EMPODERAMENTO DIGITAL, PROTEÇÃO DE DADOS E LGPD[1]

E-mail:
danielbeltran@gmail.com
adrianacarla.a@gmail.com
josemarhenrique@gmail.com
arquivista.saopaio@gmail.com

Adriana Carla Silva de Oliveira[2], Daniel Beltran Motta[3], Josemar Henrique de Melo[4], Rita de Cássia São Paio de Azeredo Esteves[5]

RESUMO

O presente artigo baseado na Mesa Redonda sobre Empoderando Digital, Proteção de Dados e a Lei Geral de Proteção de Dados, proferida pelos palestrantes: Adriana Carla Silva de Oliveira, Doutora em Ciência da Informação pela UFPB e por Daniel Beltran Motta, especialista em Gestão e Compliance e arquivista da Eletrobrás com a mediação de Josemar Henrique de Melo, Doutor em Documentação pela Faculdade de Letras da Universidade do Porto. Esta mesa redonda aconteceu como parte da 4ª Semana Nacional de Arquivo (SNA) promovida pelo Grupo de Estudos Arquivísticos (GEarq) e está disponível em sua página no Youtube. O evento ocorreu no dia 8 de junho com transmissão ao vivo e os questionamentos dos participantes foram apresentados online.

Palavras-chave: LGPD. Proteção de Dados. Acesso à Informação. Transformação Digital.

ABSTRACT

This article based on the Roundtable on Digital Empowerment, Data Protection and the General Data Protection Law, given by the speakers: Adriana Carla Silva de Oliveira, PhD in Information Science at UFPB and by Daniel Beltran Motta, specialist in Management and Compliance and archivist of Eletrobrás, with the mediation of Josemar Henrique de Melo, PhD in Information Science Doutor em Documentação pela Faculdade de Letras da Universidade do Porto. This roundtable took place as part of the 4th National Week of Archives (SNA) promoted by the Archival Studies Group (GEarq) and is available on its page on Youtube. The event took place on June 8 with live transmission and the participants' questions were presented online.

Keywords: LGPD. Data Protection. Access to information. Digital Transformation.

[1] Memória Cientifica da 4ª Semana Nacional de Arquivos – Paraíba.

[2] Doutora em Ciência da Informação e Pós-doutorado em Direito, Mestra em Engenharia de Produção, MBA em Gestão empresarial e Bacharelado em Direito e Biblioteconomia. http://orcid.org/0000-0001-7653-0022

[3] Graduado em Arquivologia pela UNIRIO e graduado em Gestão Pública. MBA em Gestão de Riscos e Compliance. Data Protection Officer – DPO da Eletrobras. https://orcid.org/0000-0002-6152-3601

[4] Doutor em Documentação pela Faculdade de Letras da Universidade do Porto. Mestre em Ciência da Informação pela Universidade Federal da Paraíba e atualmente é professor Doutor no Curso de Bacharelado em Arquivologia da Universidade Estadual da Paraíba. http://orcid.org/0000-0002-8586-518X

[5] Especialista em Administração da Qualidade – Universidade Federal do Ceará. Graduada em Arquivologia - Universidade Federal Fluminense. https://orcid.org/0000-0003-3597-7543

INTRODUÇÃO

A Semana Nacional de Arquivos (SNA), prevista no Plano Setorial de Arquivos por iniciativa do Colegiado Setorial de Arquivos, do Conselho Nacional de Política Cultural (CNPC), promovida anualmente pelo Arquivo Nacional e Fundação Casa de Rui Barbosa desde 2017, consiste em uma temporada de eventos realizados em todo o país para aproximar os arquivos da sociedade. Em sua 4ª edição, ocorrida no período de 08 a 14 de junho de 2020, a programação da SNA foi realizada apenas com eventos virtuais, em atendimento às orientações das autoridades de saúde devido ao período de pandemia do novo Coronavírus (COVID-19).

No Estado da Paraíba, o Grupo de Estudos Arquivísticos (GEarq) convidou profissionais de arquivo de instituições de memória, órgãos públicos federais, estaduais e municipais, bem como professores das universidades que oferecem o curso de Arquivologia no Estado, para promoveram um calendário único de eventos. A Mesa Redonda "Empoderamento Digital, Proteção de Dados e LGPD" integrou a programação da 4ª. Semana Nacional de Arquivos, disponibilizada na página do Arquivo Nacional. O canal do Grupo de Estudos Arquivísticos (GEarq), na plataforma YouTube, realizou a transmissão e gravação que possui, até o término da escrita deste texto, cerca de 587 visualizações e pode ser assistida no seguinte endereço eletrônico: https://www.youtube.com/watch?v=FDh0RUZnaRw&t=476s.

2 PRIVACIDADE E PROTEÇÃO DE DADOS NA SOCIEDADE DO CONHECIMENTO

No momento propício de adaptação em que vivemos o digital intensamente, torna-se necessário o debate com mais informações a respeito da nova forma de atuação dentro da vida pessoal e profissional, numa intercessão de diferentes áreas por meio de uma ponte com a Arquivologia vindo da Biblioteconomia, conversando com a Ciência da Informação, transversalmente ao Direito.

Para falar de Lei Geral de Proteção de Dados (LGPD) é importante entender o contexto que antecede a lei. Como o tema geral da 4ª Semana Nacional de Arquivos é "Empoderando a Sociedade do Conhecimento", é importante entender o *status quo* da nossa sociedade e conhecer de onde vem essa ideia de privacidade e de empoderamento digital numa sociedade em que tanto se fala de empoderamento feminino, das desigualdades e qual a intercessão com a sociedade do conhecimento.

Para situar um pouco o tema é imprescindível fazer um passeio pelo contexto doutrinário, teórico e conceitual de Sociedade do Conhecimento, de Transformação Digital, do Empoderamento Digital, até chegar ao Direito à Privacidade e à Intimidade, Proteção de Dados Pessoais e finalmente LGPD, para entendermos minimamente esse ecossistema que estamos vivendo para saber porque a referida lei é tão importante, podendo ser vista como vilã como mais uma lei no nosso universo que veio para burocratizar enquanto a ideia é descontruir ou construir uma nova visão a partir de como nós podemos nos apropriar.

Por meio de uma distinção teórica de abordagem da Sociedade do Conhecimento defendendo a importância da informação, como um bem comum, bem social. De acordo com a pesquisa, Adriana trabalhou o contexto do conhecimento como bem comum que ajuda a fazer um processo de transformação na sociedade. Mais do que nunca precisamos da divulgação de informações acerca do que estamos vivendo atualmente com relação a pandemia de COVID-19, o quão importante é cada informação publicizada pelos meios de comunicação em prol de um bem

social, para todos, para o bem comum e tem o propósito de direcionar ações que apontam para o desenvolvimento de políticas públicas que primam pela liberdade e acesso à informação e pelo fomento da comunicação e da tomada de decisão pelo cidadão comum, que precisa ser o protagonista desse processo.

A inclusão digital, inclusive do governo, não pode ser uma opção, é preciso ser realidade para o desenvolvimento da Sociedade do Conhecimento. Nós vivemos um processo, que se acelerou nos últimos meses, de transformação digital. Num contexto de mundo, já existem muitos países transformados digitalmente, a exemplo da Estônia, que apesar de ser um país muito pequeno, já é totalmente digitalizado. No Brasil já existe um contexto de governo aberto, a partir da implantação da Lei de Acesso à Informação (LAI) e hoje estamos vivendo um processo de transformação digital, algumas empresas mais outras menos, as instituições públicas talvez mais atrasadas, mesmo sem saber até onde ele está avançado e maturado, mas já vivemos a desmaterialização de documentos, a desmonetização em bancos, a exemplo do Nubank, de mais intangibilidade, de democratização, apesar de nem tudo ser tão democrático e também de disrupção, com tecnologias disruptivas, a exemplo da Inteligência Artificial, que já permeou a base da nossa infraestrutura organizacional e de empresas.

A *Digital Empowerment Foundation,* na Índia, trabalha com a capacitação digital, nesse ecossistema que gera o bem comum ao trazer um processo de transformação digital para uma sociedade do conhecimento. Ao capacitar pessoas digitalmente, com alfabetização digital, ferramentas digitais e conectividade, comunidades marginalizadas que vivem em atraso socioeconômico e pobreza de informação podem ser capacitadas para melhorar suas vidas por conta própria, simplesmente fornecendo acesso as informações.

Na realidade brasileira, hoje, quantas pessoas estão na fila para receber o Auxílio Emergencial porque não conseguem baixar um aplicativo ou porque não têm acesso à Internet. Podemos ter grandes ferramentas digitais, mas ainda assim teremos problemas pela falta de políticas públicas que ataquem um processo de alfabetização digital e de conectividade.

Nessa direção entende-se por empoderamento digital:

- Parte do princípio de que o indivíduo deve ter autonomia e liberdade;
- É necessário desenvolver no cidadão as habilidades digitais para lidar com a competitividade, o empreendedorismo, a transformação digital, as novas oportunidades e as aprendizagens advindas desse mundo digital;
- Desenvolver uma nova mentalidade no cidadão para uma consciência digital transformadora;
- Incorporar a transformação digital, tais como a Indústria 4.0, Justiça Aberta, Tecnologias Disruptivas no contexto das organizações e como forma de engajamento social;
- Proporcionar o empoderamento social e cívico aliado ao digital, sempre em busca de um propósito e bem comum;
- Tornar o cidadão/usuário/cliente protagonista de nossas demandas;
- Promover as condições para o acesso à informação e a garantia de segurança jurídica ao cidadão;
- Estimular o uso ético, consciente e cidadão da tecnologia, da informação e dos dados tanto pelas organizações como pelo próprio cidadão.

Portanto, o empoderamento digital pressupõe o engajamento em Processos, Pessoas e Tecnologias, tendo o Cidadão no foco**.**

Outro exemplo é a dificuldade do trabalho em regime de "*home office*" porque ainda não possuímos todas as habilidades digitais para usarmos tantas ferramentas tecnológicas ao mesmo tempo e nossa infraestrutura ao redor também não está acomodada, aprendizagens para usar a ferramenta que melhor se adequa a cada situação, num processo muito complexo que traz a necessidade do profissional da informação cujo núcleo de trabalho é a informação representada hoje por dados e por todo esse arcabouço documental.

Mais do que nunca precisamos ter essa consciência digital transformadora para lidar com essa transformação digital de indústria 4.0, tecnologias disruptivas, de ter um papel ativo e consciente de como o empoderamento digital e a tecnologia transformam e afetam o dia a dia e a vida das pessoas no campo pessoal e profissional.

Todo processo de transformação tem um propósito e se o profissional da informação está trazendo para o público, para o cidadão, para o usuário, o melhor que pode fazer, então estará atingindo o bem comum, mas precisa garantir que o empoderamento seja social e cívico, que tenha em mente um impacto na comunidade, mas que precisa transformar, começando a mudar nossa consciência transformadora.

O empoderamento digital institucional precisa trazer o cidadão para nossa demanda, o que já é muito recorrente para a área de profissional da informação, sendo cada vez mais necessário o diálogo multidisciplinar, tendo a estratégia de pensar o cidadão como foco, ampliando a visão de cidadão para cliente, consumidor, pois não adianta ter o melhor recurso tecnológico de recuperação e de curadoria dos documentos se não alcança a demanda do cidadão, além de promover o acesso, deve também trazer a segurança jurídica para o cidadão.

Hoje o debate é para começar a entender as normativas que trazem o mínimo de segurança jurídica para o cidadão, além de estimular mais do que nunca o uso ético e consciente das informações e dos dados que geramos, tratamos e compartilhamos.

Para situar numa linha do tempo as questões de privacidade dentro do ramo jurídico, o Direito à Privacidade é considerado um direito fundamental que faz parte do rol de direitos de personalidade e as discussões no mundo remontam a 1800, mostrando que não é nada novo ao contexto de violação de tais direitos, a exemplo do direito a vida ou ao direito a liberdade. Mas de forma histórica a partir de 1970, ou seja, 50 anos atrás, é que começaram a surgir de forma mais robusta as legislações acerca do Direito à Privacidade e de proteção de dados.

Na Europa, em especial na Alemanha, Dinamarca e até mesmo nos Estados Unidos trouxeram as primeiras legislações a partir da década de 70 e no Brasil, esse direito foi implementado de forma mais clara na Constituição de 1988 e agora mais recentemente a partir de 2018.

O Direito à Privacidade está entre a dicotomia das esferas pública e privada de forma a criar uma proteção para resguardar a dignidade da pessoa humana. Na teoria jurídica a proteção ao segredo, à intimidade e à vida privada são delimitados entre os espaços da vida privada e pública e nesse rol entra a questão dos dados pessoais, ou seja, o direito de acesso aos meus dados e as minhas informações pessoais só mediante permissão expressa do titular. É a mesma comparação com a privacidade da nossa casa de quando fechamos a nossa porta, delimitamos a vida privada e só permitimos que alguém adentre na nossa casa se nós quisermos, usando a mesma analogia para dados pessoais.

O Direito à Privacidade faz parte do rol do direito da pessoa humana, no escopo de direito de personalidade e a lei prevê que é inviolável a nossa vida privada, a honra, a intimidade e a imagem, assegurando tanto indenização material como moral em relação à violação, mas isso

ainda não é suficiente para assegurar num mundo tão digital como o que já vivemos hoje, a segurança jurídica ao cidadão.

O mapa a seguir demonstra o quão importante é esse debate acerca da privacidade, do monitoramento, da violação, e da proteção a partir dos níveis de regulação mundialmente.

A Figura 1 apresenta um panorama sobre as normativas dos países que já possuem seus regulamentos de privacidade, além de demonstrar os níveis de proteção e monitoramento.

Por meio de uma implantação efetiva da lei de proteção de dados pessoais e de sua relevância é possível perceber que alguns países já possuem regras que oferecem alta proteção de dados. Como também é visível que os países que estão com círculos pretos, demonstram baixa proteção e alto monitoramento que afeta diretamente a privacidade do cidadão, como é o caso da China, Singapura, Taiwan, onde recentemente observamos violações à privacidade de dados pessoais e dados sensíveis.

Figura 1 – Infográfico

Fonte: Estadão (2015, p.1)

No Brasil o direito a proteção de dados está previsto na Lei nº 13709/2018, de 14 de agosto de 2018, que disciplina o tratamento de dados pessoais no cenário nacional e a Lei nº 13.853/2019, de 08 de julho de 2019, que trouxe uma atualização de alguns artigos e de acréscimo à lei anterior para a criação da Autoridade Nacional de Proteção de Dados (ANPD), que foi criada, mas ainda não foi institucionalizada e ainda não está em funcionamento. E recentemente, a promulgação da Lei nº 14.010, de 10 de junho de 2020 que traz o adiamento das sanções e multas referentes a aplicação da LGPD para agosto de 2021. A previsão é que a LGPD entre em vigor em 14 de agosto de 2020, porém já houve vários Projetos de Lei (PL) para seu adiamento e, recentemente temos a Medida Provisória nº 959/2020 que prevê apenas a implantação da Lei para maio de 2021.

Porém, antes da promulgação da LGPD, o Brasil possui um rol de legislações que trouxeram mudanças significativas no rol de legislações específicas e segurança jurídica. Os marcos legais que antecederam a promulgação da LGPD, bem como as discussões advindas nos últimos 10 anos já demonstram que no Brasil, apesar de um atraso de mais de 40 anos em relação ao cenário internacional, demonstra uma maturidade legal acerca da privacidade e da proteção de dados pessoais.

São inúmeros os marcos legais que se apresentam no processo de construção da LGPD durante os últimos 10 anos. Transversalmente, observa-se que a Lei de Acesso à Informação (LAI)

foi um grande marco legal para a transparência pública e a prestação de contas por parte do governo para a sociedade, o que nos leva a perceber um empoderamento do cidadão em busca de seus direitos de acesso à informação.

Além disso, vemos também outras legislações específicas, a exemplo da Lei Carolina Dieckmann com previsão legal e alteração no Código Penal e o Marco Civil da Internet que combate as violações e os crimes cibernéticos. Dessa forma, percebemos que não há ausência de leis que discipline o tratamento de dados e informações, além de coibição de crimes, mas de sua efetividade e adequação nas organizações, no âmbito público e privado.

Então, após compreendermos o percurso histórico e o arcabouço legal que antecedeu a promulgação da LGPD, apresento breves comentários acerca do escopo de aplicação.

O Quadro 1 apresenta os 10 princípios norteadores da LGPD que são de suma importância para compreendermos os aspectos epistemológicos da referida lei. Muito embora não seja o foco da minha fala neste painel, gostaria de ressaltar a importância desses princípios para a aplicabilidade da lei.

Quadro 1 – Resumo Princípios Norteadores da LGPD

Finalidade	Propósitos legítimos, específicos, explícitos e informados.
Adequação	Compatibilidade do tratamento com as finalidades.
Necessidade	Utilização de dados estritamente necessários.
Livre Acesso	Acesso ao tratamento e à integralidade dos dados.
Qualidade dos Dados	Dados exatos, claros, relevantes e atualizados.
Transparência	Informações claras, precisas e facilmente acessíveis.
Segurança	Medidas técnicas e administrativas aptas a proteger os dados pessoais.
Prevenção	Adoção de medidas para prevenir danos aos titulares.
Não Discriminação	Não utilização para fins discriminatórios ilícitos ou abusivos.
Responsabilização e Prestação de Contas	Demonstração da adoção de medidas eficazes ao cumprimento das normas.

Fonte: Elaborado pelos autores, 2020 - Adaptação Artigo 6º da LGPD (2018, p.4)

Cada princípio norteador apresentado possui um escopo de aplicação que empresas e instituições públicas devem atender quando estiverem realizando seus projetos de conformidade à lei. Cada um está representado por uma ideia de que o órgão ou empresa deverá obedecer para um tratamento adequado dos dados pessoais e evitar ou reduzir as possibilidades de violação dos mesmos.

Dessa forma, é importantíssimo entender cada princípio em sua compreensão epistemológica, além de perceber que dependendo da natureza dos dados pessoais, alguns princípios são norteadores para o tratamento, individualmente ou agrupados entre si. Contudo, devido ao tempo exíguo da minha fala, não irei me deter em explicar cada princípio. Recomendo buscar na lei, a sua definição e o escopo de aplicação.

Vale destacar as dez bases legais que estão previstas no artigo 7º da lei, no que se refere ao tratamento de dados pessoais.

1. Consentimento;
2. Cumprimento da obrigação legal ou regulatória;
3. Execução de políticas públicas;
4. Estudos por órgão de pesquisa;
5. Execução de contrato ou de procedimentos preliminares;

6. Exercício regular de direitos;

7. Proteção da vida ou da incolumidade física;

8. Tutela da saúde;

9. Interesses legítimos do controlador ou de terceiro;

10. Proteção do crédito.

Observa-se ainda que o rol é taxativo, ou seja, é obrigatório que a organização, pública ou privada, aplique uma ou mais bases legais para o tratamento dos dados pessoais.

Percebe-se empiricamente, o desconhecimento por parte do cidadão acerca de seus Direitos Fundamentais, em especial ao seu Direito à Privacidade e à Intimidade, conforme preceitos constitucionais, e mais especificamente, ao uso e acesso aos dados pessoais para diferentes propósitos, sem que haja o consentimento prévio. Ademais, a preocupação se acentua em relação as organizações, que estão despreparadas para a adoção dos padrões de conformidade à lei e ao tratamento específico de dados pessoais de seus clientes, consumidores e cidadão comum. A ausência de uma cultura de privacidade no Brasil ainda está em estágio incipiente para o enfrentamento do processo de transformação digital. O empoderamento perpassa pelo estabelecimento do processo de cultura digital e de exercício dos direitos do cidadão brasileiro.

2.1 IMPACTOS E PARALELOS DA LGPD COM A GESTÃO DA INFORMAÇÃO

Sempre que uma nova legislação promove novas regras, formatos e padrões no tratamento da informação, as áreas de conhecimento dedicadas a este tema precisam se dedicar a sua compreensão, não apenas para se adequar ao ambiente regulatório advindo da nova legislação, mas principalmente para contribuir para soluções técnicas para os desafios que são inerentes ao surgimento de uma nova regra.

Foi assim quando do surgimento da Lei de Acesso à Informação – LAI, que tardiamente se dispôs a regulamentar o direito fundamental de acesso a informações públicas, previsto no inciso XXXIII do art. 5º da Constituição Federal de 1988. Apenas 23 anos após a promulgação da Constituição, o cidadão brasileiro pode conhecer de que maneira poderia exercer seu direito de receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral.

Apesar de limitado, por ter sido fundamentalmente aplicado aos órgãos públicos, é inegável que tal regulamentação gerou impactos positivos para um melhor desenvolvimento de programas de gestão documental nestes órgãos. E isso se deu pelo entendimento natural de que o direito de ter acesso à informação estaria diretamente prejudicado caso não houvesse a aplicação de conjunto de medidas que garantisse racionalização e eficiência na criação, tramitação, classificação e avaliação dos documentos. Em resumo, sem um programa de gestão documental, há enorme risco de não atendimento ao direito do cidadão que buscasse acesso à informação presente nestes acervos.

Agora, com chegada da Lei Geral de Proteção de Dados, efeito similar ocorre, com a característica adicional de que não está restrita apenas a órgãos da administração pública, mas a qualquer "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", conforme previsto no conceito presente no inciso VI do Art. 5º da Lei 13709/2018, a LGPD.

As empresas, os especialistas e as consultorias, em sua grande maioria, focam naquilo que é mais sensível e visível, ou seja, no tratamento de dados advindos da relação entre o cliente consumidor, e das empresas provedoras de produtos e serviços, especialmente através da internet. E nesse contexto, soluções pré-formatadas de gestão de dados de bases de clientes para vendas e *marketing* tornam-se, obviamente, bastante atraentes.

Porém, quando observamos a evolução das leis que tratam do tema da privacidade no mundo, podemos perceber que, a depender do momento histórico, outras relações que envolvem tratamento de dados já estiveram no foco principal das preocupações em relação a privacidade.

Na Europa da década de 70 e 80, portanto num período que precede a União Europeia, diversos países desenvolveram legislações nacionais que se preocupavam com a privacidade, e que nitidamente tinham como principal preocupação a relação entre Estado e seus cidadãos, e protegiam estes de eventuais abusos na gestão dos dados daqueles. Talvez essa preocupação, e esta hipótese demandaria um aprofundamento que não pretendo trazer aqui, seja advinda da necessidade de se criar ambientes regulatórios inóspitos a tentativas de implantação de governos totalitários a partir de manipulações em massa de dados sobre a vida dos cidadãos de uma nação.

Outra preocupação, está mais recente, e alinhada a existência de grandes plataformas de mídias sociais, está nas práticas de mineração de dados e processamento em massa de dados, presentes em conceitos de Big Data. Através deste tipo de processamento, muito se praticava o uso não autorizado (pelo menos não explícito e transparente) de dados pessoais de maneira indireta, para fins de definição de perfis, e geração de influência, seja em processos de venda, quanto de decisões coletivas, como eleições gerais de diversos países, ou ainda esforços para desestabilizações de governos.

Através de processamento massivo de dados, grandes corporações ganham capacidade de serem decisivas tanto nas relações entre clientes consumidores com seus fornecedores de produtos e serviços, mas também na relação entre governos e cidadãos.

Quero propor com isso, que os impactos com a LGPD tem um potencial exponencialmente maior que a LAI já nos trouxe, em relação a gestão documental e gestão da informação, e que os profissionais desta disciplina temos desafios ainda maiores, seja na adaptação a esta nova realidade, mas principalmente, como dito no início deste capítulo, no desenvolvimento de respostas e contribuições para o atingimento dos objetivos da nova legislação.

O que proponho a seguir é trazer à tona alguns paralelos entre LAI e LGPD, buscando contribuir para o entendimento dos impactos advindos dessas legislações, dando pistas de por onde os profissionais da Gestão da Informação podem buscar se inserir neste mercado.

2.1.1 O cidadão e o cliente agora também são titulares de dados

A LGPD traz o conceito de titular de dados. O titular de dados não é aquele que detém o dado, o titular de dados é aquela pessoa a quem os dados se referem, independente de quem tem a tutela desses dados.

O cidadão, enquanto titular de dados, ganha grande poder junto ao estado, no papel de controlador e operador dos dados do cidadão. O cidadão se relaciona com o Estado das mais diversas maneiras. O estado tem nossos dados em função da emissão de carteira de motorista, dados médicos, dados de identidade, dados de eleitor, uma série de dados são processados por empresas públicas como Serpro e Dataprev, o que não faz do Estado dono, titular desses dados. O Estado é controlador ou operador desses dados. O poder reside no cidadão que atua e bota o boné de titular de dados.

O cliente, enquanto titular de dados, ganha força junto ao seu provedor de produtos e serviços, no papel de controlador e operador dos dados do cliente, pois passa a ter regras que vão além de seus direitos enquanto consumidor, mas de titular de dados sob controle das empresas.

Como o tema que estamos tratando aqui é Empoderamento da Sociedade, vamos tratar mais da relação cidadão e Estado, mesmo entendendo que este empoderamento não está limitado a esta relação. O cidadão sendo tratado aqui enquanto titular, e o Estado como controlador/operador.

2.1.2 Paralelos presentes entre LAI e LGPD

Um primeiro esclarecimento em relação à LAI e a LGPD, é que apesar de parecerem conflitantes, elas possuem muito mais convergências que conflitos. Num primeiro olhar, podemos identificar um aparente conflito, pois a LAI trataria de acesso a informações e a LGPD da proteção, ou seja, sigilo.

Ocorre que a LGPD não trata propriamente do sigilo, mas das condições necessárias para a realização de um tratamento de dado de forma segura, que não exponha o titular de dados ao risco de exposição ou uso indevido.

Outro aspecto muito importante é que a LGPD também garante acesso a informação, porém na perspectiva do interesse individual, e não coletivo, diferenciando aqui o conceito de acesso, do de publicidade, pois nem todo acesso se dá através da disponibilidade pública da informação.

Por último, embora já tenhamos tratado deste ponto, vale reafirmar que o alcance da LAI se dá para o setor público, e da publicidade sobre atos que envolvam interesse público. Já a LGPD define regras para instituições públicas e privadas, conforme Quadro 2 abaixo:

Quadro 2 – Resumo LAI X LGPD

LAI	LGPD
INTERESSE COLETIVO	INTERESSE PARTICULAR
PUBLICIDADE DAS INFORMAÇÕES	PROTEÇÃO AOS DADOS DO TITULAR
DIRECIONADA A INSTITUIÇÕES PÚBLICAS	DIRECIONADA A INSTITUIÇÕES PÚBLICAS E PRIVADAS

Fonte: Elaborado pelos autores, 2020

2.1.3 Informação Pessoal X Dado Pessoal

Os conceitos de informação pessoal e dado pessoal também merecem uma análise em relação a como aparecem em ambas as legislações.

A LAI apresenta o conceito de INFORMAÇÃO PESSOAL, como aquela (informação) relacionada à pessoa natural identificada ou identificável (BRASIL, 2011). Já a LGPD mistura os conceitos de dado e informação, ao considerar o DADO PESSOAL como a "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018, p.2).

A diferença maior se dá quando ambas buscam qualificar o que seria uma espécie de categoria especial de informação/dado pessoal.

A LAI, ao garantir o sigilo para informações pessoais, define que o direito ao sigilo se configura quando tais informações pessoais são relativas à intimidade, vida privada, honra e imagem, garantindo a estas o sigilo de 100 anos. Essa diferenciação prevista no Artigo nº 31 deixa claro que não é toda e qualquer informação pessoal protegida por sigilo, e isso explica porque em algumas situações informações pessoais são divulgadas em portais do governo, em sites de

instituições e órgãos sob o argumento do interesse público. Desde que aquela informação pessoal não esteja relacionada à intimidade, vida privada, honra e imagem não faria jus a um sigilo de acordo com a LAI.

Já a LGPD trata de maneira especial, a categoria dos dados pessoais considerados sensíveis, que são aqueles que revelam características de personalidade que podem expor o titular a algum tipo de tratamento discriminatório, como origem racial ou étnica, convicção religiosa, opinião política, além de dados relacionados a sua saúde. A LGPD prevê 10 hipóteses de tratamento para os dados pessoais, mas para o tratamento de dados pessoais sensíveis existe uma limitação maior. São apenas sete bases, acrescidos da alínea G que trata de questões especificamente como autenticação em sistemas eletrônicos e combate a fraudes.

Isso se dá porque o tratamento de dados pessoais sensíveis expõem o titular a um risco maior. Podem gerar riscos às liberdades civis e aos direitos fundamentais e, portanto, tem mais restrições ao seu tratamento. Nestes casos o controlador deve ter uma atenção maior, e não pode usar como hipótese de tratamento, por exemplo, o seu legítimo interesse,

O Artigo nº 23 da LGPD que faz a ponte entre a LAI e a LGPD quando diz que o TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, ou seja, o Estado também realiza tratamento de dados pessoais e poderia haver algum conflito com a LAI, que prevê a publicidade, o acesso aos dados públicos e a LGPD prevê a proteção de dados pessoais (BRASIL, 2018).

Porém o Artigo nº 23 apresenta uma pista para um caminho que vai resolver ou endereçar o desequilíbrio nessa suposta contradição, porque desde que o tratamento do dado pessoal tenha relação direta com uma finalidade pública, o interesse público, a publicidade deve prevalecer.

Para fechar esse ponto, a LGPD contém também os conceitos da dados anonimizados e dados pseudonimizados.

O dado anonimizado é aquele relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Por exemplo uma filmagem que não captura o rosto da pessoa, dados de pesquisa que elimina o CPF, o RG ou o nome da pessoa e trabalha com dados estatísticos para fins de estudo e pesquisa são dados anonimizados. Ou seja, que não permitam maneira de identificar uma pessoa. Dessa forma o dado anonimizado não é um dado pessoal. Ele pode ter sido coletado originalmente como um dado pessoal, dento de um determinado contexto, mas se for tratado de maneira anonimizada, ele não está sujeito às limitações da LGPD. Portanto, é incorreto denominar um dado como pessoal anonimizado, pois são características excludentes.

Já o dado pseudonimizado é aquele dado pessoal que perdeu temporariamente a possibilidade de associação, direta ou indireta, a um indivíduo, em razão de uma estratégia de segregação e/ou embaralhamento de dados, mas que pode vir a ser revertida. A está justamente no fato de que o dado anonimizado não pode ter sua condição revertida, não podendo recuperar a capacidade de identificação de um indivíduo.

Se você tiver um dado que você considera anonimizado, mas existe alguma técnica disponível no momento desse tratamento que te permita reverter e voltar a identificar esse indivíduo ele não é um dado propriamente anonimizado, mas pseudonimizado. A pseudonimização é uma técnica de aumento de proteção de dados e é recomendado em muitos casos, bem como a criptografia.

A pseudonimização é inclusive um procedimento previsto no Decreto nº10.153/19, que dispõe sobre a salvaguardas de proteção à identidade dos denunciantes de ilícitos e de irregularidades praticados contra a administração pública federal direta e indireta.

2.1.4 Término do tratamento e temporalidade dos documentos

Outro impacto importante da LGPD na Gestão Documental tem relação com a temporalidade e destinação de documentos e a previsão da eliminação após o término do tratamento de dados.

Antes de mais nada é preciso aqui apontar uma contradição presente no Artigo nº 16 da LGPD, que diz que "Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades" (BRASIL, 2018, p.8).

O inciso X do Artigo nº 5 da LGPD conceitua o que vem a ser tratamento de dados. Dentre as diversas operações elencadas como exemplo, temos arquivamento, armazenamento e eliminação. Parece claro que não se poderia falar em conservação ou eliminação após o término do tratamento, se as operações arquivamento, armazenamento e eliminação são consideradas ações de tratamento de dados.

Entendo que ao ler o que consta nos artigos nº 15 e nº16 na Lei enquanto término de tratamento, deveríamos entender na verdade como término, alcance ou atingimento da finalidade de determinado tratamento, pois há tratamento subsequente ao término da finalidade, mesmo que seja a eliminação ou conservação, sob forma de arquivamento ou armazenamento.

Feito esse esclarecimento, vamos ao definido na lei. Os artigos nº15 e nº16 da LGPD tratam do término do tratamento e da eliminação dos dados. Vincula o término do tratamento a subsequente eliminação dos dados, porém autoriza sua manutenção em algumas situações, dentre elas, cumprimento de obrigação legal ou regulatória pelo controlador (BRASIL, 2018).

Os instrumentos de gestão documental, como código de classificação e tabela de temporalidade, independente da legislação para os documentos públicos, devem sempre considerar a necessidade de manutenção para comprovação cumprimento de deveres e/ou garantia de direitos. Portanto o racional por detrás de uma temporalidade deve ser a mesma que orienta o cumprimento de uma obrigação legal, para fins de manutenção de dados pessoais. Se eu mantendo determinados registros documentais para o cumprimento de uma regulação, essa mesma regulação me permite a manutenção dos dados pessoais, segundo o inciso I do Artigo nº16 da LGPD (BRASIL, 2018, p.8).

Explicando a partir de um exemplo comum a todas as empresas, cito a situação de demissão ou aposentadoria de um empregado, onde se configura encerrado o vínculo empregatício. Está configurado o término da finalidade do tratamento dos dados coletados, processados, armazenados, porém é facultado ao controlador a conservação dos dados para outra finalidade que não mais a gestão do empregado. Se encerra uma finalidade, mas o tratamento dos dados continua, para nova finalidade, a de gerenciar por exemplo os riscos de contencioso trabalhista.

Caso o titular solicite a eliminação dos dados ou o direito ao esquecimento, a empresa deverá negar porque tem potenciais obrigações legais e defesa de causas trabalhistas. E como as Tabelas de Temporalidade já são elaboradas considerando a legislação que regula a atividade que gerou os documentos arquivísticos, ela passa a ser talvez a melhor referência para definição da manutenção dos dados pessoais após o atingimento da finalidade pela qual os dados foram originalmente coletados e tratados.

Mas também há um outro aspecto que faz das Tabelas de Temporalidade não apenas referências, mas fundamentais para estar em conformidade com a LGPD. A ajudar com que os dados pessoais não sejam mantidos para além da real necessidade. Se antes não havia urgência em se tomar uma decisão sobre eliminação de dados, tratando-se apenas de uma questão de custos de manutenção de um acervo, a partir da LGPD, se não existe uma razão legal obrigatória, prevista

por exemplo numa Tabela de Temporalidade, o controlador não vai mais poder manter esses registros. Esse é um impacto direto e importante e uma grande oportunidade de fortalecer a gestão documental e trazer resposta aos gestores e empregadores sobre manutenção de dados pessoais.

2.1.5 Gestão, governança e tratamento de dados

Os conceitos de Gestão de Documentos, Governança de Dados e Tratamento de Dados são similares, trazem uma lógica ciclos ou de sequência de atividades, porém é possível realizar alguns rápidos comentários a respeito destes conceitos que podem ser muito facilmente confundidos. Tomemos por base os conceitos trazidos no Quadro 3 a seguir:

Quadro 3 - Conceitos de Gestão de Documentos, Governança de Dados e Tratamento de Dados

Gestão Documental	Conjunto de procedimentos e operações técnicas referentes à produção, tramitação, tramitação uso, avaliação e avaliação, arquivamento de documentos em documentos fase corrente e intermediária, visando sua eliminação ou recolhimento.
Governança de Dados	Sistema de tomada de decisões executado por um modelo que descreve quem age com qual informação, em que momento, usando que métodos e sob que circunstâncias.
Tratamento de Dados	Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Fonte: Elaborado pelos autores, 2020

O Tratamento de Dados é um conceito mais amplo e geral, que pode inclusive não depender de qualquer tipo de metodologia. Apenas uma denominação trazida pela LGPD, de forma a enquadrar toda e qualquer operação feita com dados pessoais, e assim garantir que não haja dúvidas sobre quando se estaria ou não realizando operações sujeitas à Lei.

A Governança de Dados, apesar de ter uma conotação de gestão, administração, normalmente é utilizada quando nos referimos a processos de tomada de decisões sobre conjuntos de dados específicos, dentro de processos específicos, normalmente ligados a atividade fim de uma organização, e quase sempre sustentada por sistemas de informação.

Por fim a Gestão Documental, mais familiar aos arquivistas, me parece ser bastante útil para a missão de quem a partir da LGPD, precisará gerir o ciclo de vida dos dados pessoais, até a conclusão de seu tratamento, ou de sua finalidade, na lógica que defendi alguns parágrafos acima. Desta forma entendo que é a partir da gestão documental que podemos ajudar a trazer respostas para a instituição que pretende gerir bem seus dados pessoais, inevitavelmente presente em documentos e informações.

Será preciso reforçar a gestão documental dos agentes de tratamento de dados, se estes quiserem estar e, conformidade com as regras de tratamento de dados trazidos pela LGPD. Sem uma boa gestão documental dificilmente se vai conseguir dar respostas sobre quais são os tratamentos que realiza, qual o volume de dados que tem em razão de cada tratamento e quais são as decisões finais em relação a deleção desses dados. Tal como é fundamental uma boa gestão documental no setor público para se poder atender aos pedidos realizados por cidadãos com base na Lei de Acesso à Informação, também uma boa gestão documental será fundamental para o atendimento aos direitos dos titulares de dados.

2.1.6 Classificação quanto ao sigilo da informação e segurança de dados

A classificação das informações quanto ao seu sigilo é fundamental para a definição do investimento necessário para sua devida proteção, logo, sigilo da informação e proteção de dados são conceitos indissociáveis. Protegemos o que é sigiloso e esta condição nos é trazida por uma valoração atribuída por um processo de classificação.

É muito comum, porém, que tenhamos uma visão restrita sobre classificação, especialmente no setor público, e principalmente após a chegada da Lei de Acesso à Informação. Isso ocorre porque a LAI conceitua informação sigilosa como sendo "aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado" (BRASIL, 2011, p.1). Porém, a própria LAI explica, em seu Artigo nº 22 que "o disposto nesta Lei não exclui as demais hipóteses legais de sigilo e de segredo de justiça nem as hipóteses de segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público" (BRASIL, 2011, p.6).

As informações classificadas e mantidas em sigilo sustentada nessas demais hipóteses legais, não seriam, portanto, informações sigilosas? Obviamente que são, e não em razão de sua imprescindibilidade para a segurança da sociedade e do Estado. São segredos industriais e comerciais decorrentes da exploração direta de atividade econômica, são informações relativa intimidade, vida privada, honra e imagem das pessoas, dentre outros motivos.

É preciso, portanto, que tenhamos clareza quanto a abrangência do conceito de informação sigilosa, pois mecanismos e critérios além dos previstos na LAI precisam ser considerados na hora de classificarmos os dados que precisarão ser protegidos para se estar em conformidade com a LGPD, entendida nesse contexto como uma nova hipótese legal para sigilo de determinadas informações, onde constam dados pessoais de titulares de dados, sob responsabilidade do controlador ou operador.

Segundo a LGPD, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Estes dados, para que sejam identificados como objeto de aplicação da proteção exigida, precisam estar classificados, ou categorizados.

Portanto, quando a LGPD trata de segurança e sigilo dos dados, isso tem menos relação com graus de sigilo, conforme previsto na LAI, e mais relação com Segurança da Informação quando pensamos no tripé: Confidencialidade, Integridade e Disponibilidade. A informação precisa estar disponível, ter qualidade, ou seja, integro e precisa estar protegido de acessos indevidos, ou seja, que não seja acessado por quem não pode ter acesso. A proteção dos dados, sob o olhar da Segurança da Informação é mais do que uma questão de sigilo, circunscrita ao pilar da Confidencialidade.

3 CONSIDERAÇÕES FINAIS

O trabalho do arquivista é, além de muito importante para as instituições, uma atividade extremamente específica, pois trata com os documentos produzidas e recebidas pelas instituições independentes dos seus suportes. Neste sentido, em algum dos conteúdos destes documentos poder

haver informações sigilosas. Por conseguinte, é importante saber equilibrar a possibilidade do acesso com a necessária sigilosidade que estes conteúdos guardam.

Desta forma, conhecer e saber equilibrar os limites da transparência com as necessidades de sigilo é fundamental para a salvaguarda dos direitos individuais e coletivos. O acesso à informação encobre-se, parcialmente, para o bem público, com um manto de opacidade que lhe é vital. O segredo, neste momento, torna-se importante e, sob certas circunstâncias legítimo, quando busca defender aos interesses sociais e deve ser também compatível com a ética, tendo uma finalidade específica. Fica evidente a duplicidade apresentada nesta discussão entre o visível e o invisível, entre o silêncio e a fala, pois existe um limite tênue entre eles.

Como foi apresentado durante a mesa redonda essa discussão também perpassa a relação público-privada. Os marcos legais ora em debate buscam definir e delimitar os espaços de segredo de transparência do Estado que durante muito tempo foi utilizado pelos gestores públicos como formas de controle assegurando-se no poder. As estratégias voltadas para o silenciamento das informações estatais encontram agora uma barreira, ao mesmo tempo que as informações que, obrigatoriamente devem ficar salvaguardadas recebem esse embasamento legal.

Entretanto, a LGPD traz em seu princípio basilar, o resguardo aos direitos fundamentais no que tange ao acesso indevido de seus dados pessoais, em cumprimento aos direitos à privacidade e à intimidade, ensejando um debate em prol do equilíbrio entre o acesso à informação e aos dados públicos e a segurança jurídica do cidadão brasileiro.

REFERÊNCIAS

BRASIL. Presidência da República. **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. 37º 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/civil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 6 jul. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/civil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 jul. 2020.

CIURIAK, Dan. The Economics of Data: Implications for the Data-Driven Economy (February 4, 2018). Chapter 2 in "Data Governance in the Digital Age, **Centre for International Governance Innovation**, 5 March 2018. Disponível em: http://dx.doi.org/10.2139/ssrn.3118022. Acesso em: 15 maio 2020.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD**: Lei Geral de Proteção de Dados Comentada. São Paulo: Thompson Reuters Brasil, 2019.

OLIVEIRA, Adriana Carla Silva de. A LGPD e a Transformação Digital. Dados & Privacidade Blog. Disponível em: https://www.dadoseprivacidade.com.br/a-lgpd-e-a-transformacao-digital. Acesso em: 12 jul. 2020.

OLIVEIRA, Adriana Silva de Oliveira. Desvendando a autoralidade colaborativa na e-science sob a ótica dos direitos de propriedade intelectual. 2016. Tese (Doutorado em Ciência da Informação). Universidade Federal da Paraíba, João Pessoa, 2016. Disponível em: https://repositorio.ufpb.br/jspui/handle/tede/8849. Acesso em: 12 jul. 2020.

RONCOLATO, Murilo. Por que debater a Lei de Proteção de Dados Pessoais? Entrevistado: Juliana Pereira Estadão, São Paulo, 28 jan. 2015. Disponível em: https://link.estadao.com.br/noticias/geral,por-que-debater-a-lei-de-protecao-de-dados-pessoais,10000029762 Acesso em: 12 jul. 2020.