Saulles (2015), nesse mundo conectado, somos produtores e consumidores de informações, e mesmo que ter seus dados expropriados e receber anúncios não seja uma preocupação para muitos usuários, é crescente uma vertente de pensamento que acredita que estamos dando cada vez mais valor a empresas baseadas em vigilância, tornando-se importante entender que tipo de dados estamos produzindo para essas companhias, quem tem acesso a eles e o que estão fazendo a partir disso.

Essa memória, formulada a partir de dados pessoais coletados das mais variadas formas, somada ao que publicamos em redes sociais e armazenamos na nuvem, ao serem cruzadas e enriquecidas com outras fontes, fornecem uma série de *insights* que podem ser aplicados nas mais variadas áreas e com os mais diversos objetivos. A título de exemplo, profissionais de marketing interessam-se pelo comportamento humano para compreender desejos e tendências

de compra, podendo, assim, adaptar mensagens para corresponder aos interesses de um determinado grupo, otimizando a distribuição de publicidade. Aparentemente inofensiva, essa situação pode causar danos desastrosos quando aplicada, por exemplo, no campo da propaganda política.

Sem leis específicas que regulem o mercado da privacidade, a relação de poder entre o proprietário do dado e os interessados em obter dados continuará sendo desleal e benéfica à segunda parte. A esse respeito, a Conferência das Nações Unidas sobre Comércio e Desenvolvimento (Unctad) reforça que, à medida que mais e mais atividades sociais e econômicas acontecem on-line, a importância da privacidade e da proteção de dados é cada vez mais reconhecida; entretanto, se faz preocupante a coleta, uso e compartilhamento de informações pessoais a terceiros sem aviso prévio ou consentimento dos consumidores (Unctad, 2020). A partir disso, a entidade vem acompanhando a situação global de adoção de legislações para a segurança e proteção de dados e do direito à privacidade, e os resultados são disponibilizados na página Data Protection and Privacy Legislation Worldwide. Em sua última atualização, de 194 países, 128 já adotaram, ou estão em processo de adoção de legislações que contemplam o direito à privacidade e a proteção de dados (Unctad, 2020). Na América Latina, o primeiro país que adotou uma lei dessa natureza foi o Chile em 1999, seguido pela Argentina em 2000, e mais recentemente outros países vêm seguindo a tendência, ao exemplo do Uruguai (2008), México (2010), Peru (2011), Colômbia (2012), Brasil (2018), Barbados (2019) e Panamá (2019) (Rodriguez; Alimonti, 2020).

Especificamente no Brasil, a proteção de dados pessoais é discutida desde 2010, a partir do anteprojeto da Lei de Proteção de Dados Pessoais (ALPDP), aprovado como lei oito anos após. Com esse dispositivo legal, a proteção dos dados pessoais no Brasil, antes apenas tangenciada pela Lei de Acesso à Informação, passou a ser objeto de norma específica – a lei n. 13.709, de 14 de agosto de 2018 –, que dispõe sobre a proteção de dados pessoais e altera a lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Em seu texto, a Lei Geral de Proteção de Dados (LGPD) define como fundamentos: I) o respeito à privacidade; II) a autodeterminação informativa; III) a liberdade de expressão, de informação, de comunicação e de opinião; IV) a inviolabilidade da intimidade, da honra e da imagem; V) o desenvolvimento econômico e tecnológico e a inovação; VI) a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018). O texto também define que a referida lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou jurídica de direito público ou privado, independentemente do meio,

do país de sua sede ou do país onde estejam localizados os dados, desde que: a) a operação de tratamento seja realizada no território nacional; b) 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 c) os dados pessoais objeto de tratamento tenham sido coletados no território nacional (a lei considera coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta) (Brasil, 2018).

Acerca das exceções do que a lei considera tratamento de dados pessoais, configura-se: tratamento realizado por pessoa natural para fins exclusivamente particulares e não econômicos; realizado para fins exclusivamente jornalísticos, artísticos, acadêmicos, de segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais ou proveniente de fora do território nacional e que não seja objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD (Brasil, 2018).

Nesse contexto insere-se também o denominado direito ao esquecimento, que passa a ser atingido – e enfraquecido – pelo fato de que, como destaca Mayer-Schonberger (2011), nossas pegadas eletrônicas deixadas durante o uso da internet em algum momento poderão ser usadas contra nós, dados que são dificilmente apagados. Segundo o referido autor, esses conjuntos de dados constituem uma memória digital, à qual não temos acesso, e apresentam inúmeros desafios do ponto de vista da privacidade, gerando a reflexão sobre o quão ético é o fato de alguma instituição guardar algo que comprometa o presente de uma pessoa (Saulles, 2015).

As discussões contemporâneas sobre privacidade on-line adotam predominantemente uma perspectiva enraizada em teorias liberais que fundamentam a crescente mercantilização da informação e aprofundam a indefinição de público e privado em ambientes de rede. Nesse espectro liberal da privacidade, o foco está na proteção do indivíduo, em que as soluções propostas incluem, mas se limitam ao fortalecimento de conhecimentos e habilidades individuais para autopreservação e à implementação de regulações de proteção à privacidade e dados em nível político (Acquisti, 2013; Greenwald, 2014; Masur, 2020).

Assim, as estruturas sociais calcadas no liberalismo favorecem a mercantilização da informação e apoiam um desequilíbrio entre os atores econômicos e os indivíduos que possuem suas privacidades ameaçadas pela coleta massiva de dados, legitimando e reproduzindo a estrutura de classe capitalista (Fuchs, 2011

apud Masur, 2020). Um exemplo disso são as já citadas redes sociais, que fornecem novos meios de comunicação, mas, ao mesmo tempo, corroem as fronteiras entre público e privado, conceitos tradicionalmente bem delimitados. Nesse sentido, aquela plataforma que oferece uma "configuração de privacidade" para "proteger" o usuário contra os riscos resultantes de seu uso, criando uma falsa ilusão de privacidade, explora e dissemina quantidades enormes de dados pessoais que ferem diretamente diversos direitos correlatos à privacidade (Masur, 2020).

A busca pela privacidade é objeto de preocupação de toda sociedade, levando à necessidade de proteção da autonomia, liberação emocional, autodesenvolvimento e autoavaliação como fundamentais (Masur, 2020), o que levou inúmeras declarações de direitos humanos a reconhecerem o direito à privacidade como fundamental. Paradoxalmente, enquanto em nossas vidas off-line trancamos portas, abaixamos a voz e fechamos cortinas em prol da privacidade, no contexto on-line tal não ocorre, pois privacidade e lucro são inversamente proporcionais: quanto maior for o nível de privacidade, menor é o lucro obtido a partir dos dados capturados (Bartsch; Dienlin, 2016).

Esse acúmulo crescente de conjuntos de dados pessoais apresenta uma série de desafios para os profissionais da informação, especialmente para os arquivistas que, tradicionalmente, têm seu trabalho orientado para o gerenciamento de informações criadas, recebidas e mantidas como evidência e/ou como um ativo por uma organização ou pessoa, em cumprimento de obrigações legais, ou na transação de negócios, ou para seus fins, independentemente do meio, da forma ou formato (ISO 30300, 2011). A adoção dos computadores e o surgimento do banco de dados como documento arquivístico alteraram drasticamente a memória e como ela é administrada, tornando necessário que esses profissionais desenvolvam um novo conjunto de habilidades para poder classificar, organizar e disseminar informações que hoje nem sempre se manifestam nos formatos tradicionais (Le Goff, 1990; Saulles, 2015).

Segundo a LGPD, os papéis e responsabilidades dos envolvidos em um processo de tratamento de dados pessoais são: *titular*, pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; *controlador*, pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; *operador*, pessoa natural ou jurídica, de direito público privado, que realiza o tratamento de dados pessoais em nome do controlador; *encarregado*, pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). No caso dos arquivos, o

desenvolvimento de suas atividades pode fazer com que assumam tanto o papel de controlador, quando lidam com a coleta, armazenamento, recuperação e descarte de dados pessoais que são essenciais para a execução de suas atividades, tais como aqueles que compõem base de dados de usuários, controle de acesso, empréstimo, colaboradores etc.; quanto o papel de operador, quando o arquivo passa a ser responsável pela salvaguarda de dados pessoais capturados a partir do interesse de outra instituição. Ou seja, os dados pessoais em arquivos podem assumir duas características distintas e serem reconhecidos como documentos ou dados de operacionalização das atividades que constituem o cerne do fazer de uma unidade arquivística.

Em suma, pondera-se para o fato de que esse novo paradigma de proteção de dados trouxe consigo a necessidade de adequação de quase todas as áreas que lidam com informação. Especialmente no que diz respeito aos arquivos, que vivem agora uma realidade híbrida, torna-se necessário que a salvaguarda dos dados pessoais seja assumida como princípio fundante no desenvolvimento de produtos e serviços arquivísticos e na atuação dos profissionais da informação.

Portanto, o presente trabalho caracteriza-se como exploratório, uma vez que tem por objetivo gerar familiaridade com as problemáticas sobre privacidade e torná-las mais explícitas, buscando, assim, contribuir para o desenvolvimento da arquivística em relação à proteção de dados. Possui também caráter documental, uma vez que o tema investigado é relativamente novo e carece de maior aprofundamento, portanto, parte do modelo de ciclo de vida dos dados na ciência da informação, proposto por Sant'Ana (2016) e correlaciona-o com abordagens centradas no indivíduo, que podem vir a subsidiar o desenvolvimento de aplicações e serviços que respeitem e propaguem o direito à privacidade e a proteção dos dados pessoais, especialmente em instituições de informação e memória, como os arquivos. O estudo justifica-se pela iminente necessidade de adequação à LGPD que surgiu a partir de sua aprovação, incluindo arquivos e demais unidades de informação.

Abordagens para gestão de dados pessoais centradas no indivíduo

O paradigma de gestão de dados pessoais estabelecido atualmente tem seu foco no acúmulo e processamento irrestrito e pouco claro desses dados ao usuário, o que leva à erosão de direitos fundamentais como a privacidade e o de ser esquecido, tornando, assim, o titular dos dados vulnerável a práticas escusas de companhias e órgãos públicos que se apoiam em dados pessoais para orientar suas atividades. A título de exemplo, em 2016 o serviço de *streaming* musical Spotify

adicionou uma cláusula em seus termos e condições de uso em que possibilitava o acesso da empresa e seus parceiros a informações de cartões de crédito, débito, código postal e histórico de transações bancárias dos usuários, situação essa que fere o sigilo bancário (*Diário de Pernambuco*, 2016).

Esses dados pessoais, por seu valor comercial ou de uso, geralmente não são descartados, ou seja, podem ficar registrados indeterminadamente nas bases de dados de empresas ou governos, afinal, diretrizes sobre temporalidade de dados dificilmente são informadas aos usuários. Entretanto, a LGPD, em seu artigo 15, define que o término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

> i) verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; ii) fim do período de tratamento; iii) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta lei, resguardado o interesse público; ou iv) determinação da autoridade nacional, quando houver violação ao disposto nesta lei. (Brasil, 2018)

Desse modo, busca-se aqui analisar ferramentas da ciência da informação e de outros campos que possam subsidiar as atividades de aplicação de temporalidade aos dados pessoais, visando à manutenção do direito, à privacidade e ao direito de ser esquecido, dos indivíduos que possuem seus dados pessoais salvaguardados por unidades de informação.

Portanto, o ponto inicial da pesquisa estabelece-se a partir do modelo de ciclo de vida dos dados (CDV) para a ciência da informação, proposto por Sant'Ana (2016). Nesse modelo, o CDV é composto por quatro fases, *coleta*, *armazenamento*, *recuperação* e *descarte*, cada uma delas permeadas pelos seguintes fatores transversais: integração, qualidade, direitos autorais, disseminação, preservação e privacidade (Sant'Ana, 2016). Com grande destaque para o fator privacidade, Sant'Ana (2016) ressalta que ele atua de diversas maneiras nas diferentes fases do ciclo de vida dos dados. Na coleta, faz-se necessário identificar, nas fontes utilizadas, aspectos que possam configurar violação da privacidade do titular; no armazenamento, deve-se ter preocupação com questões como quem poderá acessar os dados anteriormente coletados e onde os dados serão armazenados, já que uma base desconectada da rede pode estar mais segura com relação a acessos ou usos indevidos do que uma que esteja armazenada em um servidor de dados conectado à internet; na etapa de recuperação, deve-se considerar os envolvidos com os dados, identificando estruturas e possíveis usuários, lembrando-se de prever a vinculação desses dados com outros, especialmente se forem

dados sensíveis, havendo assim a necessidade de considerar a aplicação de técnicas de anonimização, mesmo que deteriorem o nível de utilidade da base de dados; por fim, no descarte, é preciso atentar para o fato de que um indivíduo pode ter o direito, ou pode vir a ter a necessidade, de excluir seus dados de uma determinada base e garantir o que poderíamos identificar com o conceito do direito ao esquecimento (Sant'Ana, 2016).

Romansky (2015), por sua vez, propõe um modelo de ciclo de vida com ênfase nos dados pessoais. Seu modelo contém sete fases, sendo elas: *coleta*, *preservação*, *utilização*, *atualização*, *transferência/doação*, *arquivamento* e *destruição*. Para o autor, quando se trata de dados pessoais, a *coleta* deve ser feita apenas com base em um motivo legítimo e com consentimento do indivíduo; a *preservação* dos dados tem de ser realizada com base em metas e critérios previamente definidos; a *utilização* deve ser feita por pessoas legítimas com base nos princípios de segurança da informação – autenticação (por meio de nome de usuário, senha, certificado digital, número de identificação pessoal e meio biométrico), autorização (com base no sistema de gestão de direitos digitais desenvolvido) e prestação de contas (personalização do acesso às estruturas de dados e registro das atividades dos usuários); na *atualização*, os dados devem ser corretos, completos e reais (integridade e gerenciamento de conteúdo); a *transferência* para outro país e a doação a outra pessoa devem ser realizadas apenas com base em regras fortes; o *arquivamento* pode ser feito se exigido por lei, mas por um período limitado de tempo; a *destruição* dos dados pessoais deve ser feita após a concretização do objetivo (Romansky, 2015).

Na visão de Romansky (2015), a computação social pode e vem causando diferentes problemas para a privacidade digital, e tais problemas estão baseados nas especificidades das comunicações na internet e na legislação não regulamentada no espaço cibernético. Diante disso, o autor resume algumas questões comuns para a privacidade digital: a) *identificação das funções* – é muito difícil especificar a configuração dos participantes nos processos de processamento de dados pessoais, o que dificulta determinar a responsabilidade pelos procedimentos de proteção de dados; b) *direito do titular dos dados* – impossibilidade de revisar, acessar, bloquear ou excluir os dados pessoais coletados por alguma instituição; c) *transferência internacional de dados* – procedimento típico em computação social, que muitas vezes não é informado ao proprietário dos dados; d) *exclusão dos dados* – se um proprietário solicitar a exclusão de um conjunto de dados, nem sempre terá a certeza de que foram realmente deletados, principalmente porque, a partir da transferência, esses conjuntos podem ser copiados e armazenados em localidades diferentes; e) *compartilhamento de informações*

– os conjuntos de dados pessoais podem ser facilmente compartilhados entre entidades, sendo armazenados, assim, em diferentes locais, nesse caso, dificultando o usuário a identificar quais políticas e medidas são usadas para reagir a eventuais danos; e f) *medidas técnicas e organizacionais* – o controlador tem a obrigação de definir uma política adequada para a proteção de dados pessoais, entretanto, medidas que elevam a segurança reduzem o desempenho do processamento da informação e aumentam o preço do processo, levando a escolhas equivocadas por parte dos controladores (Romansky, 2015).

Outra abordagem que pode auxiliar de maneira transversal na construção de ambientes que respeitem o direito à privacidade e a proteção de dados é o *Privacy by Design* (PbD), desenvolvido na década de 1990 pela comissária de informação e privacidade de Ontário, Canadá, Cavoukian (2006). O conceito busca fornecer bases para que corporações entendam e apliquem regras de privacidade em soluções e produtos oferecidos, freando, assim, a coleta indiscriminada de dados pessoais.

O *Privacy by Design* vem ao longo dos últimos anos sendo adotado em diversas entidades e *frameworks* jurídicos, tais como a Diretiva Geral de Proteção de Dados da União Europeia (GDPR) e nossa Lei Geral de Proteção de Dados (LGPD). A abordagem estrutura-se em sete pilares fundamentais, sendo eles: *proativo, não reativo*; *preventivo, não corretivo* – a abordagem é caracterizada por medidas proativas em vez de reativas. Antecipa e evita eventos invasivos de privacidade antes que aconteçam. No PbD não se espera que os riscos de privacidade se materializem, e sim evita-se que ocorram. Em suma, a privacidade vem antes do fato, não depois; *privacidade como configuração padrão* – o PbD visa oferecer o grau máximo de privacidade sem que nenhuma ação seja necessária por parte do indivíduo, ou seja, as configurações padrões do produto ou serviço levam em conta o maior grau possível de proteção da privacidade; *privacidade incorporada ao design* – o conceito do PbD deve ser incorporado na arquitetura e nas práticas de negócios, não sendo um complemento, tornando, assim, a privacidade um componente essencial do núcleo de funcionalidades que são entregues em um produto ou solução. A privacidade deve ser parte integrante do sistema, sem diminuir funcionalidades; *funcionalidade total: soma positiva, não soma zero* – a abordagem visa acomodar todos os interesses e objetivos legítimos de forma que haja uma soma positiva, ou seja, "ganha-ganha", não por uma abordagem de soma zero, em que compensações desnecessárias são feitas, evitando dessa forma falsas dicotomias, como privacidade *versus* segurança, demonstrando que é possível ter as duas; *segurança ponta a ponta: proteção total do ciclo de vida* – fortes medidas de segurança são essenciais, do início ao fim. Isso

garante que todos os dados sejam retidos com segurança, e destruídos também com segurança ao final do processamento, garantindo, assim, o gerenciamento seguro do ciclo de vida dos dados; *visibilidade e transparência: mantenha aberto* – garantir que todas as partes interessadas, seja qual for a prática do negócio ou tecnologia envolvida, tenham transparência e possam fiscalizar se, de fato, promessas e objetivos declarados são respeitados; e *respeito pela privacidade do usuário: foco no usuário* – acima de tudo, *Privacy by Design* exige que arquitetos e operadores mantenham os interesses do indivíduo em primeiro lugar, oferecendo medidas fortes como padrão de privacidade, aviso apropriado e capacitação amigável (Cavoukian, 2006).

Já em um espectro mais amplo de proteção de dados pessoais centrada no ser humano, tem-se o modelo nórdico *MyData*, cuja abordagem é construída a partir do direito de os indivíduos acessarem e controlarem os dados coletados sobre eles. A iniciativa busca fortalecer os direitos humanos digitais, ao mesmo tempo em que abre novas oportunidades para negócios se desenvolverem com base em dados pessoais, construídos sobre confiança mútua.

A iniciativa *MyData* possui três princípios: 1) *controle centrado no ser humano e privacidade* – indivíduos são atores capacitados, não alvos passivos, na gestão de suas vidas pessoais, tanto on-line quanto off-line; eles têm direito e meios práticos para gerir seus dados e sua privacidade; 2) *dados utilizáveis* – é essencial que os dados pessoais sejam tecnicamente fáceis de serem acessados e utilizados, acessíveis em formatos legíveis por máquina por meio de APIs (*application programming interfaces*) seguras e padronizadas. *MyData* é uma maneira de converter dados de silos fechados num importante recurso reutilizável. Pode ser usado para criar serviços que ajudem os indivíduos a gerir as suas vidas. Os prestadores desses serviços podem criar novos modelos de negócio e crescimento econômico para a sociedade; 3) *ambiente de negócios aberto* – a infraestrutura compartilhada do *MyData* permite gestão descentralizada dos dados pessoais, melhora a interoperabilidade, torna mais fácil o cumprimento dos rigorosos regulamentos de proteção de dados pelas empresas e permite que os indivíduos mudem prestadores de serviços sem *lock-ins* pelos proprietários dos dados (Poikola et al., 2020). Ainda a partir do documento, é formalizado que o termo *MyData* refere-se a:

> a) uma nova abordagem, uma mudança de paradigma no gerenciamento e processamento de dados pessoais que busca transformar a organização atual centrada nos sistemas num sistema centrado no ser humano, b) aos dados pessoais como um recurso que o indivíduo pode acessar e controlar. (Poikola et al., 2020)

Busca-se, com esse modelo, proporcionar aos indivíduos meios práticos para acessar, obter e utilizar *datasets* contendo suas informações pessoais, tais como dados de compra, de tráfego, de telecomunicações, registros médicos, informações financeiras, e dados derivados de diversos serviços on-line, além de encorajar as organizações que detêm os dados a dar aos indivíduos o controle sobre eles, para além dos padrões legais mínimos (Poikola et al., 2020). Além disso, para os autores do documento, os dados pessoais, atualmente, são como uma "matéria-prima bruta", subutilizada para novos serviços devido à falta de interoperabilidade e portabilidade entre *datasets* através de serviços e setores. Desse modo, o modelo *MyData* busca subsidiar o desenvolvimento de uma abordagem em nível de infraestrutura para gerenciamento de dados pessoais que proporciona benefícios para i) *os indivíduos*: fornecendo métodos fáceis de usar e ferramentas abrangentes de gestão de dados pessoais, mecanismos de transparência que mostram abertamente como as organizações utilizam seus dados, além de benefícios relacionados a serviços inovadores e maior liberdade de escolha; ii) *empresas*: a abordagem *MyData* abre oportunidades para novos modelos de negócio com base em dados, facilitando o acesso técnico e jurídico a *datasets* pessoais preexistentes quando o indivíduo está disposto a dar seu consentimento. Sendo fundado em padrões e desenvolvido para promover interoperabilidade, o *MyData* reduz a barreira de entrada para novas empresas e torna a paisagem mais equilibrada e competitiva; e iii) *sociedade civil*: cria estruturas, processos e políticas necessárias à proteção dos direitos dos indivíduos e fomenta o uso de dados pessoais no desenvolvimento de serviços inovadores (Poikola et al., 2020).

A abordagem do *MyData* ocorre em nível de infraestrutura, ou seja, reformula o ecossistema de dados pessoais na camada no mais alto nível. O conceito-chave na infraestrutura proposta é que, para o indivíduo, uma conta *MyData* será como um *hub* único para o gerenciamento de dados pessoais. Através dela, poderá fornecer serviços à autoridade para acessar dados pessoais, gerenciando, assim, as permissões e consentimentos legais para a utilização de seus dados.

A arquitetura proposta baseia-se, segundo seus idealizadores, em contas padronizadas, ou seja, um local que proporcione uma maneira facilitada de controlar seus dados, enquanto eles são criados, armazenados e processados por centenas de serviços diferentes. Dentro desse modelo, os dados são transmitidos de uma fonte para um serviço ou aplicação que os utiliza. Entretanto, a proposta é que a conta *MyData* não seja uma solução de armazenamento de dados pessoais, mas sim uma ferramenta de gestão de consentimento, isto é, o dado em si não é fornecido através dos servidores onde a conta *MyData* estará hospedada (Poikola et al., 2020).

Essa padronização das contas torna possível também que os indivíduos troquem de operadores facilmente, similarmente ao que acontece na gestão de redes

de telefonia móvel. Sendo essa uma das principais vantagens do *MyData*, também se configura como um de seus maiores desafios, afinal, a interoperabilidade e *transferabilidade* global das contas *MyData* entre operadores requer normalização e *design* adicionais, por exemplo, em redes confiáveis, formatos de dados e semântica (Poikola et al., 2020). Por fim, a abordagem *MyData* concentra o desenvolvimento do consentimento usando meta-formato de consentimento aberto (Iniciativa Kantara), o qual é compatível com regulamentos de consentimento que funcionem de maneira transfronteiriça e sejam projetados para operar conjuntamente com a legislação que está sendo adotada pela União Europeia em matéria de proteção de dados (principal fonte de inspiração para a lei geral de proteção de dados brasileira, logo, a abordagem pode corresponder quase que sem necessidade de alteração ao *framework* jurídico de nosso país) (Poikola et al., 2020).

Especificamente no campo da arquivologia, pela necessidade de adequar atividades, serviços e produtos à LGPD, o tema da privacidade e do direito ao esquecimento em contexto vem ganhando visibilidade na ciência da informação. Destacam-se os estudos de Mallet-Poujol (2018), nos quais a autora busca, na perspectiva do direito, da comunicação e da arquivologia, discutir as tensões e os problemas decorrentes do direito de acesso à informação e do direito à vida privada, problematizando a questão do direito ao esquecimento nas suas diferentes dimensões e modalidades operacionais no mundo digital; de Schwaitzer (2020), que tem por objetivo identificar os impactos mais relevantes da LGPD nas atividades de arquivos e centros de memória, enfatizando a importância de se receberem itens com regras claras quanto à restrição de acesso e de se criarem e se divulgarem políticas de acesso e de privacidade; e de Rockembach (2020), em que são abordadas questões ético-legais no desenvolvimento de estudos de usuários de arquivos a partir do uso de dados pessoais. Entretanto, a produção científica em ciência da informação em relação ao tema ainda é baixa. Em uma pesquisa realizada na data de 22 de junho de 2021, na Base de Dados em Ciência da Informação (Brapci) a partir da expressão "LGPD and arquiv*", foram obtidos somente dois resultados, e a partir da expressão "proteção de dad* and arquiv*" foram recuperados oito itens. Situação essa que pode decorrer do fato da LGPD ter entrado em vigor parcialmente em setembro de 2020; a partir de agosto de 2021 sanções serão aplicadas em casos de descumprimento da LGPD.

Discussão

À vista do exposto, pode-se dizer que essa "memória digital perfeita", que vem sendo criada a partir do enfraquecimento dos direitos relacionados à

privacidade, é antinatural, uma vez que o cérebro humano tende a selecionar, reconfigurar e reordenar memórias em que as pessoas manipulam conscientemente seus passados, destroem fotos, queimam diários etc. Esquecer não é apenas um comportamento individual, pois também esquecemos como sociedade e, nesse segundo caso, o esquecimento social dá a indivíduos que falharam em algum aspecto uma segunda chance, possibilitando que, através do apagamento de memórias externas, a sociedade possa aceitar que os seres humanos evoluem com o tempo e que temos a capacidade de aprender com experiências passadas e ajustar nossos comportamentos (Van Dijck, 2007; Mayer-Schonberger, 2011). Assim, um futuro baseado em uma "memória perfeita", que possa julgar e condenar o presente através da análise do passado, parece cada vez mais factível, uma vez que a tecnologia facilita o fim do esquecimento. No entanto, vale recordar que isso só ocorrerá efetivamente se a vontade humana assim o quiser, pois toda e qualquer memória eletrônica só age sob a ordem segundo o programa do homem, sendo senão um auxiliar, um servidor da memória e do espírito humano. Somos, portanto, os únicos responsáveis pelo desaparecimento do esquecimento, e cabe a nós revertermos essa mudança (Le Goff, 1990; Mayer-Schonberger, 2011).

Vale recordar que essa discussão traz consigo uma vertente eminentemente ética no que tange ao *métier* dos arquivistas, na qualidade de profissionais da informação, na atualidade, na medida em que o respeito e a preservação da privacidade passam a ser um valor profissional em si mesmo. Desse modo, se antes o *ethos* dessa categoria profissional residia fundamentalmente na preservação, sob as dimensões física e testemunhal/probatória de um conjunto documental, hoje o conceito de preservação se amplia para abarcar a proteção da integridade de conteúdo, envolvendo, por sua vez, a questão da segurança e, em última análise, refletindo uma responsabilidade social (Giménez-Chornet, 2017).

No que tange à segurança da informação, o tema vem sendo discutido há mais de uma década como um valor ético inerente à atuação de arquivistas, especialmente em tempos de informação digital. Mais especificamente à questão da violação de privacidade (decorrente de falha nessa segurança), em aspectos relativos, entre outros, à vigilância, ao monitoramento, rastreamento e censura, tem-se uma séria evidência de como as unidades ou sistemas de informação estão suscetíveis, ainda que de forma culposa, por negligência, imprudência ou imperícia, a promover a violação de direitos (Guimarães, 2008; Sant'Ana, 2016)

Tudo isso leva a se considerarem as abordagens aqui apresentadas, tal como o ciclo de vida dos dados, o ciclo de vida dos dados pessoais, e as abordagens *MyData* e *Privacy by Design* (Cavoukian, 2006; Romanksy, 2015; Sant'Ana, 2016;

Poikola et al., 2020). Afinal, é a partir de modelos e propostas dessa natureza que será possível frear essa incursão contra a privacidade, um dos principais problemas da sociedade contemporânea, que diversas áreas vêm estudando.

Portanto, aponta-se, com vista no exposto, que as dinâmicas das instituições da informação relativamente à questão dos dados pessoais poderiam se pautar em uma estrutura que tivesse a privacidade, a visibilidade e a transparência, além do foco no indivíduo, como fatores transversais das etapas do ciclo de vida dos dados pessoais proposto por Sant'Ana (2016). São as etapas do CDV:

a) *coleta*: fase em que os dados pessoais são capturados, em ambiente digital ou físico, de maneira manual ou automatizada. A atividade de coleta deve ser fundamentada por princípios éticos como motivo legítimo, consentimento do titular (ou responsável legal), metodologia de coleta e tipologia dos dados especificadas e publicizadas ao titular no momento da adesão ao serviço ou produto;

b) *armazenamento*: a unidade de informação deve salvaguardar os dados pessoais por um período limitado, ou seja, até a concretização dos objetivos manifestos no início da coleta. Os dados pessoais devem ser armazenados em ambiente seguro, com metas e critérios bem definidos de preservação, anonimizados e criptografados. Essa fase também se interliga com a atualização dos dados armazenados pela instituição, e esses dados devem passar por atualizações periodicamente, de modo a estarem sempre completos, corretos e reais;

c) *recuperação*: nessa fase ocorre o manuseio dos dados pessoais, por humanos ou sistemas informatizados. Essa atividade deve ser realizada mediante autorização e levar em conta ferramentas de autenticação que possam gerar trilhas e *logs* detalhados que subsidiem a prestação de contas aos titulares;

d) *descarte*: por fim, na fase final ocorre a destruição dos dados, pelo cumprimento do objetivo ou mediante solicitação do titular. Pode também ocorrer a transferência para outra instituição, por necessidade institucional ou também por solicitação do usuário, nesse caso, deve-se levar em conta aspectos como regras fortes para garantir uma transferência segura e a integridade dos dados, políticas institucionais do recebedor devem ser equivalentes em grau de proteção e a transferência deve ser devidamente informada ao titular.

Essa dinâmica traduz-se visualmente na Figura 1, a seguir:

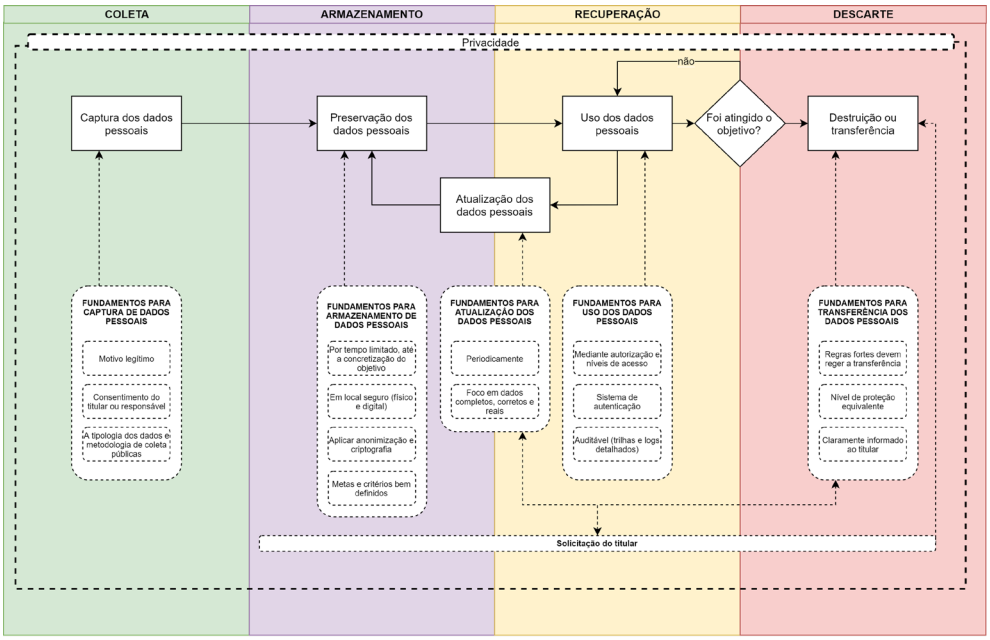

Figura 1 – Dinâmica do ciclo de vida dos dados pessoais com ênfase em privacidade. Fonte: adaptado de Cavoukian (2006), Romansky (2015), Sant'Ana (2016), Brasil (2018) e Poikola et al. (2020).

A dinâmica proposta acima pode ser publicizada a partir de um documento que contemple as políticas de privacidade do produto ou serviço prestado pela unidade de informação. O Serviço Federal de Processamento de Dados (Serpro), empresa pública brasileira de prestação de serviços em tecnologia da informação, oferece orientações acerca de como desenvolver uma política de privacidade aderente à LGPD. As sugestões do Serpro são oferecidas levando-se em conta três aspectos.

1) Antes da elaboração:

> Nessa etapa é fundamental entender o contexto do tratamento de dados pessoais e como os princípios da LGPD são atendidos no sistema ou serviço, para tanto, é necessário mapear todos os dados pessoais, a finalidade, as bases legais que legitimam o tratamento e a forma de atendimento aos direitos do titular como acesso, retificação, exclusão, revogação de consentimento, oposição, informação sobre possíveis compartilhamentos com terceiros e portabilidade. (Freitas, 2019)

2) Conteúdo da política da privacidade:

> É importante observar a presença das seguintes informações que devem estar de modo claro e preciso: informações sobre a organização responsável pelo tratamento; dados pessoais e respectivas finalidades do tratamento, inclusive os dados não informados pelo usuário (exemplo: IP, localização etc.); base jurídica do tratamento; prazo de retenção dos dados pessoais; informações de contato do *Data Protection Officer* (DPO) ou encarregado de proteção de dados da organização. [...] também deve orientar como são atendidos os direitos do titular de dados pessoais, apresentando como ele pode acessar, retificar, solicitar a exclusão de dados, transferir, limitar ou se opor ao tratamento, e retirar o consentimento. [...] quando aplicáveis, também devem estar presentes: sobre compartilhamento dos dados com terceiros e qual a finalidade, inclusive redes sociais; sobre transferência internacional e qual a finalidade; sobre o tratamento por legítimo interesse; sobre o envio de e-mail marketing e como remover o consentimento, quando autorizado inicialmente pelo titular; sobre decisões automatizadas; sobre a proteção de dados de menores de idade; sobre a proteção dos dados sensíveis. (Serpro, 2019)

3) Após a elaboração:

> A política de privacidade deve estar disponível ao titular dos dados antes do início do tratamento do dado pessoal dele, permitindo, quando aplicável, que o mesmo avalie os termos do site ou serviço. É importante garantir que a política esteja facilmente disponível, em uma linguagem apropriada ao seu público-alvo e com o conteúdo suficiente, claro e preciso para declarar todas as informações necessárias. [...] E o usuário deve demonstrar seu expresso consentimento e concordância com os termos da política antes do início do tratamento. [...] Colocar versão e a data de atualização da política de privacidade, com um registro das principais alterações, quando aplicável, além de disponibilizar um repositório com as versões anteriores ao público-alvo e também em um sistema interno de controle de políticas. (Serpro, 2019)

Com isso, a política de privacidade assume papel importante no que diz respeito à adesão das unidades de informação (ou qualquer outro tipo de instituição) quanto a se posicionarem como entidades que praticam e fomentam a proteção dos dados pessoais, elevando a privacidade a um princípio fundante para o desenvolvimento de suas atividades. Entretanto, tal documento deve traduzir práticas e dinâmicas reais de proteção de dados, que podem desenvolver-se a partir do modelo proposto na Figura 1.

Conclusão

Pela necessidade de adequação à LGPD, o estudo aqui apresentado teve por objetivo gerar familiaridade com as problemáticas sobre privacidade e torná-las mais explícitas à comunidade arquivística e da ciência da informação, buscando, assim, contribuir para o desenvolvimento da área em relação à proteção de dados. Desse modo, o presente trabalho buscou apresentar abordagens que auxiliem no desenvolvimento de políticas, serviços e soluções em arquivos, bibliotecas e museus, visto que esses espaços, cada vez mais, encontram-se envolvidos com a questão dos dados pessoais, especialmente com o seu gerenciamento.

Propôs-se também a utilização de uma dinâmica do ciclo de vida dos dados pessoais com ênfase em privacidade, que leva em conta fundamentos éticos e legais que permeiam as fases de coleta, armazenamento, recuperação e descarte desses dados em um contexto híbrido, no qual o processamento pode acontecer em ambiente físico ou digital. Por fim, foram apresentadas as políticas de privacidade como um documento a ser desenvolvido e utilizado nas unidades de informação, sendo que nele deve ser explicitado como a instituição garante um tratamento de dados pessoais adequado à LGPD e que leve em conta a proteção da privacidade de seus usuários.

Referências

ACQUISTI, A. *The economics of privacy*: theoretical and empirical aspects, 2013.

BARTSCH, M.; DIENLIN, T. Control your Facebook: an analysis of on-line privacy literacy. *Computers in Human Behavior*, v. 56, p. 147-154, 2016.

BAUMAN, Z.; LYON, D. *Liquid surveillance*: a conversation. Cambridge: Polity, 2012.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

CANADÁ. The personal information protection and electronic documents act (Pipeda), 2000. Disponível em: https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf. Acesso em: 11 jul. 2020.

CASTELLS, M. *The rise of the network society*. 2. ed. Oxford: Wiley-Blackwell, 2009.

CAVOUKIAN, A. *Privacy by Design*: the 7 foundational principles. Ontario, Canada: Information & Privacy Commissioner, 2006. Disponível em: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf. Acesso em: 11 jul. 2020.

DIÁRIO DE PERNAMBUCO. *Nova política do Spotify exige dos usuários a abertura do sigilo bancário*. Disponível em: https://www.diariodepernambuco.com.br/noticia/viver/2016/12/nova-politica-do-spotify-exige-dos-usuarios-a-abertura-do-sigilo-banca.html. Acesso em: 28 jun. 2021.

EUROPEAN PARLIAMENT; COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2016-679. Brussel, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 28 jul. 2019.

FREITAS, Carla. *Como elaborar uma política de privacidade aderente à LGPD?* Disponível em: https://www.serpro.gov.br/lgpd/noticias/2019/elabora-politica-privacidade-aderente-lgpd-dados-pessoais. Acesso

em: 23 jun. 2021.

GIMÉNEZ-CHORNET, V. Ethics and social responsibility in archival institutions: elements to consider. *El Profesional de la Información*, v. 26, n. 4, p. 765, 2 ago. 2017.

GREENWALD, GLENN. *No place to hide*: Edward Snowden, the NSA, and the U.S. Surveillance State. New York: Metropolitan Books, 2014.

GUIMARÃES, J. A. C. A dimensão teórica do tratamento temático da informação e suas interlocuções com o universo científico da International Society for Knowledge Organization (Isko). *Revista Ibero-americana de Ciência da Informação*, v. 1, p. 77-79, 2008.

HOOTSUITE; WE ARE SOCIAL. *Digital 2019*: global digital overview. [s.l: s.n.]. Disponível em: https://datareportal.com/reports/digital-2019-global-digital-overview. Acesso em: 28 jul. 2019.

ISO 30300. *Information and documentation*: records management. International Organization for Standardization, 2011.

KEMP, S. *Digital 2020*: Brazil. Datareportal, 2020. Disponível em: https://datareportal.com/reports/digital-2020-brazil. Acesso em: 20 jul. 2020.

LE GOFF, J. *História e memória*. Campinas, SP: Editora da Unicamp, 1990.

MALLET-POUJOL, N. Internet e o direito ao esquecimento digital. *Revista Ibero-americana de Ciência da Informação*, v. 12, n. 1, p. 145-170, 10 set. 2018.

MASUR, P. K. How on-line privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, v. 8, n. 2, p. 258-269, 2020.

MAYER-SCHONBERGER, V. Delete: the virtue of forgetting in the digital age. In: *The demise of forgetting - and its drivers*. 4. ed. Princeton: Princeton University Press, 2011.

POIKOLA, A.; KUIKKANIEMI, K.; HONKO, H. *MyData*: um modelo nórdico para gestão e processamento de dados pessoais centrado no ser humano. Rio de Janeiro, 2020. Disponível em: https://internet-governance.fgv.br/sites/internet-governance.fgv.br/files/publicacoes/selection_novo.pdf. Acesso em: 29 jan. 2021.

ROCKEMBACH, M. Estudos de usuários de arquivo e os desafios da Lei Geral de Proteção de Dados. Revista *Acervo*, v. 33, p. 102-115, 2020.

RODRIGUEZ, K.; ALIMONTI, V. *Un panorama retrospectivo y futuro de la protección de datos en América Latina y España*. 21 set. 2020. Disponível em: https://www.eff.org/es/deeplinks/2020/09/look-back-and-ahead-data-protection-latin-america-and-spain. Acesso em: 29 jan. 2021.

ROMANSKY, R. Social computing and digital privacy. *Communication & Cognition*, v. 48, p. 65-82, 1 nov. 2015.

SANT'ANA, R. C. G. Ciclo de vida dos dados: uma perspectiva a partir da ciência da informação. *Informação & Informação*, v. 21, n. 2, p. 116, 20 dez. 2016.

SAULLES, M. DE. *Information 2.0*: new models of information production, distribution and consumption. v. 2. London: Facet, 2015.

SCHWAITZER, L. S. LGPD e acervos históricos. *Archeion Online*, v. 8, n. 2, p. 36-51, 28 dez. 2020.

UNCTAD. Data Protection and Privacy Legislation Worldwide. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em: 28 jan. 2021.

VAN DIJCK, J. *Mediated memories in the digital age*. Stanford: Stanford University Press, 2007.

WESTIN, A. *Privacy and freedom*. Nova Iorque: Ig Publishing, 1967.

WORLD ECONOMIC FORUM. *Personal data*: the emergence of a new asset class. Geneva, 2011. Disponível em: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf. Acesso em: 28 jan. 2021.

Recebido em 31/1/2021
Aprovado em 16/6/2021