FACULDADES LONDRINA

RICARDO ALEXANDRE COSTA

A OPERACIONALIZAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NAS ATIVIDADES NOTARIAIS E REGISTRAIS: UM DESAFIO NA ERA DIGITAL PARA OS CARTÓRIOS DE PROTESTO

LONDRINA
2023

A OPERACIONALIZAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NAS ATIVIDADES NOTARIAIS E REGISTRAIS: UM DESAFIO NA ERA DIGITAL PARA OS CARTÓRIOS DE PROTESTO

Documento apresentado para trabalho final da dissertação, para a obtenção do título de Mestre do Programa de Mestrado em Direito, Sociedade e Tecnologia das Faculdades Londrina, como requisito parcial para obtenção do título de Mestre.

Orientador: Prof. Dr. Carlos Renato Cunha

LONDRINA
2023

Ficha de identificação da obra
Elaborado por: Viviane S. Paszczuk
Bibliotecária CRB9 1885/O

C387o Costa, Ricardo Alexandre.
A operacionalização da Lei Geral de Proteção de Dados (LGPD) nas atividades notariais e registrais: um desafio na era digital para os cartórios de protesto / Ricardo Alexandre Costa. - Londrina, 2023.
120 f. : il.

Orientador: Carlos Renato Cunha.
Programa de Mestrado Profissional em Direito, Sociedade e Tecnologias da Escola de Direito das Faculdades Londrina, 2023.

Inclui bibliografia.

1. Atividades Notariais e Registrais. 2. Cartórios de Protesto. 3. Direito e Tecnologia. 4. LGPD e Privacidade. 5. Proteção de Dados Pessoais. I. Cunha, Carlos Renato. II. Faculdades Londrina.

A OPERACIONALIZAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NAS ATIVIDADES NOTARIAIS E REGISTRAIS: UM DESAFIO NA ERA DIGITAL PARA OS CARTÓRIOS DE PROTESTO

Documento apresentado para trabalho final da dissertação, para a obtenção do título de Mestre do Programa de Mestrado em Direito, Sociedade e Tecnologia das Faculdades Londrina, como requisito parcial para obtenção do título de Mestre.

COMISSÃO EXAMINADORA

_____

Prof. Dr. Carlos Renato Cunha
Orientador
Faculdades Londrina

_____

Prof. Dr. Eduardo Contani
Membro titular
Faculdades Londrina

_____

Prof. Dr. Jonathan Barros Vita
Membro titular
Faculdades Londrina

Londrina, 23 de junho de 2023.

Dedico esta dissertação à minha família.

AGRADECIMENTOS

A Deus, pela dádiva da vida e por me permitir realizar tantos sonhos nesta existência.

Ao professor Dr. Carlos Renato Cunha, pela orientação, competência, profissionalismo e dedicação tão importantes. Obrigado por acreditar em mim e pelos tantos elogios e incentivos. Tenho certeza de que não chegaria neste ponto sem o seu apoio.

Aos membros da banca examinadora, Prof. Dr. Eduardo Contani, Prof. Dr. Jonathan Barros Vita, que tão gentilmente aceitaram participar e colaborar com esta dissertação.

Aos professores do Programa de Mestrado em Direito, Sociedade e Tecnologia das Faculdades Londrina, pelo tanto de conhecimento que me foi apresentado durante o curso.

À minha família, por apoiarem e compreenderem o meu isolamento em inúmeros finais de semana.

À minha mãe e ao meu pai, deixo um agradecimento especial, por todas as lições de amor, companheirismo, amizade, caridade, dedicação, abnegação, compreensão e perdão que vocês me dão a cada novo dia. Sinto-me orgulhoso e privilegiado por ter pais tão especiais.

E à minha esposa querida, sempre pronta a me apoiar em tudo nesta vida.

“A LGPD não é um projeto... é uma jornada.”
(BRONZATTI, 2019)

COSTA, Ricardo Alexandre. **A operacionalização da Lei Geral de Proteção de Dados (LGPD) nas atividades notariais e registrais: um desafio na era digital para os cartórios de protesto** 2023. 120 f. Trabalho de Conclusão de Curso de Mestrado Profissional em Direito – Faculdades Londrina, Londrina, 2023.

RESUMO

O tema desta dissertação é a operacionalização da Lei Geral de Proteção de Dados (LGPD) nas atividades notariais e registrais. O objetivo geral desta dissertação é compreender como a LGPD é operacionalizada nas atividades notarias, mediante a análise do caso de cartórios de protesto e os objetivos específicos são apresentar as dimensões da privacidade e tecer comentários sobre o direito à informação, demonstrar a evolução da proteção jurídica aos dados no Brasil e no mundo e apresentar as mudanças promovidas pela LGPD no Brasil e na operacionalização das atividades notariais e registrais em cartórios de protesto. Quanto à metodologia utilizada, a pesquisa, quanto à natureza, é básica, quanto aos objetivos, descritiva, com abordagem qualitativa. Os dados foram coletados de fonte secundária, utilizando como instrumento a análise documental, além da pesquisa bibliográfica. A análise dos dados foi feita por meio de análise de conteúdo. Ao final, pode-se concluir que compreender a operacionalização da LGPD nas atividades notariais e registrais é uma temática, apesar de recente, de fundamental importância, pois os cartórios são verdadeiros repositórios de dados pessoais, e a atividade notarial é, em nosso país, um serviço intimamente ligado ao Estado que, em certa medida, o representa como agentes políticos e sociais, exercida por particular. Ainda, esclarece-se que é obrigação de toda empresa ou profissional que tenha qualquer vínculo com dados pessoais de titulares conhecê-la e cumpri-la. Quanto à operacionalização da LGPD especificamente em cartórios de protesto, na prática, mesmo que sua função base seja dar publicidade ao descumprimento de obrigações, à inadimplência, os cartórios não podem, de forma indiscriminada, publicar ou difundir os dados que deveriam ser tornados públicos. Assim, por dever ético e legal, o tabelião deve guardar e operacionalizar suas atividades tendo como base a LGPD, observando os regramentos nela contidos e usando a publicidade de dados pessoais o mínimo necessários para a execução fim.

Palavras-chave: Atividades notariais e registrais. Cartórios de protesto. Direito e Tecnologia. LGPD. Privacidade. Proteção de dados pessoais.

COSTA, Ricardo Alexandre. **The application of the Driver's Privacy Protection Act (DPPA) in notary and registration activities**. 2022. 120 f. Completion of Professional Master's Degree in Law – Faculdades Londrina, Londrina, 2022.

ABSTRACT

The theme of this dissertation is the operationalization of the General Data Protection Law (LGPD) in notarial and registry activities. The general objective of this dissertation is to understand how the LGPD is operationalized in notary activities, through the analysis of the case of protest notaries and the specific objectives are to present the dimensions of privacy and comment on the right to information, demonstrate the evolution of legal protection to data in Brazil and in the world and present the changes promoted by the LGPD in Brazil and in the operationalization of notary and registry activities in notary offices of protest. As for the methodology used, the research, as for the nature, is basic, as for the objectives, descriptive, with a qualitative approach. Data were collected from a secondary source, using documentary analysis as an instrument, in addition to bibliographic research. Data analysis was performed through content analysis. In the end, it can be concluded that understanding the operationalization of the LGPD in notarial and registry activities is a theme, although recent, of fundamental importance, because notaries are true repositories of personal data, and the notarial activity is, in our country, a service closely linked to the State that, to a certain extent, represents it as political and social agents, exercised by private individuals. Still, it is clarified that it is the obligation of every company or professional that has any link with personal data of holders to know and comply with it. As for the operationalization of the LGPD specifically in protest notaries, in practice, even if its basic function is to publicize the non-compliance with obligations, the default, the notaries cannot, indiscriminately, publish or disseminate the data that should be made public. Thus, by ethical and legal duty, the notary must keep and operationalize its activities based on the LGPD, observing the rules contained therein and using the disclosure of personal data the minimum necessary for the final execution.

Keywords: Notarial and registry activities. Protest notaries. Law and Technology. LGPD. Privacy. Protection of personal data

LISTA DE ABREVIATURAS E SIGLAS

Anoreg/BR	Associação dos Notários e Registradores do Brasil
ANPD	Autoridade Nacional de Proteção de Dados
Arpen/BR	Associação Nacional dos Registradores de Pessoas Naturais do Brasil
BCR	*Binding Corporate Rules*
CC	Código Civil brasileiro
CENPROT	Central Nacional de Serviços Eletrônicos Compartilhados
CDC	Código de Defesa do Consumidor
CF/88	Constituição Federal de 1988
CJF	Conselho da Justiça Federal
CNB/CF	Colégio Notarial do Brasil – Conselho Federal
CNJ	Conselho Nacional de Justiça
Cogetise	Comitê de Gestão da Tecnologia da Informação dos Serviços Extrajudiciais
CPIP-JP	Comissão de Proteção de Informações Pessoais do Japão
CTN	Código Tributário Nacional
DPIA	*Data Privacy Impact Assessment*
DPO	*Data Protection Officer*
EUA	Estados Unidos da América
FAQ	Perguntas frequentes
IEPTB/BR	Instituto de Estudos de Protesto de Títulos do Brasil
Irib/BR	Instituto de Registro Imobiliário do Brasil
IRTDPJ/BR	Instituto de Registro de Títulos e Documentos e de Pessoas Jurídicas
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
LPIP-JP	Lei de Proteção de Informações Pessoais do Japão
MP	Medida Provisória
PEC	Proposta de Emenda Constitucional
PIA	*Privacy Impact Assessment*
PIHBO	*Personal Information Handling Business Operator*
RIPD	Relatório de Impacto à Proteção dos Dados Pessoais
RGPD	Regulamento Geral de Proteção de Dados

TICs	Tecnologias da Informação e Comunicação
UE	União Europeia

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

SUMÁRIO

INTRODUÇÃO

Primeiramente, é importante destacar que a sociedade contemporânea é o resultado e a síntese das inúmeras transformações que ocorreram ao longo da História da humanidade nos diferentes segmentos que a constitui. Seja qual for o âmbito – social, cultural, econômico, educacional, tecnológico, jurídico – pode-se observar mudanças e acompanhar sua evolução por meio dos dispositivos legais que surgem da necessidade de regular comportamentos sociais de uma determinado período histórico.

A evolução tecnológica vivida atualmente oferece à sociedade, em uma senda, uma contínua e acelerada melhora na área da comunicação e da informação no ciberespaço, porém a outra face da moeda é a afronta aos direitos fundamentais da privacidade e a necessidade de proteção jurídica dos dados pessoais. A capacidade de transmitir informações é um reflexo do progresso tecnológico da humanidade. O direito à informação expandiu-se e o ciberespaço passou a ser uma rede aberta, disponível a quase qualquer pessoa. A evolução da internet faz oportuna as discussões e o incremento de análises jurídicas sobre a proteção dos dados que circulam fácil e rapidamente no ciberespaço. A operacionalização de regras de proteção jurídica é um desafio na era digital, mas o Brasil, à exemplo de outros países, está evoluindo neste sentido, pois quando a sociedade muda, o Direito deve acompanhar.

No Brasil, a governança de banco de dados (físicos e virtuais) foi profundamente alterada pela Lei Federal 13.709, sancionada em 14 agosto de 2018 e em vigência desde 18 de setembro de 2020 e pela Medida Provisória (MP) n. 869/18, convertida na Lei n. 13.853, sancionada em 08 de julho de 2019, que estabeleceu a Autoridade Nacional de Proteção de Dados (ANPD). Conhecida como Lei Geral de Proteção de Dados (LGPD), a Lei n. 13.709/2018 marcou uma vitória da sociedade civil, pois criou um sistema normativo de proteção dos dados pessoais, especialmente em meios digitais, além de estabelecer uma série de deveres e exigências para as pessoas jurídicas do setor público e privado que coletam, registram, armazenam e disponibilizam informações privadas. Mais recentemente, o Projeto de Emenda Constitucional (PEC) 17/19 (que visava incluir no rol de direitos fundamentais o direito à proteção de dados pessoais, alterando o art. 5º, XII da Constituição) deu origem à

Emenda Constitucional (EC) 115/22 e foi promulgada pelo Congresso Nacional aos 10 de fevereiro de 2022, alterando a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

É importante salientar que a entrada em vigor da LGPD (apesar de ameaçada por cláusula de adiamento – MP 959/19 – que foi, posteriormente, retirada) foi em hora propícia, devido ao aumento exponencial do uso da internet e consequente acréscimo da exposição de dados pessoais, tendo em vista o enfrentamento da pandemia da Covid-19 e a necessidade de isolamento social.

No direito notarial e registral os impactos da LGPD podem ser observados em algumas frentes, já que os cartórios (serventias extrajudiciais) são verdadeiros repositórios de dados pessoais, e a atividade notarial é, em nosso país, um serviço intimamente ligado ao Estado que, em certa medida, o representa como agentes políticos e sociais, exercida por particular. Os cartórios, nesta senda, devem se adequar à lei, limitando o uso da base de dados pessoais publicamente acessíveis às suas finalidades (mínimo necessários para a execução fim).

Sendo assim, a LGPD é operacionalizada nas atividades de notários e registradores de forma integral, estando sujeitas ao sistema de regras e princípios da Lei e às regulamentações da ANPD, porém as minúcias da nova legislação forçam a adequação dos cartórios, esbarrando, inclusive, em incompatibilidade com o princípio da publicidade indireta, entre outros dispositivos legais. Nos serviços notarias e registrais, especificamente o cartório de protesto, existe o princípio da publicidade – mitigado e relativo, não amplo e irrestrito.

Por estes motivos, no âmbito das notas e registros, já se travava, mesmo antes do advento da LGPD, entendimento sobre o delicado equilíbrio entre direitos como a privacidade e a intimidade, de um lado, e o princípio da publicidade e do acesso à informação, de outro. A problemática (publicidade notarial e registras versus direito à privacidade) assume diferentes aspectos a depender da espécie de serviço extrajudicial. Em tabelionatos de notas, por exemplo, em que a publicidade tem o escopo de difundir, propagar e trazer notoriedade a um fato, seja público ou privado, a operacionalização da LGPD trouxe (trará) relevantes consectários práticos no dia a dia dessas serventias.

Especificamente sobre os serviços notariais e registrais, em 31 de julho de 2018, o Conselho Nacional de Justiça (CNJ) publicou o Provimento n. 74 que dispôs sobre os padrões mínimos de tecnologia da informação para a segurança, integridade e disponibilidade de dados para a continuidade da atividade pelos serviços notariais e de registro do Brasil. Segundo o provimento, impõe-se aos serviços notariais e de registro a adoção de políticas de segurança de informação que garantam: confiabilidade, disponibilidade, autenticidade, integridade e mecanismos preventivos de controle físico e lógico da informação. Cabe ao Comitê de Gestão da Tecnologia da Informação dos Serviços Extrajudiciais (Cogetise) a atualização anual dos pré-requisitos mínimos, além de ser responsável por divulgar, estimular, apoiar e detalhar a implementação das diretrizes do Provimento nº 74/2018.

Também, ao que tange os Cartórios de Protesto, mais especificamente, o CNJ lançou o Provimento n. 134, em 24 de agosto de 2022, que, em capítulo próprio (Capítulo XV – Do protesto de títulos e outros documentos de dívida), estabelece medidas a serem adotadas pelas serventias extrajudiciais em âmbito nacional para o processo de adequação à LGPD. Em suas considerações gerais, o Provimento n. 134/2022 estabelece que as disposições previstas na LGPD deverão ser cumpridas pelas serventias extrajudiciais. Ainda, estabelece que os responsáveis pelas delegações dos serviços extrajudiciais são os titulares das serventias, portanto controladores a quem compete as decisões referentes ao tratamento de dados pessoais. Em nome e por ordem do controlador, o operador é a pessoa natural ou jurídica, de direito público ou privado, externa ao quadro funcional da serventia – contratada, pois, para serviço que envolva o tratamento de dados pessoais.

Em observância à legislação aplicável, especialmente à LGPD e ao Provimento nº 134/2022, do CNJ, que regulamenta a LGPD no âmbito das serventias extrajudiciais, o Instituto de Estudos de Protesto de Títulos do Brasil (IEPTB), demonstrando compromisso sério com a privacidade e proteção dos dados pessoais de todos os clientes, apresentantes, parceiros e prestadores de serviços, apresentou sua Política de Privacidade e Cookies. Tal documento oferece ao cliente dos cartórios de protesto, em linguagem clara e objetiva, informações pertinentes à coleta, tratamento e compartilhamento dos dados pessoais nas atividades cotidianas do tabelionato.

É neste contexto que se encontra a problemática que foi estudada na pesquisa proposta. A pergunta respondida ao final da pesquisa foi: como é operacionalizada a LGPD nas atividades dos cartórios de protesto?

O objetivo geral é compreender como a LGPD é operacionalizada nas atividades notarias, mediante a análise do caso de cartórios de protesto.

Os objetivos específicos são:

- Apresentar as dimensões da privacidade e tecer comentários sobre o direito à informação;
- Demonstrar a evolução da proteção jurídica aos dados no Brasil e no mundo;
- Apresentar as mudanças promovidas pela LGPD no Brasil e na operacionalização das atividades notariais e registrais, mediante a análise do caso dos cartórios de protesto;

Quanto à metodologia utilizada, a pesquisa apresentada nesta dissertação foi, quanto à natureza, básica, quanto aos objetivos, descritiva, com abordagem qualitativa. Os dados foram coletados de fonte secundária, utilizando como instrumento a análise documental, além da pesquisa bibliográfica. A análise dos dados foi feita por meio de análise de conteúdo. Ainda, foi realizada análise documental, ou seja, a LGPD foi analisada do ponto de vista de sua operacionalização nas atividades notariais e registrais exercidas nos cartórios de protesto. O objetivo da análise documental é reapresentar o conteúdo de um documento sob ótica diferente da original, a fim de facilitar a identificação de fatores particulares (BARDIN, 2011).

Sobre a contribuição científica e prática da dissertação apresentada, afirma-se que, por se tratar de tema recentemente introduzido na Academia, o estudo da LGPD conta com algumas publicações de obras/livros recentes, tais como: Cardoso (2020), Garcia et al. (2020), Lima et al. (2021), Wachowicz (2021), Pinheiro (2021), Soler (2021), entre tantos outros, porém são poucos os estudos da operacionalização prática da LGPD ou de detalhamentos dos impactos da lei em atividades específicas.

Quanto à relevância científica e prática, pode-se dizer que se vive a Era da Informação. Vive-se em uma sociedade em que a informação é o elemento base para o desenvolvimento econômico e pode ser transmitida em quantidade e velocidade nunca vista. Segundo Russo (2019) entre outros, a informação é um bem tão valioso quanto o dinheiro. O protagonismo da informação nas relações sociais levou a um

cenário em que há a necessidade urgente de garantir proteção à privacidade, e cumprimento das garantias previstas na proteção dos direitos humanos, como a privacidade.

A exemplo do ocorrido no cenário global, a LGPD foi estabelecida no Brasil, em 2018, entrando em vigor em 2020, para prezar rigorosamente pela proteção à privacidade e dar proteção jurídica aos dados pessoais. O surgimento de regulamentações para proteção de dados, no mundo e no Brasil, tem como motivação as inovações tecnológicas, os avanços do modelo de negócios da economia digital (PINHEIRO, 2021), o alargamento do uso da internet (RUSSO, 2019), fomentado pela pandemia do Covid-19 e pela necessidade de isolamento social (PINHEIRO, 2021).

Quanto ao sistema notarial e registral, cabe esclarecer que, como protetor da publicidade de dados de pessoas e coisas e possibilitador da participação popular nos controles dos atos de negócio (registro público de documentos), não se aplica o segredo de justiça e se preza pela transparência e democracia no acesso à dados. O acesso aos procedimentos desjudicializados, tais como o registro de nascimento, óbito, divórcio, inventário, usucapião e, em relação à imóveis, o acesso irrestrito à verificação de informações, coíbem negociações ilícitas e facilitam o controle.

A observância e operacionalização da LGPD nas atividades notariais e registrais é uma temática que ganha espaço nas discussões acadêmicas e sociais, principalmente por ser tema relativamente recente e ainda impor questionamentos sobre algumas incompatibilidades com marcos legais já estabelecidos, como o princípio democrático da publicidade e o acesso à informação. Segundo Pinheiro (2021), a LGPD não é perfeita e alguns pontos devem ainda ser esclarecidos pela ANPD, mas é obrigação de toda empresa ou profissional que tenha qualquer vínculo com dados pessoais de titulares conhecê-la e cumpri-la.

Compreender a operacionalização da LGPD nas atividades notariais e registrais, principalmente nos cartórios de protesto é relevante para a sociedade, pois se buscou, por meio da pesquisa realizada, esclarecer algumas nuances de ordem prática e legal ainda obscuras. Para a academia, a realização desta pesquisa é justificada por ser, até o presente momento (e de todas as leituras e buscas em bancos de dados realizadas), inédita, pois pouco se publicou sobre a operacionalização da LGPD nas atividades notarias e registrais, mas nada ainda em específico às atividades dos cartórios de protesto.

Para o pesquisador este tema é particularmente importante, pois, como profissional do Direito, agente público estatal, tabelião do cartório de protesto de Foz do Iguaçu/PR, todos os resultados obtidos ao final da pesquisa serão lastro para tomadas de decisão. O trabalho em um cartório de protesto está relacionado à recuperação de créditos, que, por sua vez, está relacionado à recuperação da dignidade econômica e social do indivíduo, pelo cumprimento de obrigações creditícias. O comprometimento com a prestação de serviço público, atendendo os princípios da publicidade, autenticidade, segurança e eficácia, deve estar, da mesma forma, imbuído dos ditames protetivos da LGPD.

Justifica-se, desta forma, a realização da pesquisa proposta por esta dissertação.

1 DA PRIVACIDADE E DO DIREITO À INFORMAÇÃO À PROTEÇÃO DE DADOS PESSOAIS

1.1 Direito à privacidade: evolução da proteção jurídica diante das inovações tecnológicas

Vários autores estão se debruçando sobre as temáticas ligadas à privacidade e à proteção de dados pessoais. No entendimento de Castells (2011), Russo (2019) e Da Silva et al. (2020), a informação é um bem tão valioso quanto o dinheiro. O protagonismo da informação nas relações sociais levou a um cenário em que há a necessidade urgente de garantir proteção à privacidade (BASTOS; BASI; CASSI, 2021), e cumprimento das garantias previstas na proteção dos direitos humanos, como a privacidade (PINHEIRO, 2021). Nunca se falou tanto em segurança, proteção de dados e privacidade (ESQUÁRCIO; ESQUARCIO, 2020).

Para fins de estudo de Direito, o direito à privacidade é compreendido como gênero, sendo o direito à intimidade compreendido como uma espécie da privacidade. O direito à privacidade (manifestações da esfera íntima, privada e da personalidade da pessoa) engloba, portanto, o direito à intimidade e de sua proteção jurídica faz parte os dados pessoais, sendo vedado o tratamento de dados sem consentimento expresso do titular (GRESSLER; BACHINSKI; SILVA, 2019).

Venosa (2013) elenca, entre os direitos da personalidade, a proteção à vida, à imagem, do nome, da privacidade, entre outros aspectos que resguardam a dignidade humana. Para o autor, os princípios dos direitos da personalidade estão expressos de forma genérica em dois níveis: na CF/88, que aponta sua base, e, com complementação, no Código Civil brasileiro (CC, Lei n. 10.406, de 10 de janeiro de 2002), que os enuncia de forma mais específica. Ainda, Venosa (2013, p. 180) destaca que:

> Cada vez mais na sociedade avulta de importância a discussão acerca da proteção à imagem, à privacidade, do direito ao próprio corpo, sobre a doação e o transplante de órgãos e tecidos, matéria que também pertence a essa classe de direitos. Da mesma forma se posiciona o direito à natalidade e a seu controle, temas que tocam tanto o Direito como a Economia, Filosofia, Sociologia e religião.

Para Leonardi (2019), assuntos como a liberdade de pensamento, controle sobre o próprio corpo, quietude do lar, recato, controle sobre informações pessoais, proteção à reputação, entre outros, são parte do conceito do direito à privacidade. No mesmo sentido, Gressler, Bachinski e Silva (2019, p. 2) asseveram que:

> A temática da proteção de dados pessoais assume relevante valor social na sociedade contemporânea, uma vez que a internet possibilita diversas sofisticações tecnológicas, seja com o desenvolvimento de novos softwares, seja com o armazenamento e divulgação de dados. Este desenvolvimento tecnológico acelerado expõe dados pessoais e gera vulnerabilidade das informações dos indivíduos. Nesse contexto, a violação aos direitos da personalidade, dentre eles, o direito à privacidade e à intimidade, tornaram-se mais frequentes.

A Constituição Federal, de 1988 (CF/88), por sua vez, não faz menção ao termo "privacidade", mas dita como garantia fundamental de todo brasileiro e estrangeiros residentes no País a intimidade, a vida privada, a honra e a imagem das pessoas (Art. 5º, X). A proteção de dados pessoais pode ser interpretada como um desdobramento do direito fundamental à privacidade, protegido pela CF/88 e, também, garantida pelo art. 11 do CC – "Art. 11 – Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária"; e pelo art. 21 do CC, que prevê que "Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

Esquarcio e Esquárcio (2020) afirmam que, mesmo que o CC, em seu art. 21, salvaguarde a vida privada da pessoa natural, a vigilância ao cidadão é permanente, para o bem e para o mal. Ainda, segundo os autores:

> Vivemos tempos de uma sociedade altamente informatizada e virtualizada, em que pelo menos nos grandes centros urbanos existe uma malha de conexão tecnológica, com dados sendo coletados a todo momento. Hoje em dia, qualquer pessoa após fazer uma pesquisa em um site de busca na internet, é bombardeada por publicidades sobre o produto ou serviço que se buscou, todo tipo de informativo começa a aparecer para o usuário sem o seu consentimento. Ao pesquisar sobre um evento esportivo ou cultural para ir num sábado à noite, o usuário vai receber notificações de toda sorte de espetáculos em cartaz; ao pesquisar o preço de um produto qualquer, o usuário vai ser bombardeado por toda sorte de publicidade sobre este produto em todas as suas mídias digitais e por dias seguidos. Hoje em dia, qualquer celular com conexão à internet é como uma grande antena disponível para captar e enviar todo tipo de dados e informação sobre o seu usuário. Os governos e as grandes organizações corporativas, além dos meios de comunicação, captam de forma invisível e silenciosa os dados de todos os

> sistemas eletrônicos como celulares, tablets e computadores (ESQUARCIO; ESQUÁRCIO, 2020, p. 15).

Silva (2016) avalia que a CF/88, por não trazer expressamente positivação do direito à privacidade, exaure na terminologia da “intimidade”, diferenciando-a da proteção delegada à honra, à imagem e à vida privada. Assim, para o autor:

> O dispositivo põe, desde logo, uma questão, a de que a intimidade foi considerada um direito diverso dos direitos à vida privada, à honra e à imagem das pessoas, quando a doutrina os reputava, com outros, manifestação daquela. De fato, a terminologia não é precisa. Por isso, preferimos usar a expressão “direito à privacidade”, num sentido amplo e genérico, de modo a abarcar todas essas manifestações da esfera íntima, privada e da personalidade, que o texto constitucional em exame consagrou (SILVA, 2016, p. 206).

Já, segundo Monteiro (2007, p. 31), a intimidade, em uma acepção clássica, pode ser entendida como “[...] a prerrogativa que o indivíduo possui perante os demais, inclusive o Estado, de ser mantido em paz no seu recanto. É, na essência, o mecanismo de defesa da personalidade humana contra ingerências alheias indesejadas e ilegítimas”. O autor apresenta o princípio da exclusividade, de Hannah Arent, baseado em Kent, que postula que a intimidade contém três exigências: a solidão (o desejo de estar só), o segredo (sigilo) e a autonomia (liberdade de decidir sobre si).

Esse conteúdo normativo, a que se refere ao tratar do dito “direito à privacidade”, é visivelmente observado com maior precisão à luz do que se convencionou denominar “teoria das esferas”. A Teoria dos Círculos Concêntricos – ou Teoria das Esferas da Privacidade –, de Hubmann e Henkel, diferencia, desde a década de 1950, a esfera pública da privada e apregoa a existência de três círculos (um dentro do outro) abstratos: a circunferência externa é a privacidade (de maior amplitude), a circunferência intermediária é a intimidade e a circunferência mais oculta é a do segredo.

Sendo assim, a primeira esfera da privacidade corresponderia ao núcleo essencial, e por isso intangível, da privacidade, abrangendo aspectos íntimos da pessoa. Complementarmente, haveria uma segunda esfera, ligada sobretudo às informações sigilosas ou restritas à vida comercial, familiar e profissional da pessoa. Ao passo que a terceira esfera estaria relacionada ao aspecto social do indivíduo, aos quais situam-se o direito à imagem e à palavra.

Em uma interpretação semelhante, Costa e Dalledone (2020, p. 136) afirmam que o direito à privacidade *lato sensu* está submetido a três círculos protetivos concêntricos, de intensidade decrescente – a teoria das esferas -, explicando que:

> [...] a esfera interna, que corresponde ao âmbito mais íntimo da liberdade humana, que pode estar acobertada pelo segredo (do qual são exemplos o direito à intimidade e as liberdades de manifestação de pensamento, de consciência e de crença – art. 5º, incs. IV, VI e X); a esfera privada ampla, que abarca todas as questões relacionadas à autonomia do indivíduo enquanto integrante da sociedade (como, dentre outros, o direito à honra, ao sigilo de correspondência e a liberdade de profissão – art. 5º, incs. X, XII e XIII); a esfera pública, que engloba tudo que não esteja inserido nas anteriores.

Essa teoria, apesar de não abarcar todas as situações de fato que são envolvidas cotidianamente na proteção da privacidade, é um importante marco referencial sobre a proteção global do indivíduo e, consequentemente, de suas informações, no âmbito de proteção à privacidade.[1]

Monteiro (2007, p. 33) afirma que, pelas mudanças impostas à sociedade e pelos novos meios de comunicação social, o direito à intimidade e à privacidade confere ao indivíduo o poder de controle sobre a circulação de informações a seu respeito. É do homem, enquanto centro de referência de informações, a decisão sobre quando, como, em que extensão e para que finalidade uma informação deverá ser conhecida por terceiros. Por outro lado, nem toda informação interessa à tutela constitucional.

> Existe uma gama de dados pessoais cujo conhecimento e divulgação não avançam propriamente sobre a esfera da privacidade do indivíduo. A rigor, a informação só é objeto de proteção se relacionada com a intimidade, a identidade e a autonomia. Em geral, pode-se dizer que a invasão na intimidade e na vida privada pressupõe o conhecimento de uma particular informação que seu titular não deseja seja obtida por outros. Nessa ordem de idéias, a privacidade guarda relação com a vontade individual, com a necessidade de se expor e, ainda, de se retrair frente aos demais homens,

[1] Segundo Leonardi (2019, p. 73-77), alguns avanços tecnológicos tornam obsoletas ou incompleta algumas teorias. Apesar de ampla a aceitação e da popularidade da teoria das esferas, desenvolvida pelo Tribunal Constitucional alemão, para o autor, é a "teoria do mosaico" que conseguiria lidar com formas sofisticadas de ataque à privacidade na era digital. Leonardi (2019, p. 73-77) pondera que público e privado são conceitos relativos, que devem ser analisados em função de quem é o outro sujeito em uma 'relação informativa', pois existem dados irrelevantes *a priori* do ponto de vista da intimidade, mas que, em conexão com outros dados, igualmente irrelevantes em si, podem servir para tornar totalmente transparente a personalidade de um indivíduo, tal como ocorre com pedras que formam os mosaicos: em si mesmas, não dizem nada, mas unidas podem formar conjuntos plenos de significado.

> guardando para si, se assim necessitar, suas informações pessoais (MONTEIRO, 2007, p. 33).

Góis (2020) afirma que, no Brasil, tanto a privacidade quanto a intimidade foram tuteladas a nível constitucional – no meio do processo de constitucionalização de direitos próprio do movimento neoconstitucionalista – pela CF de 1988, Título II – Do Direito e Garantias Fundamentais, Capítulo I, art. 5º, X, que apregoa que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação".

Segundo Monteiro (2007, p. 27):

> Em meio ao catálogo de direitos fundamentais contido no artigo 5o da Constituição Federal, encontram-se aqueles destinados à tutela da intimidade e da vida privada, que são espécies de direitos da personalidade. Tais direitos englobam diferentes aspectos: o resguardo das informações, a privacidade corporal, a inviolabilidade das comunicações e a privacidade territorial, por exemplo.

Revisita-se, oportunamente, a definição de Direito Fundamental. Na definição de Tavares (2002, p. 362), os direitos fundamentais são:

> [...] um conjunto de faculdades e instituições que, em cada momento histórico, concretizam as exigências da dignidade, da liberdade e da igualdade humanas, as quais devem ser reconhecidas positivamente pelos ordenamentos jurídicos em nível nacional e internacional.

Na mesma senda, Alexandre de Moraes (2002, p. 39) conceitua tais direitos como:

> [...] o conjunto institucionalizado de direitos e garantias do ser humano que tem por finalidade básica o respeito a sua dignidade, por meio de sua proteção contra o arbítrio do poder estatal e o estabelecimento de condições mínimas de vida e desenvolvimento da personalidade humana.

Para Mendes (2018, p. 204), "[...] da perspectiva material, podem ser considerados direitos fundamentais todas aquelas pretensões reconhecidas em determinado período histórico como indispensáveis ao livre desenvolvimento da dignidade da pessoa humana".

Ainda, se faz oportuna a distinção de direitos fundamentais de outras categorias, tais como as garantias individuais ou as garantias institucionais –

categorias também relevantes do direito constitucional –, para que se compreenda adequadamente sua definição. Segundo as lições de Miranda (1990, p. 88-9), a distinção se opera nos seguintes termos:

> Os direitos representam só por si certos bens, as garantias destinam-se a assegurar a fruição desses bens; os direitos são principais, as garantias acessórias e, muitas delas, adjectivas (ainda que possam ser objecto de um regime constitucional substantivo); os direitos permitem a realização das pessoas e inserem-se directa e imediatamente, por isso, as respectivas esferas jurídicas, as garantias só nelas se projectam pelo nexo que possuem com os direitos; na acepção jusracionalista inicial, os direitos declaram-se, as garantias estabelecem-se.

Além disso, a categoria dos direitos fundamentais não se confunde com as chamadas garantias institucionais. Essa categoria resulta da concepção de que certos institutos (direito privado) ou instituições (direito público) são tão indispensáveis à ordem jurídica que devem ter sua essência preservada, mediante um complexo de normas jurídicas. As garantias institucionais, portanto, não se constituem em direitos atribuídos diretamente aos indivíduos, mas sim a determinadas instituições ou institutos que detém sujeito e objeto distintos. Alguns exemplos dessas garantias são: a tutela da liberdade de imprensa, da autonomia universitária, da propriedade privada, do funcionalismo público, dos entes federativos, da família, da maternidade, dentre outras.

No mesmo sentido, importa trazer o entendimento de Laureano e Benfatti (2021, p. 92) quando afirmam que:

> [...] é curial apontarmos para distinção existente entre direitos e garantias fundamentais, eis que o art. 5º, da Constituição Federal de 1988, trata dos direitos e deveres individuais e coletivos como sendo espécie do gênero direitos e garantias fundamentais, entretanto o texto constitucional não define com exatidão o real delineamento das distinções existentes.

Segundo os autores, as garantias constitucionais possuem caráter instrumental, ou seja, não são um fim em si mesmas, já que “[...] são mecanismos criados para proteger os direitos fundamentais e assegurar a sua afetividade. Já os direitos fundamentais são bens e vantagens inseridos na norma constitucional” (LAUREANO; BENFATTI, 2021, p. 92).

Segundo Botelho (2020), a proteção das pessoas, relativamente ao tratamento de seus dados pessoais, é, portanto, um direito fundamental, garantido pela Carta

Magma. A Proposta de Emenda Constitucional (PEC) 17/19 teve origem em um cenário conturbado pela *Big Data*[2], *Data Mining*[3] e pressões internacionais para a regulamentação das formas de obtenção e tratamento dos dados pessoais. A tramitação da PEC 17/19, dentre outras coisas, visava incluir no rol de direitos fundamentais o direito à proteção de dados pessoais, alterando o art. 5º, XII da Constituição. Após algumas modificações de caráter apenas estilístico, a PEC 17/19 deu origem à Emenda Constitucional (EC) 115/22[4] e foi promulgada pelo Congresso Nacional aos 10 de fevereiro de 2022. Atualmente, por meio da EC nº 115, de 10 de fevereiro de 2022, passou a ser citado no art. 5º, inciso LXXIX, com o seguinte texto:

> DOS DIREITOS E GARANTIAS FUNDAMENTAIS
> CAPÍTULO 1
> DOS DIREITOS E DEVERES INDIVIDUAIS E COLETIVOS
> [...]
> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]
> LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Tal EC inaugura uma nova era, incluindo a proteção dos dados pessoais aos direitos fundamentais individuais e coletivos. Ainda, a EC nº 115 acrescentou à CF/88 o inciso XXVI ao art. 21, e o inciso XXX ao art. 22, que passaram a determinar que a União é a responsável por organizar, fiscalizar e legislar sobre a proteção e tratamento de dados pessoais.

> DA ORGANIZAÇÃO DO ESTADO
> [...]
> CAPÍTULO II

---

[2] Etimologicamente o termo *Big Data* surgiu no meio da década de 1990, utilizado pela primeira vez por John Mashey, um cientista aposentado, para se referir à manipulação e análise de um grande volume de dados, com capacidade de rápida expansão (KITCHIN, 2014, p. 99), tendo como elemento principal o registro de qualquer fenômeno, natural ou não, em dados (AMARAL, 2016, p. 9).

[3] *Data Mining* (ou mineração de dados) é o processo de explorar grandes quantidades de dados à procura de padrões consistentes. Por meio do *Data Mining*, uma empresa é capaz de explorar um conjunto de dados, extraindo padrões específicos que auxiliam na confecção de relatórios direcionados. As empresas são capazes de acumular grande volume de dados brutos que dizem quem comprou o quê, onde, quando e em que quantidade e analisar para que empresa o indivíduo é melhor cliente (RUSSO, 2019).

[4] "Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais".

> DA UNIÃO.
> Art. 21. Compete à União:
> [...]
> XXVI – organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termo da lei.
> [...]
> Art. 22. Compete privativamente à União legislar sobre:
> [...]
> XXX – proteção e tratamento e dados pessoais.

Ocupando-se da teoria de Schreiber (2013), faz-se importante para esta dissertação apresentar as duas dimensões da problemática que envolve a privacidade e a proteção jurídica de dados pessoais. A primeira dimensão se debruça sobre o modo como são obtidos e tratados os dados pessoais (dimensão procedimental) e a segunda se ocupa do uso em si que se faz dos dados pessoais (dimensão substancial).

Na dimensão procedimental, com foco na forma pela qual a informação pessoal é coletada e tratada até eliminação, pode ocorrer a coleta clandestina ou desautorizada – evidente invasão de privacidade e considerada ilegal – facilitada principalmente pelo emprego de tecnologias (SCHREIBER, 2013). Keinert e Cortizo (2018) também entendem que a "sociedade da vigilância" ("sociedade do risco" ou "sociedade da informação") – cibercultura, ciberespaço, uso de Tecnologias da Informação e Comunicação (TICs), onde o indivíduo é vigiado por seus pares, por meio de redes sociais e comunicacionais – ao desafiar as normas democráticas, tem acesso facilitado a informações pessoais, o que reflete evidentemente na privacidade. Importa apresentar a definição dada por Wachowicz (2020, p. 598):

> Na Sociedade Informacional a computação se desenvolve através do uso das Tecnologias da Informação e Comunicação (TICs), em especial por meio de redes de conexão e transmissão de dados, conhecida como Internet, qual se popularizou e institucionalizou a chamada Governança Global. [...] A nova ordem mundial nas relações internacionais do século XXI se perfaz pelo uso massivo das novas Tecnologias da Informação e Comunicação (TIC's), a exemplo da Internet na capacidade de compartilhar em tempo real a mesma informação a milhões de pessoas desde que conectadas a uma rede.

É oportuno exibir o conceito de internet apresentado por Leonardi (2019). Segundo o autor, a internet é definida como uma rede internacional de computadores conectados entre si, que serve, entre outras coisas, como um meio de comunicação que possibilita o intercâmbio de informações de toda natureza, em escala global. Ainda, para Leonardi (2019), todo o operador de Direito deveria compreender os

elementos técnicos fundamentais sobre a internet para ações e decisões corretas em âmbito judicial.

Schreiber (2013) trata como dimensão procedimental, enquanto Keinert e Cortizo (2018) nomeiam dimensão tecnológica, mas ambas visões coadunam que a privacidade dos dados pessoais é seriamente ameaçada pelo uso extensivo e ofensivo das tecnologias da comunicação como forma de extrair, mercantilizar (transmitir) e controlar as informações pessoais do indivíduo.

No entendimento de Schreiber (2013), na dimensão substancial – que tange o emprego oferecido às informações pessoais colhidas – é importante que haja o consentimento para que não se violem direitos fundamentais. Segundo Soler (2021, p. 60):

> A primeira observação a ser feita é que o consentimento não pode ser encarado como uma presunção, ele deve ser fornecido por escrito, com cláusula destacada, ou por meio que demonstre a efetiva manifestação da vontade do titular, cabendo ao agente de tratamento a responsabilidade para tanto, mais especificamente ao controlador.

Por um lado, há a necessidade de fornecer informações pessoais para que se concretizem inúmeras ações (tais como: compras, acessos à documentos, acessos bancários, serviços públicos, entre outras), por outro lado, há a subversão da finalidade primeira do fornecimento de tais dados. Russo (2019) esmiúça o processo chamado de *data mining* (mineração de dados), que ocorre quando os dados pessoais são armazenados em bancos de dados de acordo com características consideradas relevantes por um controlador, mas são acessados à procura de padrões consistentes, direcionados a atividades específicas.

> No exercício de suas atividades, as empresas acumulam grande volume de dados pessoais em seus aplicativos operacionais. São dados brutos que dizem quem comprou o quê, onde, quando e em que quantidade e a análise sobre eles serve para conhecer melhor os clientes, seus padrões de consumo e suas motivações. Nesse cenário, o cidadão assume papel de protagonismo no fornecimento de suas informações, mas por outro lado, de coadjuvante no seu uso (RUSSO, 2019, p. 28).

Portanto, não há, na sociedade atual, a possibilidade de um indivíduo ter todas as suas informações, totalmente privadas, por todo o tempo. Desde o nascimento, o indivíduo passa a ser conhecido por meio de suas informações e estas informações

encontram-se armazenadas nos bancos de dados de um hospital, depois de um cartório de registro de pessoas naturais, depois de uma escola (Educação Infantil, seria a primeira experiência) e assim, para o resto da sua vida em sociedade, suas informações serão acessadas a cada vez que dele forem necessários dados pessoais.

1.2 Direito à informação e o acesso às informações pessoais na era digital

É imprescindível, para que se entenda a discussão apresentada neste capítulo, que se observe a diferença entre dado e informação. Em diversos contextos jurídicos, a informação, sob o aspecto de documentação organizada, é o produto da análise dos dados existentes e que um dado é qualquer elemento identificado em sua forma bruta que, por si só, não conduz a uma compreensão de determinado fato ou situação. Infere-se, portanto, que um dado, após interpretação, análise, tratamento torna-se informação. Amaral (2016) afirma que dados são os fatos que são coletados e armazenados.

Nesse mesmo sentido, Hoffman (2009, p. 11) define o dado como uma "[...] informação bruta, sendo considerado a matéria-prima a ser utilizada na obtenção de informações e que podem ser: registros quantitativos ou qualitativos [...]", que descrevem algum evento representados por meio de símbolos, letras, números, textos entre outras formas e suportes. A difícil compreensão do propósito dos dados esbarra na falta de estruturação e o estabelecimento de relações, o que os tornam informação. A informação, por sua vez é caracterizada por "[...] uma mensagem com dados que são compreendidos, podendo ser audível ou visível, e onde existir um emitente e um receptor" (HOFFMAN, 2009, p. 11). O processo de transformação de dados em informação envolve ferramentas de análise, aplicação da matemática a grandes quantidades de dados (MAYER-SCHÖNBERGER; CUKIER, 2013).

Ao escrever sobre privacidade e transparência no acesso à informação pública, Doneda (2011, p. 94) distingue dado e informação desta forma:

> [...] em relação à utilização dos termos 'dado' e 'informação', vale uma especificação. O conteúdo de ambos se sobrepõe em várias circunstâncias, o que justifica uma certa promiscuidade na sua utilização. Ambos os termos podem ser utilizados para representar um fato, um determinado aspecto de uma realidade. Não obstante, há uma carga semântica específica em cada um desses termos. Assim, o termo dado apresenta conotação um pouco mais primitiva e fragmentada, como se fosse uma informação em estado potencial,

> antes de ser transmitida; o dado estaria, portanto, associado a uma espécie de ‘pré-informação’, anterior à interpretação e a um processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Sem aludir ao seu significado ou conteúdo em si, na informação já se pressupõe uma fase inicial de elaboração de seu conteúdo – daí que a informação carrega também um sentido instrumental, no sentido de ser capaz de, objetivamente, reduzir um estado de incerteza.

Bioni (2019) esclarece que, para melhor compreender a diferença de dados e informações, na Era da Informação, dados (*lato sensu*) são fatos isoladamente considerados, que dependem de processamento e sozinhos não acrescem conhecimento a nenhuma área; informações são o encadeamento dos fatos (dados) que possibilite uma conclusão lógica, isto é, informação é a organização que converte o dado em algo decifrável e que em conjunto com a interpretação agrega conhecimento.

Interessa apresentar a análise de Sampaio (1998): a pessoa, isoladamente ou enquanto ser social, é um “centro de referência de informações”; o direito à intimidade, espécie do gênero vida privada, consiste numa gama de faculdades que permitem a seletividade de informações que penetram (“*inputs*”) e que partem (“*outputs*”) do campo perceptivo da pessoa.

O controle, não absoluto, sobre os *inputs* de informação (as informações que vem do exterior), reflete-se no direito de a pessoa selecionar as impressões que transmitem informações (como o som, por exemplo) das quais ela quer ou não ser receptora. Assim, a pessoa tem o direito de abster-se de impressões sensitivas que veiculem uma informação que “[...] interfira em sua tranqüilidade e provoque ou possa provocar turbação moral” (SAMPAIO, 1998, p. 364-5). Já, o controle sobre os *outputs* de informação representa o direito de a pessoa controlar a circulação de suas informações pessoais.

O autor trata como informação pessoal aquela que diz respeito a uma pessoa, em um sentido amplo, capaz de abranger o fenômeno conhecido como “projeção da personalidade” (SAMPAIO, 1998, p. 374). Essa visão, atualmente, encontra apoio em grande parte da doutrina que, segundo o referido autor, reconhece que existem dois modos de violação da intimidade: o conhecimento e a difusão de fatos privados.

No entendimento de Esquárcio e Esquarcio (2020), nunca se produziu tanto conteúdo com temáticas ligadas à segurança, proteção de dados e privacidade. A situação apresentada pelos autores é tão perturbadora que se torna relevante

reproduzir, pois, apesar de parecer enredo de um cenário visto apenas em filmes futuristas, descreve exatamente o que os indivíduos vivem diariamente.

> Vivemos tempos de uma sociedade altamente informatizada e virtualizada, em que [...] existe uma malha de conexão tecnológica, com dados sendo coletados a todo momento. Hoje em dia, qualquer pessoa após fazer uma pesquisa em um site de busca na internet, é bombardeada por publicidades sobre o produto ou serviço que buscou, todo tipo de informativo começa a aparecer para o usuário sem o seu consentimento. Ao pesquisar sobre um evento esportivo ou cultural para ir num sábado à noite, o usuário vai receber notificações de toda sorte de espetáculos em cartaz; ao pesquisar o preço de um produto qualquer, o usuário vai ser bombardeado por toda sorte de publicidade sobre este produto em todas as suas mídias digitais e por dias seguidos. Hoje em dia, qualquer celular com conexão à internet é como uma grande antena disponível para captar e enviar todo tipo de dados e informação sobre o seu usuário. Os governos e as grandes organizações corporativas, além dos meios de comunicação, captam de forma invisível e silenciosa os dados de todos os sistemas eletrônicos como celulares, tablets e computadores. A vigilância ao cidadão é permanente, para o bem ou para o mal (ESQUÁRCIO; ESQUARCIO, 2020, p. 15).

Os autores asseveram, ainda, que a internet foi criada para compartilhar informações e interligar pessoas e não para “esconder” dados (ESQUÁRCIO; ESQUARCIO, 2020). Neste mesmo viés, novas e inimagináveis tecnológicas são desenvolvidas em diversas áreas do conhecimento e os avanços na informatização, as inovações tecnológicas, a criação de *softwares* de alta *performance* e alargamento do acesso à internet, e a todos estes avanços, impactam, em particular, os meios de coleta, armazenamento, tratamento e divulgação de informações e dados pessoais.

Na visão de Bioni (2019, p. 30):

> A informação é o (novo) elemento estruturante que (re)organiza a sociedade, tal como o fizeram a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós-industrial. Ainda que essa nova forma de organização social não se resuma apenas ao meio ambiente virtual, a computação eletrônica e a internet são ferramentas de destaque desse processo.

No mesmo sentido, para Monteiro (2007), a liberdade de expressão e informação é uma das mais estimadas características dos regimes democráticos. A Declaração Universal dos Direitos do Homem, em seu artigo 19, versa sobre o direito à liberdade de opinião e expressão, e declara que todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado

pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e ideias por qualquer meio de expressão.

No entendimento de Russo (2019) e Da Silva et al. (2020), a informação é um bem tão valioso quanto o dinheiro, porém, apesar de ser o núcleo para o desenvolvimento econômico, de modo geral, a problemática do acesso à informação está em sua geração, seu processamento, e sua transmissão (BASTOS; BASSI; CASSI, 2021). Para Almeida e Soares (2022, p. 27):

> Os avanços tecnológicos trazidos pela era digital, fizeram com que as informações coletadas pelas empresas e instituições (pública e privada), se tornassem valorosos ativos para o aspecto econômico. Esse movimento demandou uma nova visão, ao celebrar a informação como um bem valioso, e sua proteção, uma prioridade. Nesse espaço, diversos países se viram diante da necessidade de elaborar leis como forma de regulamentar o tratamento, disponibilidades, acessibilidade e uso desses bens, os dados pessoais e informações.

Neste viés, segundo Botelho (2020), o centro da discussão é a produção e manipulação de dados pessoais e o limite do tratamento das informações disponibilizadas no *Big Data*, na era da sociedade da informação. Desta forma, na era da informação, o que se observa é a vulnerabilidade dos dados pessoais, da segurança, privacidade e intimidade. Silva (2017) já assegurava ser perigosa a facilidade e rapidez com que a informática interconecta fichários formados por grandes bancos de dados – *Big Data* –, que podem devassar a vida de pessoas, sem seu consentimento. Por outro lado, de acordo com Mayer-Schönberger e Cukier (2013), o aumento da disponibilização de informações faz com que as corporativas ganhem margem para inovar, possibilitando a melhora da competitividade.

Botelho (2020) afirma que, no momento histórico vivido, dado e informação são importantes ativos das empresas e configuram-se imprescindíveis para a consecução das atividades e objetivos corporativos. Em outras palavras, "[...] os dados se tornaram matéria-prima dos negócios, um recurso econômico vital, usado para criar uma nova forma de valor econômico" (MAYER-SCHÖNBERGER; CUKIER, 2013, p. 4). É neste contexto que o direito à informação, positivado pela CF/88, no art. 5º, incisos XIV[5] e XXXIII, e 220, § 1º, assume extraordinária relevância. Ressalta-se que, neste último,

[5] "XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;"

a privacidade figura como limite constitucional expresso à liberdade de comunicação social.

A Lei nº 12.527, de 18 de novembro de 2011, conhecida como Lei de Acesso à Informação (LAI), regula o acesso a informações previsto no inciso XXXIII[6] do art. 5º, no inciso II[7] do § 3º do art. 37 e no § 2º[8] do art. 216 da CF/88, além de alterar a Lei nº 8.112, de 11 de dezembro de 1990 (regime jurídico dos servidores públicos civis da União) e revogar a Lei nº 11.111, de 5 de maio de 2005 (acesso aos documentos públicos de interesse particular ou de interesse coletivo ou geral), e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991 (acesso e sigilo dos documentos públicos), dando outras providências. Segundo Wachowicz (2020, p. 367):

> A Lei de Acesso à Informação (Lei nº 12.527/2011) é outro marco importante na discussão sobre proteção de dados face ao poder público, pois estabelece procedimentos que devem ser respeitados pelos entes estatais para assegurar o direito fundamental de acesso à informação.

A LAI prevê que o acesso às informações sobre os atos realizados pela Administração Pública é de interesse coletivo, portanto, qualquer cidadão tem o direito de fiscalizar os processos licitatórios, as execuções de obras e as prestações de contas, dentre outros exemplos que se pode citar. Sendo assim, a LAI se fundamenta sobre o princípio da publicidade dos atos administrativos nas três esferas de poder. Neste mesmo sentido, a LAI inclui a obrigação de o Poder Público observar a proteção de dados pessoais (o que acaba por ser complementado pela proteção prevista na LGPD, como será visto posteriormente).

É importante esclarecer que o direito à informação se apresenta sob duas faces: a primeira consiste no direito de informar, isto é: a prerrogativa de comunicar de maneira não violenta algo a outrem, como decorrência direta do direito de liberdade de expressão (art. 5º, incs. IV e IX); a segunda, consiste no direito de ser informado, isto é: de receber mensagens, ideias e dados, seja por terceiros, pelos meios de

---

[6] "XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;"

[7] "II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII;"

[8] "§ 2º Cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem."

comunicação ou pelo próprio Estado (art. 5º, incs. XIV e XXXIII; art. 37, § 3º, II; e 220, caput).

Segundo Costa e Dalledone (2020, p. 137):

> Já foi assinalado que a liberdade informacional é requisito para um regime democrático [...]. Como qualquer direito fundamental, todavia, a liberdade de informação não é absoluta, encontrando limites expressos no próprio texto constitucional, como nos casos de sigilo das comunicações pessoais (art. 5º, inc. XII), das fontes jornalísticas (art. 5º, inc. XIV), do exercício de determinadas profissões, e do sigilo "imprescindível à segurança da sociedade e do Estado" (art. 5º, XXXIII). Há, ainda, os casos de "segredo de justiça" no âmbito dos processos judiciais (art. 93, inc. IX). Além disso, há possibilidade de colisão entre o direito à informação e o direito à privacidade, a demandar a tarefa de ponderação dos valores em conflito.

Passa-se, após tal esclarecimento, à discussão do direito à informação versus o direito à privacidade.

1.3 Direito à privacidade versus direito à informação: desafio da era digital

Segundo Góis (2020), não é nova a temática que se debruça sobre a tensão existente entre o anseio/afã humano de preservar a intimidade e a vida privada – reservando e preservando seu círculo social – e a necessidade histórica de expressar e saber – consubstanciada na liberdade de expressão e no direito difuso à informação. No entendimento de Leonardi (2019, p. 122), a individualidade da pessoa deve ser incorporada ao conceito de bem comum, e não entendida como seu contraponto. Quando a individualidade é separada do bem comum, o valor da privacidade diminui, e o sopesamento de princípios tende a favorecer aqueles tradicionalmente relacionados a interesses coletivos, já que os interesses sociais tendem a preponderar sobre interesses individuais.

Assim, uma das colisões de direitos fundamentais mais clássica que existe é o conflito entre a liberdade de informação e o direito à privacidade, pois tais direitos estabelecem diretrizes em direções opostas: "[...] os direitos de personalidade se orientam no sentido da proteção da esfera privada [...]; já a liberdade de expressão segue o rumo da transparência, da publicidade, da livre circulação de informação, ou seja, caminha em direção totalmente contrária" (MARMELSTEIN, 2008, p. 59).

Barroso (2022, p. 616) corrobora tal entendimento ao afirmar que a ponderação de valores, tais como "[...] o debate acerca do papel da imprensa, da liberdade de

expressão e do direito à informação em contraste com o direito à honra, à imagem e à vida privada", é um dos grandes temas da atualidade constitucional no Brasil. Em seu artigo 12, em 1948, a Declaração Universal dos Direitos do Homem apregoa que "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação".

Nascimento (2021) afirma que a CF/88 amadureceu discussões relacionadas ao acesso à informação. Segundo o autor, ainda na década de 1970, surgiu no meio arquivístico uma nova preocupação com o objeto científico do conhecimento, no qual antes estava resignado em uma ótica, agora passava por uma mudança de paradigmas, o eixo central deixava de ser o arquivo, e passa ser à informação. A preocupação com a preservação de objetos digitais está ligada à dinâmica da problemática de acesso à informação.

> Logo, é visto que a preocupação com o acesso à informação gera um cenário particular. Uma alusão que encaixa bem neste conceito, seria o simbolismo de uma moeda, a face da cara, seria o caráter interdisciplinar da ciência da informação, que permite contextualizar, nas humanidades digitais, um conjunto da produção civilizatória que sofre ação em um ambiente digital; e na coroa, a face da governança eletrônica (*e-governance*), sendo a ação do Estado dentro do ambiente digital, a sua forma de trazer controle e segurança a esse espaço. Em ambos os aspectos a preservação do objeto digital pode se encaixar no conceito figurativo, sendo uma moeda com essas duas faces, em que o valor monetário é a garantia do acesso à informação (NASCIMENTO, 2021, p. 16).

De acordo com Gonçalves e Varella (2018), o respeito aos dados pessoais tem sido discutido amplamente após a publicação do Marco Civil da Internet (Lei n. 12.965/2014) e dos decretos de regulamentação, pois tal lei positivou a demanda da sociedade por maior transparência, com informações claras, inclusive, de natureza pessoal ou sigilosa, sob guarda da Administração Pública Federal. Por outro lado, o direito fundamental à privacidade, intrínseco a personalidade e dignidade da pessoa humana, é digno de atenção diante do avanço tecnológico na chamada Era da Informação, pois o comércio de dados pessoais ameaça a proteção deste bem jurídico e causa danos ao titular. Sendo assim:

> Um dos grandes desafios da atualidade é tentar atender às regras de transparência e publicidade exigidas pela chamada Lei de Acesso à Informação – LAI (Lei nº 12.527, de 18 de novembro de 2011) e, ao mesmo tempo, respeitar as necessárias restrições quanto à confidencialidade da

> informação no caso de grandes bases de dados que apresentam informações sensíveis (GONÇALVES; VARELLA, 2018, p. 514).

Segundo Bioni (2019, p. 8), tanto o direito à informação, quanto o direito à proteção de dados pessoais são direitos fundamentais:

> [...] expressamente previstos na Constituição Federal de 1988, regulamentados, respectivamente, pela Lei de Acesso à Informação (LAI – lei 12.527/2011) e pela Lei Geral de Proteção de Dados (LGPD – lei 13.709/2018). Ambas são resultado de anos de intenso trabalho e pressão conjuntos da sociedade civil em prol da garantia efetiva de direitos fundamentais dos cidadãos brasileiro.

Destaca-se o entendimento do Conselho da Justiça Federal (CJF, 2021), em seu Enunciado 531, sobre o direito de a personalidade ser o direito da pessoa de defender o que lhe é próprio, como a vida, a identidade, a liberdade, a imagem, a privacidade, a honra, entre outros. Tal enunciado defende o direito ao esquecimento, tratando como implícito à regra legal que assegura a proteção à intimidade, à imagem e à vida privada, assim como o princípio de proteção à dignidade da pessoa humana.

Ressalta-se, porém, que o acesso livre à informação coloca qualquer cidadão em igualdade com a administração pública, democratiza e dá transparência e retira do mando (e desmando) e do domínio de alguns o poder que da informação é proveniente, gerando *status* de igualdade e retirando valor àquele que consegue acessar e processar informações exclusivas.

Bioni, Silva e Martins (2022, p. 9) afirmam que o livre acesso às informações públicas é um fator essencial para o efetivo funcionamento das democracias, “[...] por permitir que os cidadãos tenham a possibilidade de avaliar políticas públicas, fazer o controle social e participar nos processos políticos de maneira qualificada.”. No entanto, para os autores, assim como o direito à informação, a proteção de dados pessoais também é um fator fundamental para a garantia da democracia, especialmente em uma sociedade cada vez mais orientada a dados e progressivamente tecnológica.

Gonçalves e Varella (2018, p. 519) afirmam que:

> [...] de um lado, o direito constitucional à privacidade, que abrange a intimidade, a vida privada, a honra e a imagem; de outro, o direito fundamental de acesso à informação, pautado pela transparência ativa da Administração Pública, ou seja, a busca pela proatividade na divulgação das informações. Ambos são princípios constitucionais e, como tais, não há hierarquia entre

> eles. Trata-se de uma antinomia aparente, devendo haver, tão somente na análise do caso concreto, o processo de harmonização e ponderação entre eles.

Costa e Dalledone (2020), ainda, ressaltam que a situação foi agravada pelo alargamento do uso da internet, destacando que:

> O direito “à vida privada”, insculpido no artigo 5º, inciso X da Constituição Federal, por representar um anteparo entre a esfera individual e o escrutínio público, sempre esteve sujeito a constantes colisões com o direito à informação, não havendo uma solução a priori para os conflitos daí decorrentes (COSTA; DALLEDONE, 2020, p. 133).

Ainda sobre o cenário vivenciado atualmente, no qual se observa um amplo uso de tecnologias e a exposição de dados pessoais, o que leva a uma vulnerabilidade do direito à privacidade, Russo (2019, p. 10) afirma que:

> A nova era digital apresentou ao mundo um bem quase tão valioso quanto o dinheiro: a informação. O volume de tráfego de dados digitais decorrente da utilização das novas tecnologias parece ser infinito, assim como sem fim parece ser o interesse pelo conteúdo por ele produzido. Nesse cenário [...] cabe refletir sobre a proteção dos dados pessoais e o direito à privacidade no contexto do desenvolvimento econômico e na utilização de tecnologias nas atividades empresariais.

No mesmo sentido, Laureano e Benfatti (2021) afirmam que o uso expansivo das tecnologias relacionadas à informação demanda gerenciamento e armazenamento avançado de dados, pois as informações pessoais estão disponibilizadas na internet, para as mais variadas finalidades, expondo as pessoais e tornando os dados pessoais uma mercadoria. Os autores, a par de reconhecerem que os avanços tecnológicos são benéficos, esclarecem que que um dos efeitos negativos é “[...] o atentado aos direitos fundamentais de honra, de privacidade e de proteção de dados” (LAUREANO; BENFATTI, 2021, p. 90).

Monteiro (2007) afiança, de igual forma, que, na hipótese de colisão entre direitos fundamentais, deve-se proceder resolução atribuída aos juízes ou tribunais e demais aplicadores do Direito, podendo haver dois tipos de tensão entre as normas: o conflito de regras e a colisão de princípios. Deve-se atentar para o fato de que: princípios são proposições normativas básicas com grau de abstração relativamente elevado (traduzem valores mais relevantes da ordenação jurídica e são normas que ordenam que algo seja realizado na maior medida possível, dentro das possibilidades

fáticas (condições de fato para a sua eficácia) e jurídicas (relações com outras regras igualmente válidas) existentes); regras são normas com grau de abstração relativamente reduzido, que já contêm, em si, determinações no âmbito do fático e juridicamente possível – por isso, só podem ser cumpridas ou não. Se uma regra é válida, deve ser observada na sua exata medida, nem mais, nem menos.

Marmelstein (2008, p. 23) afirma que “A positivação constitucional dos valores ligados à dignidade da pessoa humana e da limitação do poder fez com que a jurisdição constitucional se tornasse um importante mecanismo de proteção dos direitos fundamentais”. Para Godoy (2008), ambos os direitos (de informação e de privacidade) expressam-se sob a forma de regras, mas não perdem sua essência de princípio (são os chamados princípios-garantia), com fonte no princípio fundamental da dignidade humana, que é o máximo valor do ordenamento jurídico pátrio.

De acordo com Monteiro (2007, p. 29):

> Conforme a natureza das normas colidentes – se regras ou princípios –, as formas de superação de impasses são distintas. O conflito entre regras resolve-se no âmbito da validade. Se uma regra vale e é aplicável ao caso concreto, então, valem também suas conseqüências jurídicas, vez que contidas dentro do sistema normativo.

Um dos problemas, como percebido, diz respeito à hermenêutica, pois os termos jurídicos utilizados não se encontram padronizados causando imprecisão na interpretação das normal legais, o que suscita dificuldade em entender o que são dados pessoais, o que é informação protegida, um dado sigiloso, um dado protegido, um dado restrito e, desta forma, o que exatamente estaria abrangido no direito à privacidade. Bem como, é notável a dificuldade na doutrina e nos tribunais em diferenciar os termos privacidade, intimidade, vida privada.

Para Bioni, Silva e Martins (2022, p. 12), LAI e LGPD são, de forma e regra geral, convergentes e não colidentes, pois convergem no objetivo de:

> [...] dar maior transparência, ativa e passiva, para as informações e dados produzidos ou custodiados por órgãos e entidades públicos. Esse reforço à transparência permite a redução da assimetria informacional existente na relação entre cidadão e Estado, de forma a garantir maior controle e participação do cidadão, considerado a parte mais vulnerável.

A LAI estabelece, em seu art. 4º, que:

> I- informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
> [...]
> III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;
> IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável (BRASIL, 2011).

A Lei de Proteção de Dados (LGPD), Lei Federal n. 13.709/2018, sancionada em 14 agosto de 2018 e em vigência desde 18 de setembro de 2020, alterou a governança de banco de dados (físicos e virtuais) profundamente. A LGPD marcou uma vitória da sociedade civil, pois criou um sistema normativo de proteção dos dados pessoais, especialmente em meios digitais, além de estabelecer uma série de deveres e exigências para as pessoas jurídicas do setor público e privado que coletam, registram, armazenam e disponibilizam informações privadas. Nessa seara, a Lei n. 13.709/2018 fornece um elemento relevante para a resolução de controvérsias que envolvam o direito à privacidade.

Assim, nesse contexto, a Lei Federal n° 13.709/2018, busca trazer proteção de diversos valores constitucionais, tais como "[...] o respeito à privacidade; à autodeterminação informativa; à inviolabilidade da intimidade, da honra e da imagem; ao desenvolvimento econômico e tecnológico; e à inovação" (LAUREANO; BENFATTI, 2021, p. 90).

De fato: ambas as leis – Lei de Acesso à Informação (LAI – lei n. 12.527/2011) e Lei Geral de Proteção de Dados (LGPD – Lei n. 13.709/2018) – que regulamentam, respectivamente o direito à informação e o direito à proteção de dados pessoais, são fruto de intenso trabalho e debate social e servem para garantir efetivamente os direitos fundamentais dos cidadãos brasileiros. Bioni, Silva e Martins (2022) julgam inadequado o uso da LGPD para negar acesso à informações públicas, como feito, de forma sistemática, em diversas ocasiões nos últimos anos, o que, de alguma forma, fez com que se levantasse um aparente (e falso) conflito entre as leis.

Ambas as leis, de acordo com os autores, convergem, sendo pautadas pela redução de assimetria de informação da parte vulnerável. Não se pode (e não se deve), segundo Miriam Wimmer – diretora da ANPD – utilizar a LGPD como obstáculo

ao exercício de competências investigativas e fiscalizadoras, bem como para o exercício de direitos decorrentes do ordenamento jurídico brasileiro, devendo ser avaliado o pedido de acesso à informação em cada caso individual (CÂMARA DOS DEPUTADOS, 2021).

A LGPD é a temática específica, estudada na próxima seção, o que dá continuidade à discussão aqui apresentada.

2 LEI DE PROTEÇÃO DE DADOS: NO BRASIL E NO MUNDO

2.1 As inovações tecnológicas e a proteção jurídica dos dados pessoais no ciberespaço: uma necessidade mundial

A existência de um contrato social próprio, criado pelos próprios usuários, foi uma utopia idealizada e romantizada pelos que argumentavam que o ciberespaço não deveria sofrer interferências governamentais (legislativas ou jurídicas). Esta ideia é impossível de se sustentar, pela impossibilidade de se obter qualquer tipo de consenso entre o grupo heterogêneo de usuários da Rede, e deu reconhecimento de que há "[...] a necessidade de regras e princípios para o convívio entre os 'cidadãos' desse 'espaço'" (LEONARDI, 2019, p. 26).

Para Castells (2011), a sociedade informacional é fruto da revolução tecnológica "[...] eclodida vigorosamente a partir do final do século XX [e] cada vez mais se baseia no modelo econômico denominado de economia movida a dados ("data-driven economy"), onde as informações [...] são insumos essenciais". Porém, mesmo que se entenda as contribuições do desenvolvimento tecnológico, segundo o autor, surgem situações negativas decorrentes do monitoramento e vigília constante da vida das pessoas.

Vive-se a era da informação. Vive-se em uma sociedade em que a informação é o elemento base para o desenvolvimento econômico e pode ser transmitida em quantidade e velocidade nunca vista. Harari (2017), em seu best-seller *Sapiens*, apresenta uma situação bastante intrigante: o mundo ainda seria familiar para um camponês que adormecesse, no ano 1000, por quinhentos anos, acordando de seu sono com a chegada dos marinheiros de Colombo no ano 1500, porém seria totalmente estranho a um marinheiro em situação similar ao ser despertado ao toque de um iPhone do século XXI.

Da mesma forma, Castells (2011, p. 53-54) apresenta a diferenciação entre os modos de desenvolvimento anteriores à revolução causada pela internet (agrária e industrial) e destacada a centralidade atual da informação, confirmando que as TICs foram determinantes para a evolução do capitalismo e a sua atual dimensão.

> Cada modo de desenvolvimento é definido pelo elemento fundamental à promoção da produtividade no processo produtivo. Assim, no modo agrário

> de desenvolvimento, a fonte do incremento de excedente resulta dos aumentos quantitativos da mão-de-obra e dos recursos naturais (em particular) no processo produtivo, bem como da dotação natural desses recursos. No modo de desenvolvimento industrial, a principal fonte de produtividade reside na introdução de novas fontes de energia e na capacidade de descentralização do uso de energia ao longo dos processos produtivo e de circulação. No novo modo informacional de desenvolvimento, a fonte de produtividade acha-se na tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos. [...], o que é específico ao modo informacional de desenvolvimento é a ação de conhecimentos sobre os próprios conhecimentos como principal fonte de produtividade. O processamento da informação é focalizado na melhoria da tecnologia do processamento da informação como fonte de produtividade, em um círculo virtuoso de interação entre as fontes de conhecimentos tecnológicos e a aplicação da tecnologia para melhorar a geração de conhecimentos e o processamento da informação.

Considerando as características peculiares (meio de comunicação diferente em muitos aspectos da interação tradicional, por exemplo) e o alcance (ilimitado e globalizado) da Rede, observou-se, ainda na década de 1990, a necessidade da criação de um direito do ciberespaço, separado do direito convencional, que garantisse o cumprimento dos direitos fundamentais, principalmente o direito fundamental à proteção de dados pessoais.

Ao escrever sobre a revolução digital e sua influência no judiciário, Araújo e Gomes (2022) afiançam que a aceleração tecnológica impacta o comportamento das pessoas, bem como os setores mais tradicionais da economia. Os autores apresentam a “quarta revolução industrial”[9], que trata da “[...] revolução tecnológica que alterará fundamentalmente a maneira como vivemos, trabalhamos e nos relacionamos uns com os outros” (ARAÚJO; GOMES, 2022, p. 107 [tradução nossa][10]). Segundo os autores, essa transformação digital:

> [...] tem sido recorrentemente mencionada e trazida à tona, dada a sua relevância não somente de impacto em nossas vidas como também pela sua escala, abrangência e complexidade. Iniciou-se no bojo da terceira revolução industrial, então chamada de Revolução Digital, que mudou radicalmente a sociedade, as formas de comunicação e o estado do mundo globalizado (ARAÚJO; GOMES, 2022, p. 107).

O sociólogo Castells (2011, p. 119) denomina como “Terceira Revolução Industrial” e apresenta seus conceitos:

---

[9] Termo apresentado por Klaus Schwab no Fórum Econômico Mundial de 2016.
[10] “technological revolution that will fundamentally alter the way we live, work, and relate to one another”

> Uma nova economia surgiu em escala global no último quartel do século XX. Chamo-a de informacional, global e em rede para identificar suas características fundamentais e diferenciadas e enfatizar sua interligação. É informacional porque a produtividade e a competividade de unidades ou agentes nessa economia (sejam empresas, regiões ou nações) dependem basicamente de sua capacidade de gerar, processar e aplicar de forma eficiente a informação baseada em conhecimentos.
> É global porque as principais atividades produtivas, o consumo e a circulação, assim como seus componentes (capital, trabalho, matéria--prima, administração, informação, tecnologia e mercados) estão organizados em escala global, diretamente ou mediante uma rede de conexões entre agentes econômicos. É rede porque, nas novas condições históricas, a produtividade é gerada, e a concorrência é feita em uma rede global de interação o entre redes empresariais.

Neste contexto, em que a inovação tecnológica, indiscutivelmente, dinamiza a comunicação, por um lado, e potencializa a captação, o armazenamento e envio de dados e informações, abusos podem ser cometidos, por outro lado. Sobre as inovações tecnológicas e a necessidade de o Direito intervir pela proteção jurídica dos dados pessoais no ciberespaço, Araújo e Gomes (2022, p. 11) afirmam que

> [...] os novos tempos chegam e o verdadeiro desafio de quem atua profissionalmente com o Direito é o de identificar, nas inovações tecnológicas, as oportunidades de progresso para a humanidade. [...] a fim de promover modelos inovadores de aplicação do Direito em linha com a eficiência e o atendimento aos anseios sociais.

No mesmo viés, Barroso (2022, p. 33) afiança que

> A internet trouxe a democratização do acesso à informação e ao espaço público, mas suprimiu, em ampla medida, a intermediação do jornalismo profissional, que fora a marca do último século. Com ela vieram, também, a invasão de privacidade, a difusão da mentira deliberada e de notícias falsas, condutas utilizadas como estratégia de chegada ao poder e de desmoralização das instituições democráticas.

Boff e Fortes (2014) já afiançavam, mesmo antes da LGPD, que a construção de um modelo normativo de governança do ciberespaço deveria, indispensavelmente, respeitar as premissas de construção da Web, sem que ocorram rupturas paradigmáticas com a arquitetura adotada com a sua constituição e com a constante adaptação que culminou na constituição da cibercultura e do ciberespaço.

Além disso, segundo Bortali (2020), atualmente, todo indivíduo já está acostumado a realizar cadastros *on-line* para acessar conteúdos digitais, incluindo os sítios eletrônicos de serviços governamentais, que exigem cadastro completo para

acessar determinada informação. Iramina (2020, p. 92) ressalta, no mesmo sentido, que:

> Em uma sociedade cada vez mais informatizada, na qual o fluxo de dados se tornou um componente crucial para o comércio, as comunicações e as interações sociais, a proteção de dados pessoais passou a ser uma preocupação para grande parte dos países. Nesse contexto, muitos países têm adotado novas regras de proteção de dados ou modernizado as que já tinham, como Coreia do Sul, Chile, Tailândia, Índia, Indonésia e Brasil. Atualmente, já são mais de cem países com marcos regulatórios para proteção de dados pessoais em todo o mundo.

Assim, entende-se que a era da informação disponibiliza maravilhosas inovações tecnológicas à sociedade, porém, recentemente os impactos, positivos e negativos, destes avanços começam a ser mensurados. “Toda beleza e eficiência dos recursos tecnológicos e das possibilidades de interação travam uma batalha fervorosa com a privacidade, lembrando que esta já possui garantia constitucional [...]” (PINHEIRO, 2019). Micheletti e Borges (2021) concordam que a sociedade brasileira está passando por profundas e aceleradas transformações, impulsionadas pelas inovações tecnológicas.

Boff e Fortes (2014), ao fazer referência à privacidade e à proteção dos dados pessoais no ciberespaço, afirmam que a evolução tecnológica e a inclusão digital (democratização do acesso à internet) refletiram na exposição maciça de informação no ciberespaço, o que “[...] oferece novas e diferentes possibilidades de futuro, mas pode representar uma afronta aos direitos fundamentais da privacidade e da proteção aos dados pessoais”.

Bortali (2020) informa que, ao longo da história, diversas criações legislativas foram promulgadas a fim de proteger dados, citando as leis: do Estado Alemão de Hesse (1970), Lei de Dados da Suécia (1973), Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974), e Lei Federal de Proteção de Dados da Alemanha (1977). Porém, foi na União Europeia (UE) que o Brasil – e outros países, já que é a UE que apresenta a base legal mais completa sobre o tema, sendo um exponencial na legislação sobre proteção de dados – buscou tendências para a constitucionalização da proteção de dados, deixando manifesta a convergência de orientações entre as legislações adotadas.

A exemplo do ocorrido no cenário mundial, a Lei Geral de Proteção de Dados (LGPD) foi estabelecida no Brasil para prezar rigorosamente pela proteção à

privacidade e dar proteção jurídica aos dados pessoais (BASTOS; BASI; CASSI, 2021). O surgimento de regulamentações para proteção de dados, no mundo e no Brasil, tem como motivação os avanços do modelo de negócios da economia digital (PINHEIRO, 2021), as inovações tecnológicas, o alargamento do uso da internet (RUSSO, 2019), fomentado pela pandemia do Covid-19 e pela necessidade de isolamento social (PINHEIRO, 2021).

Apresenta-se, *a priori*, um breve histórico, que demonstrará os antecessores legais da proteção jurídica aos dados pessoais no Brasil. Além disso, na tentativa de demonstrar a operacionalização da proteção de dados pessoais, faz-se, nesta seção, a comparação entre a lei brasileira e a lei europeia e, após, a apresentação de elementos da proteção de dados pessoais em outros países de relevância econômica e tecnológica, Estados Unidos e Japão.

2.2 Antecessores legais da LGPD no Brasil: breve resumo

De acordo com a lei, o objetivo da LGPD é proteger os direitos fundamentais de liberdade e privacidade dos brasileiros quanto aos seus dados pessoais, inclusive nos meios digitais, protegendo dados pessoais de pessoas naturais. Aplicando-se a todo território nacional, a lei inclui tanto pessoas jurídicas de direito público quanto privado. Cardoso (2020) enfatiza, entretanto, que a LGPD não é a primeira a tratar do assunto no país. O juiz federal afirma que a temática da proteção dos dados é anterior ao alargamento do acesso à internet e ao uso de meios digitais para fins comerciais.

> Assim, a LGPD não é a primeira lei no Brasil que regula e protege os direitos dos titulares de dados pessoais, sendo que a temática é objeto de atenção do Legislativo há alguns anos, mesmo antes do enquadramento jurídico da matéria em sua amplitude atual (CARDOSO, 2020).

Da mesma forma, Garcia et al. (2020) citam a Constituição Federal (CF/88), o Código de Defesa do Consumidor (Lei n. 8.078/1990), o Decreto do Comércio Eletrônico (Lei n. 9.507/1997), a Lei de Acesso à Informação (Lei n. 12.527/2011), a Lei do *Habeas Data* (Decreto n. 7.962/2013), o Marco Civil da Internet (Lei n. 12.965/2014), como textos antecessores à LGPD, mas que, de alguma forma regem o direito à privacidade e dão proteção jurídica aos dados pessoais.

Como tutela ao direito da personalidade da pessoa natural, o CC – Lei n. 10.406 – dispõe conteúdo em defesa da dignidade da pessoa humana, na forma da lei, intransmissíveis e irrenunciáveis, em seus arts. 11 e 21 (como já apresentado). De forma indireta, o próprio Código Tributário Nacional (CTN; Lei n. 5.172, de 25 de outubro de 1966) veda à Fazenda (e seus servidores) que divulguem informações acerca da situação econômica/ financeira ou sobre as negociações ou atividades dos contribuintes. Conforme Art. 198, Lei Complementar n. 104, de 10 de janeiro de 2001:

> Art. 198. Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades.

Cardoso (2020) tece um rápido resumo histórico e cronológico sobre as leis e normas que antecederam a promulgação da LGPD, oportunamente apresentado. Primeiramente, o autor destaca que "[...] o Código de Defesa do Consumidor (Lei nº 8.078/90) contém as primeiras normas sobre a regulação da formação dos bancos de dados no Brasil", sendo, portanto, uma das primeiras leis brasileiras a tratar da matéria dos dados, datada de 1990. Sobre o Código de Defesa do Consumidor (CDC), Cardoso (2020) defende que as relações jurídicas estabelecidas entre pessoas, de ordem natural ou empresarial, são perpassadas por dados.

> As relações jurídicas mantidas entre uma pessoa (natural ou jurídica, de direito público ou privado) que realiza atividades de tratamento de dados e outra pessoa (natural) titular desses dados, em regra, enquadra-se no conceito de relação de consumo submetida ao microssistema do Código de Defesa do Consumidor (CARDOSO, 2020, s/p).

Além do CDC, outra legislação anterior à LGPD, e que também trata de dados, é a LAI – amplamente discutida na seção 2.2 e 2.3. A LAI, destaca-se, representa um marco significativo, pois permite a fiscalização de processos financeiros, administrativos, fiscais e quaisquer outras atividades realizadas pelo poder público mas que sejam de interesse coletivo. Assim, a LAI obriga a Administração Pública a dar publicidade de seus atos administrativos, possibilitando a fiscalização, de ações dos poderes Executivo, Legislativo e Judiciário.

Através dos breves apontamentos sobre os mecanismos legais antecessores à LGPD, Cardoso (2020) enfatiza o diálogo das fontes, isto é, as outras legislações que

se entrecruzam nos artigos da Lei Geral. Garcia et al. (2020) afiançam que a LGPD, inspirada na RGPD, é a mais específica e exclusiva lei e, por isso, tem principal relevância.

É importante destacar que a LGPD é um marco legal de grande impacto, atingindo tanto as instituições privadas como as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação, por qualquer meio, que envolva o tratamento de informações classificadas como dados pessoais de pessoa natural ou jurídica.

2.3 Direito Comparado: LGPD e RGPD

Esclarece-se, primeiramente, que a análise comparativa entre os modelos jurídicos exige, por finalidade, clareza metodológica. Por essa razão é que se adota o método funcional de direito comparado, apresentada por Cury (2014, p. 178), onde se procura respeitar o núcleo desse método, que pressupõe a compatibilidade do que se compara, isto é, de elementos que preencham as mesmas funções jurídicas. Uma das formas de demonstrar as semelhanças e diferenças (comparar, portanto) duas ou mais regras é por meio da apresentação de quadros – o que será feito.

No Brasil, ainda em 2010, houve a primeira consulta pública sobre a versão do anteprojeto de lei que, mais tarde, seria a LGPD. Em 14 de agosto de 2018, em complementação ao Marco Civil da Internet, a Lei n. 13.709 foi aprovada, sob a alcunha de Lei Geral de Proteção de Dados, entrando em vigência em 18 de setembro de 2020 (PINHEIRO, 2021). Da mesma forma, a Medida Provisória (MP) n. 869/18, convertida na Lei n. 13.853/2019, estabeleceu a Autoridade Nacional de Proteção de Dados (ANPD). No entendimento de Pinheiro (2021), a LGPD não é perfeita, cabendo à ANPD esclarecer alguns pontos. Mendes (2019, p. 35) ressalta que:

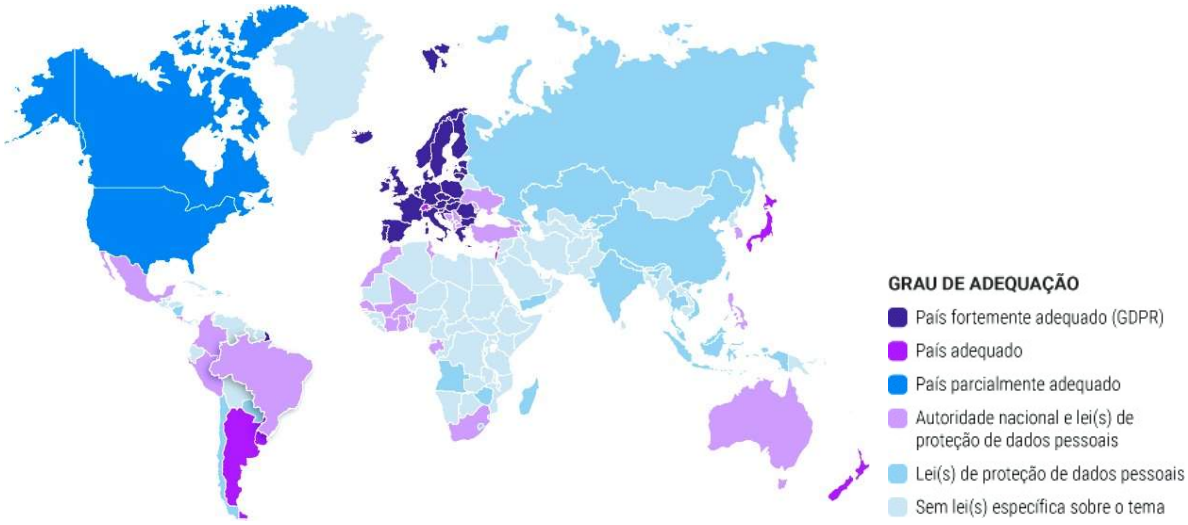
> A disciplina da proteção de dados pessoais emerge no âmbito da sociedade de informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. A função não é a de proteger os dados per se, mas, sim, a pessoas que é titular desses dados.

Elucida-se que o Regulamento Geral de Proteção de Dados (RGPD), aprovado em 2016, entrou em vigor em maio de 2018 (em substituição a Diretiva de Proteção

de Dados, de 1995), sendo o principal regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na UE e Espaço Econômico Europeu. A UE é um bloco econômico de natureza supranacional, com um modelo de Direito Comunitário, com escopo territorial abrangendo, atualmente, 27 Estados membros – Alemanha, Áustria, Bélgica, Bulgária, Chipre, Croácia, Dinamarca, Eslováquia, Eslovênia, Espanha, Estônia, Finlândia, França, Grécia, Holanda, Hungria, Irlanda, Itália, Letônia, Lituânia, Luxemburgo, Malta, Polônia, Portugal, República Tcheca, Romênia, Suécia (o Reino Unido já não faz parte da UE).

Ainda, importa trazer o mapa apresentado pelo Serpro (2022a)[11], que demonstra a abrangência das leis da proteção de dados pessoais no mundo (figura 1).

Figura 1 – Mapa da abrangência de leis de proteção de dados pessoais: mundo



Fonte: Serpro (2022b).

Wachowicz (2020) inicia sua análise dos princípios jurídicos de tratamento de dados pessoais comparando a LGPD e a RGPD, pois afirma que a análise simultânea e comparativa dos ordenamentos brasileiro e europeu é justificável, em razão da similaridade dos dois textos. Tal similaridade não é, obviamente, acidental, como já

[11] Maior empresa pública de Tecnologia da Informação do mundo, responsável por mais de 90% das soluções digitais do Estado brasileiro e líder do mercado nacional de TI. O Serpro tem compromisso com a segurança e garantia da revolução tecnológica brasileira e é protagonista na LGPD, auxiliando o país na adequação aos princípios da lei (SERPRO, 2022a).

comentado. O Brasil – em decorrência das exigências europeias em manter negociações comerciais apenas com países que, da mesma forma que eles, protegessem os dados pessoais legalmente – editou uma legislação inspirada no modelo europeu, a exemplo de outros países. A promulgação da RGPD "[...] ocasionou um 'efeito dominó', visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a UE também deveriam ter uma legislação de mesmo nível [...]" (PINHEIRO, 2021, s/p). Segundo Iramina (2020, p. 92):

> Considerando que empresas geralmente operam extraterritorialmente, a convergência global das normas que regulam a proteção de dados tem-se mostrado fundamental, não só para facilitar o fluxo de dados e, consequentemente, o comércio e a cooperação entre as organizações e as autoridades públicas, mas também para aumentar o nível de proteção de dados pessoais em todo o mundo. Não por acaso, grande parte das mais recentes legislações de proteção de dados são inspiradas no Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, em vigor desde maio de 2018, e, portanto, apresentam características similares, como: 1) legislação geral e abrangente (em vez de normas setoriais); 2) proteção de direitos individuais; 3) autoridade supervisora independente.

Neste mesmo sentido, para corroborar tais afirmações, Almeida e Soares (2022, p. 30) afirmam que:

> No Brasil, em 14 de agosto de 2018, entrou em vigor a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, publicada no Diário Oficial da União (D.O.U.) em 15/8/20183 . A Lei de Proteção de Dados Pessoais (LPD), buscou no então recente Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* – GDPR), sigla em inglês da União Europeia, orientações para a elaboração de normas para a proteção dos dados pessoais, de indivíduos [...].

Uma observação a ser feita diz respeito à divisão de ambas as leis. A LGPD está dividida em 10 capítulos, com 65 artigos, já a RGPD possui 11 capítulos, com 99 artigos. Sendo assim, a lei nacional brasileira é mais enxuta, deixando alguns aspectos em aberto, como o caso dos prazos de cumprimento de decisões – a RGPD fixa 72 horas, a LGPD prevê prazo razoável. Porém, muito embora existam diferenças, a LGPD e o GDPR têm muito mais pontos de convergência do que de divergência.

Sob a perspectiva regulatória, ambas as leis adotam uma abordagem estratégica para o tratamento de dados pessoais, incentivando e regulamentando as boas práticas de privacidade das empresas e instituições. Outras semelhanças gerais

são: “[...] a adoção de uma legislação abrangente sobre o tema, o estabelecimento de direitos fundamentais para os titulares dos dados e a criação de uma autoridade supervisora independente” (IRAMINA, 2020, p. 93).

O quadro 1 apresenta, trecho a trecho as semelhanças das atividades de gerenciamento de privacidade e proteção de dados pessoais encontradas nas duas leis, RGPD e LGPD respectivamente.

Quadro 1 – Quadro comparativo entre RGPD e LGPD

Categorias	**Atividades de Gerenciamento de Privacidade e Proteção de Dados Pessoais**	**GDPR**	**LGPD**
1. Manter estrutura de governança	Atribuir a responsabilidade pela privacidade e proteção dos dados a um indivíduo (por exemplo, *Privacy Officer*, *Privacy Counsel*, DPO (Data Protection Officer ou encarregado da proteção dos dados), entre outros)	Art. 27	Art. 61
	Designar um encarregado de proteção de dados/DPO com uma função independente	Art. 37, 38	Art. 41
	Atribuir responsabilidade pela privacidade e proteção dos dados em toda a organização (por exemplo, Rede de Privacidade, *Privacy Champions* etc)	Art. 24, §2º	Art. 50
	Manter funções e responsabilidades dos responsáveis pela privacidade e proteção dos dados (por exemplo, descrições de cargo)	Art. 39	Art. 41, §2º
	Conduzir comunicação regular entre o *privacy office*, *privacy network* e outros responsáveis pela privacidade e proteção de dados	Art. 38	Art. 41, §2º
	Realizar uma avaliação de risco de privacidade e proteção de dados da empresa	Art. 24, 39	Art. 50
2. Manter inventário de dados pessoais	Manter um inventário de dados pessoais que são tratadas (5W2H dos dados pessoas)	Art. 30	Art. 37
	Manter fluxogramas dos fluxos de dados (por exemplo, entre sistemas, entre processos, entre países)	Art. 30	Art. 37
	Manter registros do mecanismo de transferência usado para fluxos de dados transfronteiriços (por exemplo, cláusulas contratuais padrão, regras corporativas vinculativas (BCR), aprovações de órgãos reguladores, se necessário, entre outros)	Art. 45, 46, 49	Art. 33
	Adotar Regras Corporativas Vinculativas (BCR - *Binding Corporate Rules*) como um mecanismo de transferência de dados	Art. 46, 47	Art. 33
	Adotar contratos como um mecanismo de transferência de dados (por exemplo, cláusulas contratuais padrão)	Art. 46	Art. 33
	Obter a aprovação do regulador e/ou autoridade para transferência de dados	Art. 46	Art. 33, 36
	Adotar uma das bases legais para transferência de dados	Art. 45, 48, 49	Art. 33
	Manter EU-US *Privacy Shield* como um mecanismo de transferência de dados	Art. 46	
3. Manter uma política de privacidade e proteção de dados	Manter uma política de privacidade e proteção de dados	Art. 5, 24, 91	Art. 6, 14, 15, 50
	Documentar a base legal para o tratamento de dados pessoais	Art. 6, 9, 10	Art. 7, 10, 11,14
	Integrar ética ao tratamento de dados (códigos de conduta, políticas e outras medidas)	Art. 40	Art. 50, II
	Manter um código de conduta organizacional que inclua privacidade e proteção de dados	Art. 40	Art. 50, II

Categorias	Atividades de Gerenciamento de Privacidade e Proteção de Dados Pessoais	GDPR	LGPD
4. Incorporar privacidade de dados nas operações	Manter políticas / procedimentos para coleta e uso de dados pessoais e dados sensíveis	Art. 9, 10	Art. 11
	Manter políticas / procedimentos para coleta e uso de dados pessoais de crianças e menores	Art. 8, 12	Art. 14
	Manter políticas / procedimentos para manter a qualidade dos dados	Art. 5	Art. 6
	Manter políticas / procedimentos para a identificação de dados pessoais	Art. 30	Art. 37
	Manter políticas / procedimentos para revisar o tratamento total ou parcialmente por meios automatizados	Art. 12, 22	Art. 20
	Manter políticas / procedimentos para usos secundários de dados pessoais	Art. 6, 13, 14	
	Manter políticas / procedimentos para obter consentimento válido	Art. 6, 7, 8	Art. 8
	Manter políticas / procedimentos para destruição segura de dados pessoais	Art. 5	Art. 6
	Integrar privacidade e proteção de dados em práticas de retenção de registros	Art. 5	Art. 16
	Integrar privacidade e proteção de dados em práticas de marketing direto	Art. 21, recital 43	
	Integrar a privacidade e proteção de dados nas práticas de marketing por email	Art. 21	
	Integrar a privacidade e proteção de dados às práticas de telemarketing	Art. 21	
	Integrar a privacidade e proteção de dados às práticas de marketing digital (por exemplo, celular, mídia social, publicidade comportamental)	Art. 21, recital 43	
	Integrar a privacidade de dados ao uso de práticas de mídia social da organização	Art. 8	
	Integrar a privacidade e proteção de dados em práticas para divulgação e para fins de aplicação da lei		Art. 50, §3º
	Integrar a privacidade e proteção de dados nas práticas de pesquisa	Art. 21, 89	Art. 13
5. Manter programa de treinamento e conscientização	Conduzir treinamento em privacidade e proteção de dados	Art. 39	Art. 41, 50
	Conduzir treinamento de privacidade e proteção de dados para atividades especificas	Art. 43	Art. 41, III
	Incorporar a privacidade e proteção dos dados ao treinamento operacional, como RH, segurança, call center	Art. 39	Art. 41, III
	Oferecer treinamento / conscientização em resposta a questões / tópicos que vierem a surgir oportunamente	Art. 39	Art. 41, III
	Manter e disponibilizar material de conscientização de privacidade e proteção de dados (por exemplo, pôsteres e vídeos)	Art. 39	Art. 41, III
	Realizar eventos de conscientização de privacidade e proteção de dados (por exemplo, um dia / semana anual de privacidade de dados)	Art. 39	Art. 41, III
	Avaliar a participação em atividades de treinamento em privacidade e proteção de dados (por exemplo, número de participantes, pontuação)	Art. 39	Art. 41, III
	Fornecer educação e treinamento contínuos para o *Privacy Office* e / ou DPOs (por exemplo, conferências, seminários on-line, palestrantes convidados)	Art. 39	Art. 41, III
6. Gerenciar riscos de segurança da informação	Integrar o risco de privacidade e proteção de dados nas avaliações de risco de segurança	Art. 32	Art. 50
	Integrar privacidade e proteção de dados em uma política de segurança da informação	Art. 5, 32	Art. 6, 46, 49
	Manter medidas técnicas de segurança (por exemplo, detecção de intrusões, firewalls, monitoramento)	Art. 32	Art. 46
	Manter medidas para criptografar dados pessoais	Art. 32	

Categorias	Atividades de Gerenciamento de Privacidade e Proteção de Dados Pessoais	GDPR	LGPD
	Manter procedimentos para restringir o acesso a dados pessoais (por exemplo, acesso baseado em função, segregação de funções)	Art. 32	
	Manter medidas de segurança de recursos humanos (por exemplo, pré-triagem, avaliações de desempenho)		Art. 47
	Conduzir testes regulares quanto ao desempenho de segurança de dados	Art. 32	
	Manter uma certificação de segurança (por exemplo, ISO)	Art. 43	
7. Gerenciamento de riscos de terceiros	Manter política de privacidade e proteção de dados para terceiros (por exemplo, clientes, fornecedores, processadores, afiliados)	Art. 28, 32	Art. 39
	Manter procedimentos para executar contratos ou acordos com todos os processadores	Art. 28, 32	Art. 39
	Realizar a devida diligência em torno da postura de privacidade e proteção de dados, segurança de dados de fornecedores / operadores em potencial	Art. 28	Art. 39
	Conduzir diligência em torno da postura de privacidade e proteção de dados, segurança de dados de fornecedores / processadores	Art. 28	Art. 39
8. Atualizar os avisos	Manter um aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização	Art. 8, 13, 14	Art. 6, 7, 9, 14
	Fornecer aviso de privacidade e proteção de dados em todos os pontos em que os dados pessoais são coletados	Art. 13, 14, 21	Art. 9, 14
	Fornecer aviso nas comunicações de marketing (por exemplo, e-mails, folhetos, ofertas)	Art. 13, 14	Art. 6
	Fornecer aviso em contratos e termos	Art. 13, 14	Art. 6
	Manter scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e proteção de dados	Art. 13, 14	Art. 6
9. Responder a solicitações e reclamações dos Titulares de Dados	Manter procedimentos para tratar de reclamações	Art. 24, §2º	Art. 50
	Manter procedimentos para responder a solicitações de acesso a dados pessoais	Art. 15	Art. 6, 18, 19
	Manter procedimentos para responder a solicitações e / ou fornecer um mecanismo para os indivíduos atualizarem ou corrigirem seus dados pessoais	Art. 16, 19	Art. 18
	Manter procedimentos para responder a pedidos de exclusão, restrição ou oposição ao processamento	Art. 7, 18, 21	Art. 8
	Manter procedimentos para responder a pedidos de informações	Art. 12	Art. 18
	Manter procedimentos para responder a solicitações de portabilidade de dados	Recital 45, 47, 55 Art. 20	Art. 18
	Manter procedimentos para responder a pedidos a serem esquecidos ou para apagar dados	Recital 45, 47, 53, 54 Art. 17, 19	Art. 18
	Manter perguntas frequentes (FAQ) para responder a perguntas de indivíduos	Art. 13,14	Art. 6
10. Monitorar novas práticas operacionais	Integrar o Privacy by Design no desenvolvimento de sistemas e produtos da organização	Art. 25	Art. 46
	Manter diretrizes e modelos do RIPD(Relatório de Impacto à Proteção dos Dados Pessoais)/ DPIA (*Data Privacy Impact Assessment*)/ PIA (*Privacy Impact Assessment*)	Recital 70a, Art. 35	Art. 5, XVII, 38
	Conduzir RIPD/ DPIA/ PIA para novos programas, sistemas, processos que envolva tratamento de dados pessoais	Recital 66a, 70-72, 74 Art. 5, 6, 25, 35	Art. 38

Categorias	Atividades de Gerenciamento de Privacidade e Proteção de Dados Pessoais	GDPR	LGPD
	Conduzir RIPD/ DPIA/ PIA para alterações nos programas, sistemas ou processos existentes que envolva tratamento de dados pessoais	Art. 5, 6, 25, 35	
	Envolver as partes interessadas externas como parte do processo da RIPD/ DPIA/ PIA	Art. 35	
	Rastrear e solucionar problemas de proteção de dados identificados durante RIPD/ DPIA/ PIA	Art. 35	
	Relatar a análise e os resultados do RIPD/ DPIA/ PIA aos reguladores (quando necessário) e partes interessadas externas (se apropriado)	Art. 36	
11. Manter o programa de gerenciamento de violação de privacidade de dados	Manter um plano de resposta a incidentes / violações da privacidade de dados	Art. 33, 34	Art. 48, 5
	Manter um protocolo de notificação de violação (para as pessoas afetadas) e relatórios (para reguladores, agências de crédito, órgãos policiais)	Art. 12, 33, 34	Art. 48
	Manter o registro quanto o rastreamento de incidentes / violações de privacidade e proteção de dados	Art. 33	
12. Monitoramento de tratamento de dados	Conduzir autoavaliações de gerenciamento de privacidade e proteção de dados	Art. 24,25, 39	Art. 50
	Conduzir auditorias internas do programa de privacidade e proteção de dados (ou seja, auditoria operacional do *Privacy Office*)	Art. 25	Art. 50
	Conduzir *walk-throughs* (treinamentos/ orientações) periódico	Art. 39	Art. 41,III
	Conduzir avaliações com base em eventos externos, como reclamações / violações, entre outros	Art. 12, 34	Art. 18, 46, 48
	Envolver a auditoria externas para avaliações independentes	Art. 25	Art. 50
	Manter a documentação como evidência a fim de demonstrar conformidade e / ou prestação de conta	Art. 5, 24	Art. 6, 50
	Manter certificações, acreditações ou selos de proteção de dados para demonstrar conformidade com os reguladores	Art. 42	
13. Rastrear critérios externos	Identificar e/ou monitorar as obrigatoriedades/ requerimento e as melhorias contínuas de conformidade com a privacidade e e proteção de dados, por exemplo, lei, jurisprudência, códigos etc.	Art. 39	Art. 50
	Documentar as decisões em torno de novos requisitos/exigências, incluindo sua implementação ou qualquer justificativa por trás de decisões para não implementar mudanças/ recomendações	Art. 25	

Fonte: Adaptado de Yun (2020).

O que se disse até aqui basta, por si só, a fim de demonstrar que a proteção de dados pessoais é hoje um domínio em que, a par da circulação de modelos jurídicos através das fronteiras – de que o RGPD e a LGPD constituem um exemplo paradigmático –, deparamos também com conceções muito diversas nos sistemas jurídicos nacionais; e em que a comparação jurídica, permitindo descortinar as semelhanças e as diferenças entre esses sistemas jurídicos e explicá-las por apelo aos seus fundamentos e origens, constitui um instrumento essencial para a sua compreensão.

2.4 A proteção jurídica de dados pessoais em perspectiva: Estados Unidos e Japão

Por sua relevância econômica e tecnológica, tanto nos Estados Unidos (EUA) quanto no Japão a temática da proteção jurídica de dados pessoais é importante e amplamente discutida há décadas. Apresentam-se informações pertinentes e traçam-se divergências e convergências entre as leis dos EUA e do Japão com a RGPD e LGPD, da UE e Brasil, respectivamente.

2.4.1 Estados Unidos

Os Estados Unidos da América (EUA) são, mesmo em meio às muitas incertezas do cenário global pós pandemia, a maior economia do mundo e o terceiro país com maior população. Seu produto interno bruto (PIB) voltou a crescer no último trimestre de 2022 (2,6%) e o dólar (moeda corrente norte americana) continua se fortalecendo (IPEA, 2022).

Na década de 1970, o país foi marcado pelo caso do *National Data Center*. A proteção jurídica de dados pessoais foi posta em debate após ser proposta a unificação das bases de dados e o uso das TICs para armazenamento e processamento de grande volume de dados pessoais. Parte da população norte americana se opôs à centralização de conteúdos e o congresso nacional acabou não apoiando a criação do *National Data Center* até que fosse provada a proteção da privacidade e garantida proteção aos cidadãos.

Nenhuma lei foi criada após este episódio e as leis de proteção de dados pessoais nos Estados Unidos ainda são fragmentadas e liberais, diferentemente do que ocorre, em particular, nos Estados-Membros da União Europeia e no Brasil, que apresentam uma regulamentação de índole fortemente abrangente, pormenorizada e protetora. A proteção jurídica dos dados nos EUA é, portanto, contrastante com a praticada e imposta pela LGPD e RGPD.

Segundo Cardoso (2020), nos EUA, a legislação que trata sobre a temática da proteção dos dados conta com uma série de leis e não com uma lei geral, como é o caso do Brasil e da União Europeia. Detalha-se, convenientemente, que, tanto no Brasil quanto na UE, a noção de dados pessoais sujeitos a proteção é muito ampla,

entendidos como “toda a informação relativa a uma pessoa singular identificada ou identificável”, porém a noção norte-americana, muito mais restritiva, confere particular ênfase à proteção da privacidade dos indivíduos perante as agências públicas – há o *Privacy Act of 1974*, cujas normas limitam a coleta de dados dos cidadãos pelo governo.

Assim, enquanto no Brasil e nos países europeus a privacidade é essencialmente uma exigência da dignidade da pessoa humana, “[...] a salvaguardar em particular perante entidades privadas, os norte-americanos veem antes nela uma expressão da liberdade individual, primariamente ameaçada pelo Estado” (WACHOWICZ, 2020, p. 14).

Ainda, RGPD e LGPD baseiam-se no princípio do consentimento, enquanto no Direito norte-americano, o recente aprovado *California Consumer Privacy Act* (Lei de Privacidade do Consumidor da California) limita-se a acolher nesta matéria um direito de *opting-out* (optar para sair), nos termos do qual o consumidor pode recusar a possibilidade de venda a terceiros da sua informação pessoal.

O direito ao esquecimento – tão caro ao RGPD e à LGPD – também não encontra qualquer correspondência no Direito norte-americano. Encontra-se, no entanto, e de forma contrária, que o tratamento de dados alheios faz parte do direito à liberdade de expressão, defendido como fulcral e reiteradamente blindado por tribunais federais estadunidenses, protegido pela 1ª Emenda à Constituição norte-americana.

Há, porém, tramitando desde 30 de dezembro de 2022 (após ser aprovado pelo Comitê de Energia e Comércio da Câmara em 21 de junho de 2022) a *American Data Privacy and Protection Act* (ADPPA), que seria uma lei federal abrangente de proteção de dados e substituiria a maioria das leis estaduais que regem a privacidade do cidadão estadunidense. A promulgação da ADPPA se aplicaria amplamente a organizações e empresas que operam nos Estados Unidos. As principais definições na legislação proposta estão apresentadas no quadro 2.

Quadro 2 – Definições da ADPPA: uma prévia

Consentimento expresso afirmativo	O termo "consentimento expresso afirmativo" significa um ato afirmativo por um indivíduo que comunica claramente a autorização dada livremente, específica e inequívoca do indivíduo para um ato ou prática após ter sido informado, em resposta a uma solicitação específica solicitação de uma entidade coberta [...].

Autenticação	O termo “autenticação” significa o processo de verificação de um indivíduo ou entidade para fins de segurança.
Informações biométricas	O termo "informações biométricas" significa quaisquer dados cobertos gerados a partir do processamento tecnológico das características biológicas, físicas ou fisiológicas únicas de um indivíduo que estão vinculadas ou razoavelmente vinculáveis a um indivíduo, incluindo: (i) impressões digitais; (ii) impressões de voz; (iii) varreduras de íris ou retina; (iv) mapeamento facial ou manual, geometria ou modelos; ou (v) andar ou identificar pessoalmente os movimentos físicos. EXCLUSÃO.—O termo "informações biométricas" não inclui: (i) uma fotografia digital ou física; (ii) uma gravação de áudio ou vídeo; ou (iii) dados gerados a partir de fotografia digital ou física, ou gravação de áudio ou vídeo, que não possam ser usados para identificar um indivíduo.
Entidade coberta	O termo “entidade coberta” significa qualquer entidade ou qualquer pessoa, que não seja um indivíduo atuando em um contexto não comercial, que sozinho ou em conjunto com outros determina os propósitos e meios de coleta, processamento ou transferência de dados cobertos
Dados cobertos	O termo "dados cobertos" significa informações que identificam ou estão vinculadas ou razoavelmente vinculáveis, sozinhas ou em combinação com outras informações, a um indivíduo ou a um dispositivo que identifica ou está vinculado ou razoavelmente vinculável a um indivíduo , e pode incluir dados derivados e identificadores persistentes exclusivos.
Dados derivados	O termo "dados derivados" significa dados cobertos que são criados pela derivação de informações, dados, suposições, correlações, inferências, previsões ou conclusões de fatos, evidências ou outra fonte de informações ou dados sobre um indivíduo ou dispositivo de um indivíduo.
Dados sensíveis cobertos	O termo "dados confidenciais cobertos" significa os seguintes tipos de dados cobertos: (i) Um identificador emitido pelo governo, como um número de Seguro Social, número de passaporte ou número da carteira de motorista, que não é exigido por lei para ser exibido em público. (ii) Qualquer informação que descreva ou revele o passado, presente ou futuro da saúde física, saúde mental, deficiência, diagnóstico ou condição de saúde ou tratamento de um indivíduo. (iii) Um número de conta financeira, número de cartão de débito, número de cartão de crédito ou informações que descrevam ou revelem o nível de renda ou saldos de contas bancárias de um indivíduo, exceto que os últimos quatro dígitos de um número de cartão de débito ou crédito não serão considerados dados cobertos sensíveis. (iv) Informações biométricas. (v) Informação genética. (vi) Informações precisas de geolocalização. (vii) As comunicações privadas de um indivíduo, como correios de voz, e-mails, textos, mensagens diretas ou correio, ou informações que identifiquem as partes de tais comunicações, comunicações de voz, comunicações de vídeo e qualquer informação relacionada à transmissão de tais comunicações, incluindo telefone números chamados, números de telefone dos quais as chamadas foram feitas, a hora em que as chamadas foram feitas, a duração da chamada e as informações de localização das partes da chamada, a menos que a entidade coberta ou um prestador de serviços agindo em nome da entidade coberta seja o remetente ou um destinatário pretendido da comunicação. As comunicações não são privadas para os fins desta cláusula se tais comunicações forem feitas de ou para um dispositivo fornecido por um empregador a um funcionário, desde que tal empregador forneça um aviso visível de que tal empregador pode acessar tais comunicações. (viii) Credenciais de login de conta ou dispositivo ou códigos de segurança ou acesso para uma conta ou dispositivo.

	(ix) Informações que identificam o comportamento sexual de um indivíduo de maneira inconsistente com a expectativa razoável do indivíduo em relação à coleta, processamento ou transferência de tais informações. (x) Informações de calendário, informações de catálogo de endereços, registros de telefone ou texto, fotos, gravações de áudio ou vídeos, mantidos para uso privado por um indivíduo, independentemente de tais informações serem armazenadas no dispositivo do indivíduo ou acessíveis a partir desse dispositivo e serem backup em um local separado. Essas informações não são confidenciais para os fins deste parágrafo se forem enviadas de ou para um dispositivo fornecido por um empregador a um funcionário, desde que tal empregador forneça um aviso visível de que pode acessar essas informações. (xi) Uma fotografia, filme, gravação de vídeo ou outro meio semelhante que mostre a área privada nua ou vestida com roupas íntimas de um indivíduo. (xii) Informações revelando o conteúdo de vídeo solicitado ou selecionado por um indivíduo coletadas por uma entidade coberta que não seja prestadora de um serviço descrito na seção 102(4). Esta cláusula não inclui dados cobertos usados exclusivamente para transferências para medição de vídeo independente. (xiii) Informações sobre uma pessoa física quando a entidade ou prestador de serviço coberto tiver conhecimento de que a pessoa é um menor coberto. (xiv) Raça, cor, etnia, religião ou filiação sindical de um indivíduo. (xv) Informações que identificam as atividades online de um indivíduo ao longo do tempo e em sites ou serviços online de terceiros. (xvi) Quaisquer outros dados cobertos coletados, processados ou transferidos com a finalidade de identificar os tipos de dados cobertos listados nas cláusulas (i) a (xv).
Provedor de serviços	“uma pessoa ou entidade que coleta, processa ou transfere dados cobertos em nome de, e sob a direção de, uma entidade coberta com a finalidade de permitir que o provedor de serviços execute um serviço ou função em nome de , e sob a direção de tal entidade coberta.”
Entidade de coleta de terceiros	“uma entidade coberta cuja principal fonte de receita é derivada do processamento ou transferência dos dados cobertos que a entidade coberta não coletou diretamente dos indivíduos vinculados ou vinculáveis aos dados cobertos”.
Danos potenciais	Danos potenciais relacionados a indivíduos menores de 17 anos; Danos potenciais relacionados à publicidade, acesso ou restrições ao uso de moradia, educação, emprego, saúde, seguro ou oportunidades de crédito; Danos potenciais relacionados à determinação do acesso ou restrições ao uso de qualquer local de acomodação pública, particularmente quando esses danos se relacionam a características protegidas, incluindo raça, cor, religião, nacionalidade, sexo ou deficiência; e Danos potenciais relacionados a impactos díspares com base na raça, cor, religião, nacionalidade, sexo ou status de deficiência dos indivíduos.

Fonte: Adaptado de Patel et al. (2022).

Ao se visitar o texto completo do projeto de Lei, introduzido em 30 de dezembro de 2022 (Relatório nº 117-669), observa-se que o principal objetivo da proposta é fornecer aos consumidores direitos fundamentais de privacidade de dados, criar mecanismos de supervisão fortes e estabelecer uma aplicação significativa.

Esclarece-se que, embora a definição de entidade coberta seja inegavelmente ampla, a ADPPA identifica vários tipos diferentes de entidades com obrigações ou isenções adicionais. Para certas obrigações, as entidades abrangidas são divididas por “impacto” (ou seja, receita global anual e número de titulares de dados afetados pelas operações da entidade) e “relação com o titular dos dados” (por exemplo, relações diretas, com terceiros ou prestadores de serviços). A título de exemplo, uma entidade “grande” é definida como aquela com receita bruta anual de pelo menos US$ 250 milhões e que coletou dados cobertos em mais de 5 milhões de indivíduos ou dispositivos ou coletou dados confidenciais cobertos de mais de 100.000 indivíduos ou dispositivos.

É importante ressaltar que tanto os dados dos funcionários quanto os dados disponíveis publicamente estão excluídos desta definição. Certos tipos de dados cobertos são definidos como dados cobertos confidenciais, que incluiriam identificadores do governo (como carteira de motorista ou números de seguro social), bem como informações "tradicionalmente" confidenciais relacionadas a saúde, geolocalização, finanças, credenciais de login, raça, e história ou identidade sexual. Os dados confidenciais também podem incluir outras categorias, como dados de exibição de televisão, imagens íntimas e “informações que identificam as atividades online de um indivíduo ao longo do tempo ou em sites ou serviços online de terceiros”.

Ainda, uma entidade de coleta de terceiros seriam obrigadas a fornecer aos consumidores um aviso de sua atividade e se registrar na *Federal Trade Commission*[12] (FTC) se processarem dados pertencentes a mais de 5.000 indivíduos ou dispositivos que possam ser razoavelmente vinculados a um indivíduo, bem como fornecer aos consumidores a oportunidade de exigir que tal entidade exclua os dados cobertos de um consumidor.

Resta apresentar as regras propostas para a supervisão de Inteligência Artificial (IA) e o uso de algoritmos[13]. A seção 207 (Direitos Civis e Algoritmos) assevera que entidades ou provedores de serviços cobertos "não podem coletar, processar ou

---

[12] Comissão Federal de Comércio

[13] O projeto de lei define um algoritmo como: um processo computacional que usa aprendizado de máquina, processamento de linguagem natural, técnicas de inteligência artificial ou outras técnicas de processamento computacional de complexidade semelhante ou maior que toma uma decisão ou facilita a tomada de decisão humana com relação aos dados, inclusive para determinar o fornecimento de produtos ou serviços ou para classificar, ordenar, promover, recomendar, ampliar ou determinar de forma semelhante a entrega ou “exibição de informações a um indivíduo”.

transferir dados cobertos de maneira que discrimine ou torne indisponível o aproveitamento igual de bens ou serviços com base em raça, cor, nacionalidade, sexo ou deficiência". Ao contrário da maioria das leis estaduais de privacidade existentes, a Seção 207 da ADPPA iria um passo além, exigindo que as empresas avaliassem certas ferramentas de IA e submetessem essas avaliações à FTC.

Por enquanto, espera-se e observam-se vários movimentos relutantes e de oposição à promulgação da ADPPA, inclusive de apoiadores de mudanças no sentido de viabilizar e flexibilizar a cada Estado o uso ou não das regras legais expostas. A própria California afirma que a CCPA dá mais proteção aos consumidores e mais controle de suas informações do que o texto do projeto de lei da ADPPA.

2.4.2 Japão

Atualmente, o Japão é a terceira maior economia mundial (considerando o PIB nominal) e o décimo primeiro país com maior população no mundo, sendo uma das mais antigas democracias da Ásia (com parlamento bicameral e uma monarquia constitucional com um imperador). Além disso – e um dos fatores que mais sustenta a relevância deste país quando o assunto é acesso à informação e direito à privacidade e proteção jurídica de dados pessoais – o Japão é o país líder em inovações tecnológicas. Ainda, importa ressaltar que, mesmo após sofrer influência do sistema jurídico do ocidente (por volta de 1858), as regras jurídicas japonesas são conhecidas como pouco flexíveis – o que reflete a cultura moral rígida e o código de honra que molda e fundamenta as relações nipônicas (o *giri*).

A Lei de Proteção de Informações Pessoais do Japão (LPIP-JP) foi promulgada em 2003 e sofreu reforma em 2013 e ampla mudança em 2017 (GREENLEAF, 2014), que, inclusive, estabeleceu revisão trianual obrigatória (a mais recente foi em 2020). Até 2011, segundo Miyashita (2011, p. 233 [tradução nossa]):

> As regras legais para os mecanismos de aplicação são muito particulares no Japão e diferem da forte aplicação da lei nos países europeus. No entanto, é extremamente importante entender que uma violação de dados no Japão significa a ruptura da confiança social e do relacionamento íntimo com os clientes. No Japão, o risco de perda de confiança social e reputação empresarial é considerado muito mais significativo do que pagar uma multa. Assim, as empresas geralmente seguem as diretrizes emanadas dos

> ministérios governamentais, e algumas também adotam suas próprias diretrizes [...].[14]

De acordo com Greenleaf (2014), as reformas ocorreram, principalmente, para sanar as fragilidades da lei japonesa e cumprir as expectativas internacionais sobre a privacidade dos dados pessoais no ciberespaço. A Comissão Europeia lançou comunicado, em janeiro de 2017, que confirmou a modernização da legislação do Japão, tornando o regime abrangentes em matéria de proteção de dados (COMISSÃO EUROPEIA, 2017). Em Decisão de Execução (UE) 2019/419, de 23 de janeiro de 2019, a LPIP-JP foi considerada compatível com a RGPD (COMISSÃO EUROPEIA, 2019).

A LPIP-JP é aplicada a todos os Controladores de Dados Pessoais (CDP), sejam pessoas físicas ou jurídicas, e modificada pela Comissão de Proteção de Informações Pessoais do Japão (CPIP-JP).

Destacam-se algumas definições, pois são relevantes para fim de comparação com a RGPD e LGPD. Segundo Hounslow (2021), na LPIP-JP, em suas diretrizes gerais, há a definição de:

- Informações pessoais: Informações sobre pessoa que resida no Japão. Nessa categoria, incluem-se 'códigos de identificação pessoal', tais como: itens como caracteres, números, símbolos e/ou outros códigos para uso do computador que representam certas características físicas pessoais especificadas (como sequências de DNA, aparência facial, impressões digitais e palmares), e que são suficientes para identificar um indivíduo específico, bem como determinados números de identificação, como os de passaportes, carteiras de habilitação e cartões de residente e os números de identificação individual da previdência social.
- Dados pessoais: Informações pessoais contidas em um banco de dados.
- Dados sensíveis: informações pessoais relacionadas a questões como: raça, credo, religião, deficiência física ou mental, registros médicos, tratamento

[14] The legal rules for enforcement mechanisms are very particular in Japan, and differ from the strong enforcement of the law in European countries.33 However, it is crucially important to understand that a data breach in Japan means the disruption of social trust and the intimate relationship with customers. In Japan, the risk of loss of social trust and business reputation is regarded as much more significant than paying a fine. Thus, businesses generally follow the guidelines issued by government ministries, and some also adopt their own guidelines […].

médico e farmacológico, prisão, detenção ou processo criminal (seja adulto ou jovem), ou vitimização criminal.

- Titular dos dados: o indivíduo que é o titular das informações pessoais.

Outros aspectos de divergência e convergência entre a LGPD e a LPIP-JP são apresentados no quadro 3.

Quadro 3 – Aspectos de convergência e divergência entre LGPD e LPIP-JP

Instituição Jurídica	LGPD (Brasil)	LPIP (Japão)
Autoridade de Proteção de Dados	Não Autônoma/ Não Independente Art. 5º (XIX): "autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional"	Autônoma/ Independente Art. 59 (n. 2) e art. 62: "(2) A Comissão pertence à jurisdição do Primeiro-Ministro"; "O presidente e os comissários da Comissão devem exercer a sua autoridade oficial de forma independente".
Titulares de Dados	Art. 5º (V): "titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento"	Art. 2º (n. 8): "Um 'titular' de informações pessoais, nesta Lei, significa um indivíduo específico identificável por informações pessoais"
Direito de ser informado	Art. 6º (VI): "transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial"	Art. 27 (n. 1; i a iv): "(1) Um PIHBO[15], em relação às informações pessoais retidas por si, disponibilizará os tópicos descritos a seguir de forma que o titular possa conhecê-los (incluindo aqueles casos em que, a pedido de um titular, responderá sem demora).
Direito de acesso	Artigo 6º (IV): "livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais"	Artigo 28 (nº1): "(1) Um titular pode exigir de um PIHBO a divulgação de dados pessoais retidos que possam identificar ele ou ela por um método de fornecimento de registro eletromagnético ou outros métodos prescritos pelas regras da Comissão de Proteção de Informações Pessoais."
Direito à limitação do tratamento	Artigo 18 (IV): "anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei"	Artigo 16 (n.1), Artigo 29 (n.1) e Artigo 30 (n.1 e n.5): "(1) Um PIHBO não deve tratar informações pessoais, sem obter previamente o consentimento do titular, para além do âmbito necessário para cumprir uma finalidade de utilização especificada de acordo com o disposto no artigo anterior."; "(1) Um titular pode, quando o conteúdo de dados pessoais retidos que podem identificá-lo não estiver exato, exigir que um PIHBO faça uma correção, adição ou exclusão (de agora

[15] *Personal Information Handling Business Operator* – figura semelhante ao controlador de dados.

		em diante denominada "correção etc." no presente artigo) em relação ao conteúdo dos dados pessoais retidos."; "(1) Um titular pode, quando dados pessoais retidos que possam identificá-lo estão sendo tratados em violação às disposições do Artigo 16 ou Artigo 16-2, ou, foram adquiridos em violação às disposições do Artigo 17, exigir de um PIHBO a cessação da utilização ou eliminação (doravante referida como "cessação da utilização etc." neste Artigo) dos dados pessoais retidos."; "(5) Um titular pode exigir que o PIHBO cumpra uma cessação de utilização etc. dos dados pessoais retidos, ou cesse uma provisão a terceiros, se tiver se tornado desnecessário para o PIHBO utilizar dados pessoais retidos que possam identificar o titular, se uma situação prescrita na cláusula principal do Artigo 22-2, parágrafo (1) ocorreu em conexão com os dados pessoais retidos que possam identificar o titular, ou existe a possibilidade de que o tratamento dos dados pessoais retidos que possam identificar o titular prejudiquem os direitos ou interesses legítimos desse."

Fonte: Adaptado de Marques (2021).

A evolução da proteção jurídica das informações pessoais no Japão fez com que o país esteja considerado como zona em *compliance* (confiança) no tratamento de dados pela UE. Como se pode observar na figura 1, o Japão é reconhecido pela UE como um dos únicos países asiáticos considerados adequado para ser zona de trânsito seguro de dados. Tanto o Japão quanto a Coreia do Sul são reconhecidos pela UE em relação à confiança de procedimentos em tratamentos de dados, porém o Japão é considerado como zona de tratamento de alto nível no que se refere a dados, o que cria um sistema de livre trânsito de dados, em que as barreiras burocráticas não são necessárias.

Assim, após avaliação de adequação, a UE, em 2019, afirmou que a relação em Japão e UE é a maior área de fluxo de dados seguros do mundo e colocou em vigor o Acordo de Parceria Econômica UE-Japão, contando com fluxo livre de dados entre empresas de ambos os países.

3 A LGPD NO BRASIL E SUA OPERACIONALIZAÇÃO NAS ATIVIDADES NOTARIAIS E REGISTRAIS: CASO DE CARTÓRIOS DE PROTESTO

3.1 A LGPD: detalhes relevantes

Para resumir os principais pontos de que trata a LGPD, organizou-se um quadro referencial que, sinteticamente, permite visualizar algumas das fronteiras desta legislação (quadro 4).

Quadro 4 – Quadro referencial da LGPD

CAPÍTULO	SEÇÕES	Arts.
Capítulo I – DISPOSITIVOS PRELIMINARES	-	Art. 1º ao 6º
Capítulo II – DO TRATAMENTO DE DADOS PESSOAIS	Seção I – Dos Requisitos para o Tratamento de Dados Pessoais	Art. 7º ao 16
	Seção II – Do Tratamento de Dados Pessoais Sensíveis	
	Seção III – Do Tratamento de Dados Pessoais de Crianças e de Adolescentes	
	Seção IV – Do Término do Tratamento de Dados	
Capítulo III – DOS DIREITOS DO TITULAR	-	Art. 17 ao 22
Capítulo IV – DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO	Seção I – Das Regras	Art. 23 ao 32
	Seção II – Da Responsabilidade	
Capítulo V – DA TRANSFERÊNCIAS INTERNACIONAL DE DADOS	-	Art. 32 ao 36
Capítulo VI – DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS	Seção I – Do Controlador e do Operador	Art. 37 ao 45
	Seção II – Do Encarregado pelo Tratamento de Dados Pessoais	
	Seção III – Da Responsabilidade e do Ressarcimento de Danos	
Capítulo VII – DA SEGURANÇA E DAS BOAS PRÁTICAS	Seção I – Da Segurança e do Sigilo de Dados	Art. 46 ao 51
	Seção II – Das Boas Práticas e da Governança	
Capítulo VIII – DA FISCALIZAÇÃO	Seção I – Das Sanções Administrativas	Art. 52 ao 54
Capítulo IX – DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE	Seção I – Da Autoridade Nacional de Proteção de Dados (ANPD)	Art. 55 ao 59
	Seção II – Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade	
Capítulo X – DISPOSIÇÕES FINAIS E TRANSITÓRIAS	-	Art. 60 ao 65

Fonte: O autor (2023).

Como se observa, a LGPD está dividida em 10 capítulos, com 65 artigos. Ressalta-se que a privacidade e a própria proteção de dados são elementos já protegidos juridicamente em nosso ordenamento, como já exposto, e, da mesma forma, o formato atual da LGPD pode (e irá) sofrer alterações considerando diversos cenários tecnológicos possíveis.

Para Pinheiro (2020), a LGPD, como versão mais enxuta da RGPD, deixa alguns aspectos abertos à interpretação, sendo, portanto, menos assertiva. Porém, segundo o autor, a criação da ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, mesmo após veto presidencial[16], preencheu uma lacuna estruturante e permitiu maior segurança na implementação da nova regulamentação. É relevante, para a discussão proposta, que se relate, mesmo que brevemente, o caminho das revisões feitas na criação da ANPD por meio dos vetos – mantidos e rejeitados – e a mudança de sua natureza jurídica.

O texto original da criação da ANPD – Lei n. 13.853/2019 – sofreu vetos do então presidente da República, Jair Bolsonaro. Todos os itens vetados haviam sido incluídos pelos parlamentares. Os nove vetos do presidente foram: (1) foi vetado o dispositivo que permitia à autoridade cobrar taxas por serviços prestados (a autoridade deverá arcar com recursos próprios consignados no Orçamento Geral da União); (2) vetados os dispositivos que ampliavam o rol de sanções administrativas aplicadas pela ANPD (prever sanções de suspensão ou proibição podem gerar insegurança aos responsáveis por essas informações e impossibilitar o uso e o tratamento de bancos de dados essenciais a diversas atividades privadas); (3) vetado o dispositivo que proibia o poder público de compartilhar, com outros órgãos públicos ou com pessoas jurídicas de direito privado, os dados pessoais de requerentes que utilizaram a LAI (a proibição poderia gerar insegurança jurídica já que o compartilhamento de informações relacionadas à pessoa natural identificada ou identificável, que não deve ser confundido com a quebra do sigilo ou com o acesso público, é medida recorrente e essencial para o regular exercício de diversas atividades e políticas públicas); (4) vetos de regras para a revisão de decisões automatizadas (dispor que toda e qualquer decisão baseada unicamente no

[16] A criação da autoridade nacional estava prevista na LGPD, sancionada em agosto de 2018, pelo presidente Michel Temer. No entanto, o dispositivo da lei que criava a ANPD foi vetado por Temer que, posteriormente, em dezembro de 2018, recriou a autoridade, por meio de medida provisória. A MP foi aprovada em maio de 2019 pela Câmara e pelo Senado (SERPRO, 2019).

tratamento automatizado seja suscetível de revisão humana contrariaria o interesse público[17], impactaria na análise de risco de crédito e de novos modelos de negócios de instituições financeiras[18]; (5) vetados artigos que traziam requisitos para o cargo de encarregado[19] (exigência com rigor excessivo e interferência do Estado) (SERPRO, 2019).

Após apreciação pelo Congresso, três vetos foram mantidos e cinco foram rejeitados. No que tange à ANPD, os vetos presidenciais para retirar os dispositivos que ampliavam o rol de sanções administrativas aplicadas pela ANPD foram rejeitados. Já o veto ao dispositivo que permitia à autoridade cobrar taxas por serviços prestados foi mantido pelos senadores e deputados. Outro veto mantido foi o sobre o dispositivo que proibia o poder público de compartilhar, com outros órgãos públicos ou com pessoas jurídicas de direito privado, os dados pessoais de requerentes que utilizaram a Lei de Acesso à Informação (LAI). Além disso, foram mantidos os vetos aos artigos que traziam requisitos para o cargo de encarregado (SERPRO, 2019).

Corrigido em tempo, a criação da autoridade nacional de fiscalização independente permitiu que o Brasil recebesse reconhecimento da UE. A ANPD é imbuída de uma estrutura fiscalizatória de natureza específica. Segundo definição legal, a autoridade nacional é um órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional. Sua estrutura regimental a conceituou como órgão integrante da Presidência da República, "[...] dotado de autonomia técnica e decisória, [...] com sede e foro no Distrito Federal, criado com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural" (LIMA et al., 2021, p. 613). A estrutura da ANPD pode ser mais bem verificada na figura 2.

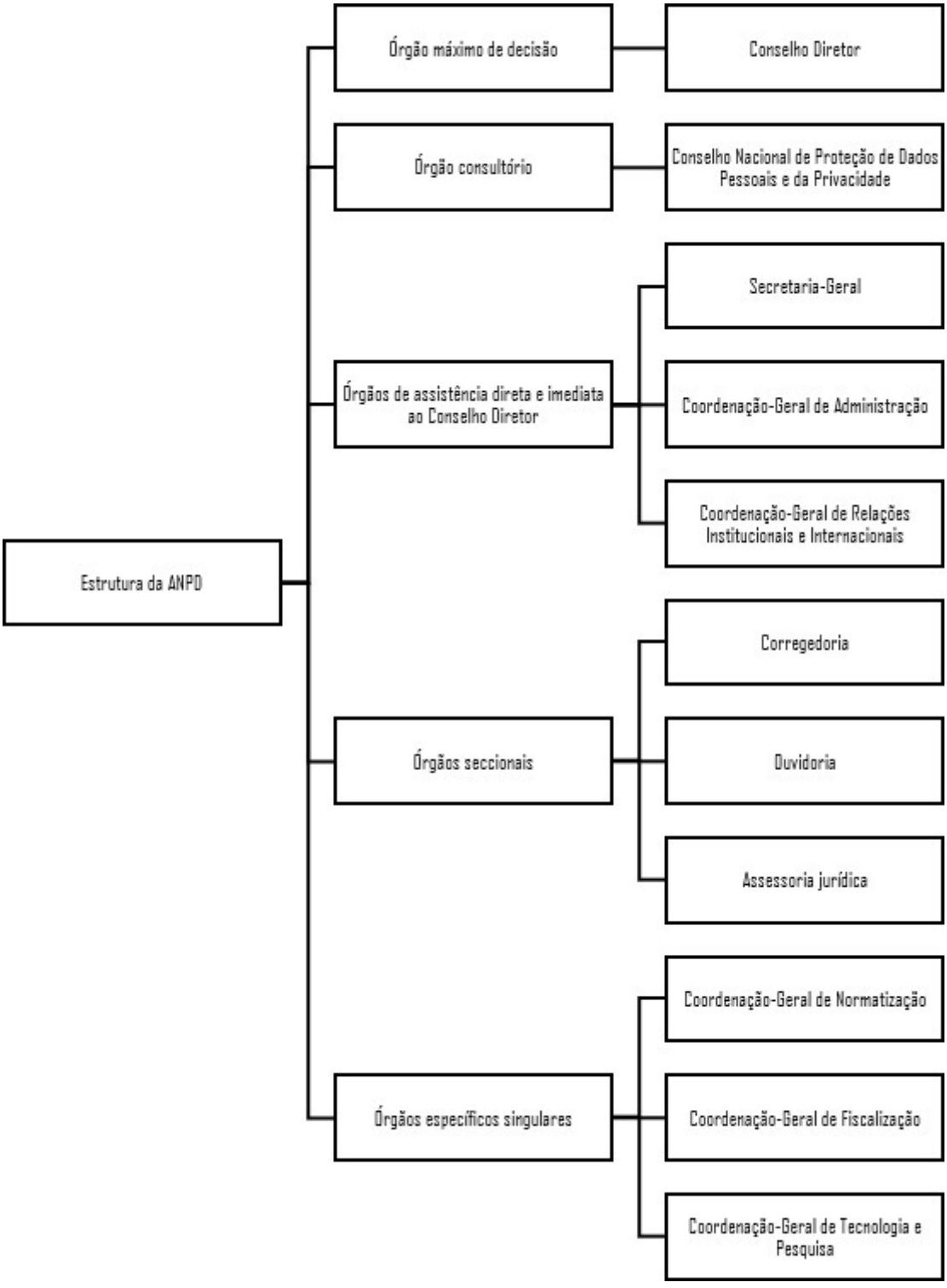
---

[17] Tendo em vista que tal exigência inviabilizaria os modelos atuais de planos de negócios de muitas empresas, notadamente das startups. (SERPRO, 2019)

[18] Poderia, segundo Jair Bolsonaro, gerar efeito negativo na oferta de crédito aos consumidores, tanto no que diz respeito à qualidade das garantias, ao volume de crédito contratado e à composição de preços, com reflexos, ainda, nos índices de inflação e na condução da política monetária. (SERPRO, 2019)

[19] A pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. (SERPRO, 2019)

Figura 2 – Esquematização da estrutura da ANPD



Fonte: Lima et al. (2020, p. 617).

Sobre a mudança de sua natureza jurídica, interessa, da mesma forma, entender que a ANPD, atualmente, é uma autarquia de natureza especial, ou seja,

não é subordinada hierarquicamente a ministérios ou à Presidência, possuindo autonomia técnica e decisória. A natureza jurídica da ANPD foi modificada pela MP 1.124/2022, convertida em Lei n. 14.460/2022. A MP, que alterou a Lei n. 13.709, de 14 de agosto de 2018, transformou a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e transformou cargos em comissão.

> O objetivo da mudança, segundo a explicação do Poder Executivo, é evitar a descontinuidade administrativa da ANPD e trazer mais confiabilidade ao sistema regulatório de proteção de dados. No novo formato, ele será compatível com outros regimes regulatórios e experiências internacionais, alega o Executivo.
> A lei cria ainda, sem aumento de despesa, um cargo comissionado para o diretor-presidente da ANPD e aloca os atuais servidores na nova autarquia. A iniciativa também prevê outras mudanças estruturais para viabilizar o funcionamento da nova entidade administrativa como: regras para requisição de pessoal, transferência de patrimônio e de pessoal de outros órgãos ou entidades da administração pública (CÂMARA DO DEPUTADOS, 2022, s/p).

O funcionamento da ANPD como órgão ocorreu de forma transitória – estipulados dois anos para a definição da natureza jurídica da entidade, conforme artigo já revogado 55-A da LGPD. Assim, anterior à mudança para autarquia, a ANPD era órgão da administração pública federal, integrante da Presidência da República. Cabe salientar que a mudança de órgão para autarquia já estava prevista na Lei n. 13.853/2019 e que regulamentação da transição de órgão vinculado à Presidência para autarquia independente será feita em ato conjunto entre secretário-geral da presidência e diretor-presidente da ANPD (CÂMARA DOS DEPUTADOS, 2022).

Destaca-se que, em Agenda Regulatória para o biênio 2023-2024 (Portaria ANPD n. 35, de 4 de novembro de 2022), a ANPD, para fins de planejamento das ações, estabelece quatro fases. Assim: (1) na primeira fase há a previsão de cumprir os processos regulatórios iniciados no biênio 2021-2022; (2) na segunda fase estão estabelecidos os processos regulatórios que deverão ocorrer em até 1 ano; (3) na terceira fase os que devem acontecer em 1 ano e 6 meses; e, (4) na quarta fase, os que devem acontecer em 2 anos (DIÁRIO OFICIAL, 2022). A Portaria ANPD n. 35 está anexada ao final do texto da dissertação (Anexo 1).

Estão, a seguir, apresentados conceitos específicos e os critérios para o tratamento de dados pessoais contidos na LGPD.

3.1.1 Conceitos específicos

O art. 5º da LGPD define, para fins de conceituação, o apresentado no quadro 5.

Quadro 5 – Conceitos específicos da LGPD

TÍTULO	CONCEITO
Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável
Dado pessoal sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural
Dado anonimizado	Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento
Banco de dados	Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico
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 ou privado, que realiza o tratamento de dados pessoais em nome do controlador
Encarregado	Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a autoridade nacional de proteção de dados (ANPD)
Agentes de tratamento	O controlador e o operador
Tratamento	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
Anonimização	Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo
Consentimento	Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada
Bloqueio	Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados
Eliminação	Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado
Transferência internacional de dados	Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro
Uso compartilhado de dados	Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados

Relatório de impacto à proteção de dados pessoais	Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco
Órgão de pesquisa	Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no país, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico
Autoridade nacional	Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei em todo o território nacional

Fonte: Baseado na LGPD (BRASIL, 2018).

Reforça-se, no contexto da operacionalização da LGPD, a diferença entre dado e informação. Para Cintra (2021):

> Dado e informação são conceitos tecnicamente diferentes, embora muitas vezes utilizados como sinônimos em determinados contextos. Contudo, em especial no contexto da Lei 13.709/18 - Lei Geral de Proteção de Dados Pessoais (LGPD), diferenciar esses conceitos permite aos profissionais do Direito uma compreensão mais profunda da Lei, permite análises menos abstratas de situações fáticas e, portanto, essencial para aplicação eficiente dos institutos do dispositivo legal.

Dado, no entendimento de Cintra (2021), não tem significado algum fora de um contexto, sendo algo identificável por um receptor, mas que sem a devida análise/tratamento não significa algo e não pode, desta forma, ser utilizado para um fim específico. Já a informação é o produto da interpretação/tratamento de um dado bruto.

Outro aspecto importante da lei são os dez princípios que devem ser observados em qualquer atividade que trate dados pessoais, salvaguardando a boa-fé. O art. 6º estabelece que:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

> IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII – segurança: utilização de medidas 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 difusão;
> VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de com provar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

A leitura atenta do dispositivo legal permite inferir exatamente o sentido dado a cada princípio, eis que explicados literal e diretamente no próprio texto normativo, em forma de conceitos dados a serem seguidos. Soler (2021) apresenta, para cada um destes princípios, exemplos específicos e práticos e perguntas a serem feitas para que se apliquem de forma didática.

O primeiro princípio, o da finalidade, estabelece que é preciso ser específico, legítimo, explícito e informar sobre o motivo de tratar dados. Podem-se fazer as seguintes perguntas: Por que os dados estão sendo tratados? Qual a motivação? Um exemplo de sua aplicação está no caso: somente para a conclusão e devido pagamento da compra, a empresa x trata os dados financeiros de quem utiliza a sua plataforma e repassa as instituições financeiras, unicamente (SOLER, 2021, p. 43).

O segundo princípio, o da adequação, afirma que os dados devem ser tratados conforme sua finalidade específica. Pergunta que seve ser feita: os dados que estão sendo tratados estão alinhados com a finalidade? Um exemplo prático seria: caso não se venda roupa, não é preciso saber o tamanho de seu manequim. Quanto ao terceiro princípio, o da necessidade, estabelece que devem ser tratados o mínimo de dados necessários, na proporção da finalidade (realmente é preciso todos os dados que estão sendo tratados? Quais são os mínimos dados que são preciso para realizar esse tratamento?). Como exemplo prático, o autor apresenta: quando há venda de alimentos, não é preciso saber o gênero e a orientação sexual da pessoa. Eventualmente, é preciso saber a idade para não vender bebidas alcoólicas a

menores de 18 anos (no Brasil) ou, eventualmente, o mínimo sobre a saúde, no caso, somente a existência de alergia, para não incluir leite em um prato a um alérgico a lactose (SOLER, 2021, p. 43-44).

O quarto princípio estabelece o livre acesso, gratuito e fácil sobre como os dados pessoais são tratados (será que qualquer pessoa, mesmo não sendo da área jurídica ou de tecnologia, sem a devida acessibilidade ao computador, conseguiria localizar as informações sobre os dados pessoais dela na página da internet da empresa?). O quinto princípio estabelece a qualidade dos dados, ou seja, os dados devem ser mantidos atualizados, claros, relevantes e exatos, coadunando com a finalidade do tratamento (quão claro, exato, relevante e atualizados são os dados que são informados ao titular? Como o titular exercerá sua "autodeterminação informativa" se não for empregada qualidade dos dados?) (SOLER, 2021, p. 44-46).

Como sexto princípio a LGPD estabelece a transparência – as informações precisam ser claras, precisas e facilmente acessíveis a respeito do tratamento de dados e os seus agentes. Pergunta-se: uma senhora de 75 anos ("homem médio") entenderia essas informações? O sétimo princípio estabelece a segurança, ou seja, a obrigatoriedade da utilização de medidas técnicas e administrativas para a proteção de ilícitos, acesso não autorizado ou mesmo de acidentes com os dados pessoais (estão sendo implementadas internamente medidas técnicas e administrativas proteger os dados pessoais?) (SOLER, 2021, p. 47-48).

O oitavo princípio estabelece a preservação (quais medidas estão sendo tomadas para evitar que aconteça um acidente/um vazamento de dados?). A não discriminação está apresentada pelo nono princípio (é possível discriminar alguém com o tratamento de dados que está sendo realizado?). O décimo princípio rege a responsabilização e prestação de contas, ou seja, a adequação à LGPD (é possível demonstrar a eficácia do programa de adequação à LGPD usado?) (SOLER, 2021, p. 48-51).

Aos agentes de tratamento, para Soler (2021, p. 51)

> [...] a LGPD criou diversas metas que precisam ser alcançadas [...]. Para além do exercício dos direitos dos titulares, há também o dever de responsabilização e de controle dos riscos para a atividade de proteção de dados pessoais, entre outros. De tal sorte que, por um lado, os agentes de tratamento são dotados de discricionariedade sobre a realização de suas atividades e de seu programa de adequação, mas devem, por outro lado,

> prestar contas acerca de tais tratamentos e demonstrar o seu estrito cumprimento.

Sendo assim, no tratamento de dados pessoais, em resumo, deve-se observar a boa-fé, associada à finalidade do tratamento e a sua compatibilidade com as finalidades informadas, com a limitação do tratamento dos dados ao mínimo necessário para a consecução de suas finalidades, garantindo-se aos titulares dos dados a transparência e o acesso aos dados por meio de consulta facilitada e gratuita sobre a forma de tratamento, assegurando-se a correção de dados, se for o caso, com a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais e mediante prestação de contas, pelo agente, da adoção de medidas capazes de comprovar a proteção dos dados.

3.1.2 Critérios para o tratamento de dados

A LGPD, em seu artigo 7º, define dez bases legais ou hipóteses autorizativas para o tratamento de dados pessoais. A primeira situação autorizadas pela LGPD para tratamento de dados pessoais é mediante o fornecimento de consentimento pelo titular. Exemplificando tal situação: o titular que, antes de efetuar o seu cadastramento em uma plataforma de e-commerce, é direcionado para a leitura do termo de consentimento, no qual ele é informado o que será feito com seus dados pessoais, podendo aceitar ou não. Isso não deve ser confundido com um Aviso ou Política de Privacidade, que também deve ser disponibilizado ao titular, contendo todas as informações sobre os tratamentos, servindo, neste caso, como um instrumento de transparência.

A segunda situação autorizadas pela LGPD para tratamento de dados pessoais é para o cumprimento de obrigação legal ou regulatória pelo controlador. Assim, é autorizado tratamento para cumprir obrigações relacionadas ao tratamento de dados pessoais de funcionários, com a finalidade específica de efetivar a realização do pagamento de salários e benefícios. Situação em que lidar com os dados pessoais dos funcionários seja, portanto, necessário para o cumprimento de leis trabalhistas.

Outra situação autorizada, pela administração pública, é para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos

congêneres, observadas as disposições do Capítulo IV da Lei. Ou seja, em política de controle de tabagismo, por exemplo; em situação em que a Secretaria de Saúde efetua o tratamento de dados pessoais de pessoas que fazem uso de cigarros com a finalidade de execução de políticas públicas de controle do tabagismo e conscientização social.

Ainda, é autorizado o tratamento para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais. Por exemplo, para pesquisas e desenvolvimento científico, social e econômico como função administrativa do Estado, como as funções do Ministério da Ciência, Tecnologia, Inovações e Comunicações. Também, é autorizado que se tratem os dados quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados, na formalização de um contrato entre duas partes com termos que permitem o uso de dados pessoais, por exemplo. Dessa forma, o tratamento de dados pode ser feito normalmente, pois, ao assinar o contrato, o titular dá permissão para que a empresa utilize essas informações.

Outra hipótese rege que é autorizado o tratamento de dados para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem). Assim, é autorizado quando uma parte desejar ingressar em face da outra. Nesse sentido, não precisará de consentimento para que possa utilizar os dados, podendo se valer desta base para validar esse tratamento.

Em casos de emergência ou situações graves, para a proteção da vida ou da incolumidade física do titular ou de terceiro, da mesma forma é autorizado tratamento de dados pessoais. Bem como, para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (quando nome, endereço e telefone são obtidos e, constando no termo para qual finalidade se presta, principalmente quando existe o compartilhamento de informações comerciais com outras redes e parceiros de clínicas, hospitais, ou instituições do mesmo grupo, planos de saúde, seguradoras, entre outros).

Há a autorizado quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais – por exemplo:

situação em que uma entidade pública efetua o tratamento de dados pessoais dos seus servidores com a finalidade específica de garantir a segurança dos sistemas utilizados para promover a autenticação dos usuários e garantir que não haja a inserção de vulnerabilidades na rede interna por parte de softwares maliciosos.

Finalmente, há a autorizado de tratamento de dados pessoais para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. Um exemplo da utilização desta hipótese seria uma situação em que o titular tem suas informações tratadas por instituição financeira que precisa avaliar a possibilidade de concessão ou não de crédito (Adaptado de Serpro, 2023).

Já, o art. 11 define as hipóteses autorizativas para o tratamento de dados pessoais sensíveis, conforme quadro 6. Novamente, apresenta-se a regra e sua aplicação prática, por meio de exemplo aplicados.

Quadro 6 – Situações autorizadas pela LGPD para tratamento de dados pessoais sensíveis

O QUE DIZ A LGPD	EXEMPLO
I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;	Exemplo: o titular disponibiliza suas informações sobre sua origem racial ou étnica em inscrições nos exames como ENEM, PAS ou concursos públicos para obtenção do direito a cotas raciais.
II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:	
a) cumprimento de obrigação legal ou regulatória pelo controlador;	Exemplo: um Município decreta a obrigatoriedade do comprovante de vacinação do titular em estabelecimentos públicos e privados.
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;	Exemplo: quando adotadas medidas urgentes em função da emergência de saúde pública decorrente do coronavírus.
c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;	Exemplo: a utilização do resultado do exame de uma pessoa que é diagnosticada com HIV – positivo para fins de estudos científicos e conscientização social.
d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;	Exemplo: a utilização da prova de DNA, com dados genéticos, em uma demanda investigatória de paternidade.
e) proteção da vida ou da incolumidade física do titular ou de terceiro;	Exemplo: quando o uso de dados sobre a saúde do titular é essencial em um setor ou serviço de emergência que presta cuidados primários.
f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência	Exemplo: o compartilhamento de informações sobre prontuários médicos entre serviços de saúde.

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.	Exemplo: a realização de cadastramento de dados biométricos para identificação do titular nas urnas eletrônicas em eleições.

Fonte: Adaptado de Serpro (2023).

Doneda (2011), ao escrever sobre a proteção dos dados pessoais como um direito fundamental, afirma que o tratamento de dados pessoais, em particular por processos automatizados, é uma atividade de risco, pois possibilita o controle das atividades de um indivíduo em múltiplas situações cotidianas.

3.2 LGPD *versus* Poder Público

Em janeiro de 2022, a ANPD lançou um guia orientativo sobre o tratamento de dados pessoais especialmente para ações do Poder Público. Já na apresentação, o guia afirma que:

> O tratamento de dados pessoais pelo Poder Público possui muitas peculiaridades, que decorrem, em geral, da necessidade de compatibilização entre o exercício de prerrogativas estatais típicas e os princípios, regras e direitos estabelecidos na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018 – LGPD) (GUIA, 2022, p. 4).

Um dos desafios enfrentados pela ANPD é ser objetiva nos parâmetros impostos aos órgãos públicos e entidades jurídicas para a operacionalização de dados pessoais, pois deve estar garantida a celeridade e a eficiência à execução e prestação de serviços públicos sem, no entanto, desrespeitar os direitos à proteção de dados pessoais e à privacidade.

O guia inicia com uma breve explanação sobre a LGPD, o conceito de Poder Público e as competências da ANPD. A seguir, são apresentadas orientações sobre as bases legais mais comuns e os mais relevantes princípios que devem nortear o tratamento de dados pessoais por entidades e órgãos públicos. Na parte final, são abordadas duas operações específicas de tratamento de dados pessoais pelo Poder Público. É interessante apresentar a visão de Pinheiro (2020, p. 14), quanto à implementação da LGPD e sobre a ANPD:

> Ainda que seja por uma boa causa, a implementação da conformidade à LGPD trará um impacto grande nas instituições, podendo contribuir para o aumento do “custo Brasil”, especialmente nos setores de Startups, pequenas empresas e no setor público, com especial atenção aos que tratam muitos dados pessoais sensíveis, como os de saúde.
> Mas é importante ter em mente que não basta ter a lei de proteção de dados pessoais, é preciso educar, capacitar. Por isso a importância do papel orientantivo da Autoridade (ANPD) e a relevância de sua atuação proativa junto à sociedade e às instituições, para encontrar medidas viáveis de implementação da nova regulamentação, que gerem menor impacto possível nos setores produtivos e que sejam adaptados e aderentes aos usos e costumes.

Para fins pertinentes a esta dissertação, esclarece-se que a LGPD estabelece regras a serem seguidas por todos os agentes de tratamento de dados pessoais, o que inclui o Poder Público. Ainda, o termo “Poder Público” é definido de forma ampla e inclui órgãos ou entidades dos entes federativos (União, Estados, Distrito Federal e Municípios) e os três Poderes (Executivo, Legislativo e Judiciário), inclusive das Cortes de Contas e do Ministério Público.

Estão incluídos no conceito de Poder Público, portanto,

> (i) os serviços notariais e de registro (art. 23, § 4º); e (ii) as empresas públicas e as sociedades de economia mista (art. 24), neste último caso, desde que (ii.i.) não estejam atuando em regime de concorrência; ou (ii.ii) operacionalizem políticas públicas, no âmbito da execução destas (GUIA, 2022, p. 5).

O quadro 7 apresenta as normas que se aplicam especificamente em relação ao Poder Público e, após, é realizada análise de cada um dos artigos, individualmente, que rege a operacionalização da LGPD em entes do Poder Público.

Quadro 7 – A LGPD e o Poder Público

Artigo	O QUE DIZ A LGPD
Art. 4º	Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: [...] IV - provenientes de fora do território nacional e que não sejam 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 nesta Lei. [...] § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.

CAPÍTULO IV DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO Seção I Das Regras	Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; II - (VETADO); e III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e IV - (VETADO). § 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento. § 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) . § 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) . § 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei. § 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo. Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei. Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo. Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral. Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

	§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto: I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) ; II - (VETADO); III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei. IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. § 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional. Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto: I - nas hipóteses de dispensa de consentimento previstas nesta Lei; II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou III - nas exceções constantes do § 1º do art. 26 desta Lei. Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação. Art. 28. (VETADO). Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.
Seção II Da Responsabilidade	Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação. Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.
Art. 55-J, XI e XVI	Art. 55-J. Compete à ANPD: […] XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; [...] XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o

	tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

Fonte: Baseado na LGPD (BRASIL, 2018).

Como se observa no quadro 7, a LGPD guarda capítulo próprio para dispor sobre o tratamento de dados pessoais pelo Poder Público. De acordo com Tasso (2019), o capítulo IV da LGPD elenca as hipóteses legais em que o Estado é investido do poder de tratar dados pessoais, excluindo, por via de consequência, qualquer outra, atrelando-as ao propósito de cumprir sua finalidade pública e desde que tenham como premissa o interesse público. Sendo assim, a "[...] atuação do Poder Público é, portanto, excepcional e condicionada" (TASSO, 2019, p. 277).

O art. 23 serve como complemento das hipóteses autorizadoras complementares, apresentando especificamente o tratamento de dados com finalidade pública, além de estabelecer as adequações necessárias para harmonizar a LGPD e a LAI (já que ambas tratam de pessoas jurídicas de direito público ou privado). As pessoas jurídicas devem possibilitar o acesso à informação do titular de dados, fornecendo informações necessárias para a persecução do interesse público.

Há quatro requisitos para o tratamento de dados pessoais pelas pessoas jurídicas de direito público: (1) atendimento ao interesse público; (2) execução das competências legais ou cumprimento das atribuições legais do serviço público; (3) publicidade das hipóteses em que o ente ou órgão público realiza o tratamento de dados pessoais (claro, atualizado, fácil acesso em sítios eletrônicos); (4) indicação de um encarregado pela realização das operações de tratamento de dados pessoais.

É importante lembrar que a redação deste artigo foi modificada pela Lei n. 13.853/19, mantendo o escopo do inciso III, mas vetando o inciso IV, que visava acrescentar mais uma especificação para o tratamento de dados realizado pelos entes públicos, com o objetivo de proteger e preservar os dados pessoais dos requerentes da Lei de Acesso à Informação, vedando o compartilhamento na esfera do poder público e com pessoas jurídicas de direito privado:

> [...] do art. 23 demandando análise à luz da LAI quanto às suas previsões. Ademais, ainda restam algumas dúvidas sobre esse tema, em que se espera a atuação da ANPD, como a definição de dados públicos, a ratificação de certos atos do governo e os limites da sua função fiscalizadora, que hoje podem aparentar estar alinhados com a LGPD, porém, também podem vir a ser objeto de questionamento dos titulares de dados.

> A título de exemplo, podemos citar o uso dos dados que estão em redes sociais, visto que por descuido dos usuários, existem dados que são tornados públicos e nem sempre seu titular teria esse interesse neste sentido. Neste sentido, atualmente a Receita Federal do Brasil utiliza as informações publicadas nas redes sociais para o cumprimento da sua finalidade fiscalizatória e arrecadatória (SOLER, 2021, p. 109).

O art. 24 equipara as empresas públicas e as sociedades de economia mista às pessoas jurídicas e de direito privado particulares, dando-lhes o mesmo tratamento quanto à obrigação de atender às regras do tratamento de dados pessoais. Em parágrafo único, o artigo afirma que, quanto de interesse público – quando estiverem exercendo função/operação política pública, empresas públicas e sociedades de economia mista terão tratamento semelhante aos dispensados às entidades do Poder público. Portanto, ora será tratado como ente privado, ora a ente público, dependendo da atividade exercida.

Para Pinheiro (2020, p. 61), o art. 24 quis "[...] dar uma diferenciação sobre o tratamento de dados pessoais nas instituições públicas, já se vislumbrando situações futuras relacionadas inclusive ao atendimento de outras legislações, como a Lei de Acesso à Informação."

Teixeira e Guerreiro (2022, s/p) exemplificam tal situação, apresentando o caso do Banco do Brasil, ocorrido em 2013. Segundo os autores: "[...] clientes do Banco do Brasil tiveram seus dados expostos devido a uma falha no site [...] qualquer pessoa conseguia visualizar nome, número do CPF, endereço, telefone, e-mail, agência e número da conta de outro segurado [...]". Neste caso, se a LGPD estivesse em vigência, o Banco do Brasil teria sido tratado como ente privado, já que não estava operacionalizando políticas públicas.

No que tange os conceitos trazidos pelo art. 25, segundo Teixeira e Guerreiro (2022), interoperabilidade é a capacidade de um sistema se comunicar com outro sistema, pressupondo a transparência no tratamento de dados no que tange à execução de políticas públicas, prestação de serviços públicos e à descentralização de atividades públicas. O banco de dados que ajude a implementação de políticas públicas e prestação de serviços públicos deve, portanto, ser o mais fidedigno possível.

O art. 26 destaca a aplicabilidade de todos os princípios da lei para o compartilhamento de dados pelo Poder Público, estabelecendo três requisitos cumulativos: (1) a existência de finalidade específica no compartilhamento; (2) a

existência de base legal para os entes envolvidos; (3) a validação do compartilhamento pelo Teste de Proporcionalidade, decorrente do atendimento dos princípios do artigo 6°.

O texto dos incisos IV e V foi incluído pela Lei n. 13.853/19, que legitimou a possibilidade da transferência de dados pessoais do Poder Público para entidades privadas nas situações em que há a previsão legal, ou para a prevenção de fraudes e irregularidades, segurança ou ainda para garantir a integridade do titular dos dados.

De acordo com Pinheiro (2020), essa alteração é interessante para os entes privados, já que funciona como um aliado na prevenção ao crime. O Controlador deverá ter um encarregado de proteção de dados constituído e poderá – por meio de contratos – garantir a prevenção a fraudes com ajuda do Poder Público, inclusive para transferência de dados do titular, independentemente do consentimento desse sujeito de direito.

O art. 27, por sua vez, trata das hipóteses e requisitos para que se proceda às operações remanescentes: comunicação, difusão, interconexão e tratamento compartilhado. Em parágrafo único, a Lei n. 13.853/19 inclui garantia de abertura e flexibilização no compartilhamento de dados entre os entes públicos e privados, mas demonstrou preocupação em garantir a transparência das relações, pontuando a necessidade de comunicar à ANPD quando houver o compartilhamento de dados pessoais entre Pessoa Jurídica de Direito Público e Pessoa Jurídica de Direito Privado.

Art. 28 foi vetado. No art. 29, a LGPD versa sobre solicitação e poder de requisição. Ressalta-se que “[...] a solicitação é o instrumento jurídico utilizado no pedido de providências entre autoridades de igual hierarquia ou que possuem elevado grau de autonomia, mas, de modo algum, implicam mera facultatividade em seu atendimento” (TASSO, 2019, p. 318). De tal forma, a Lei n. 13.853/19 adicionou a possibilidade de solicitação de informações pela ANPD aos órgãos e entidade governamentais.

No art. 30, ficam estabelecidas as atividades de comunicação e uso compartilhado de dados pessoais no âmbito do Poder Público e esclarece-se que a ANPD pode expandir as normas da LGPD para garantir efetividade e segurança nas atividades de comunicação e uso compartilhado de dados pessoais.

No que tange os conceitos trazidos pelo art. 31, seção II, que trata das responsabilidades da autoridade nacional, Tasso (2019, p. 319-20) afirma que:

> [...] o artigo 31 trata da possibilidade (“poderia”) de a autoridade nacional enviar informe com medidas cabíveis para fazer cessar a violação.
> Sob a ótica da atividade administrativa, tal possibilidade consiste em genuíno poder-dever, pois é uma das atribuições que justificam sua própria razão de existir [...]. Seria possível questionar qual a função, bem como quais seriam as consequências da inobservância das recomendações de cessação da violação.
> Não resta dúvida de que o ato de informar as medidas cabíveis para cessação da violação de direitos e garantias fundamentais decorrentes do tratamento de dados pessoais pelo Poder Público não retira ou mitiga o poder sancionatório da autoridade nacional. Antes, funciona como parâmetro a ser levado em conta no escalonamento da penalidade a ser imposta, sendo tão mais severa quanto o grau de desídia e incúria do administrador público, uma vez ciente da operação de tratamento potencialmente danosa e das medidas passíveis de conter ou mitigar os danos.

O art. 32 estabelece a possibilidade da autoridade nacional solicitar relatórios de impacto à proteção de dados pessoais. Para Teixeira e Guerreiro (2022), tais relatórios deveriam ser regra e não apenas uma possibilidade.

É importante destacar que, em Agenda Regulatório para o biênio 2023-2024 (Portaria ANPD n. 35, de 4 de novembro de 2022 – Anexo 1), a ANPD estabelece mudanças para o compartilhamento de dados pelo Poder Público como iniciativa para o próximo 1 ano (prioridade de fase 2, portanto). Na descrição da iniciativa, a portaria estabelece que:

> O capítulo IV da LGPD dispõe sobre o tratamento de dados pessoais pelo Poder Público. A lei determina que a ANPD disponha sobre as formas de publicidade das operações de tratamento, bem como que contratos e convênios estabelecidos entre o Poder Público e entidades privadas que tenham acesso a dados pessoais constantes de bases de dados deverão ser comunicadas à ANPD. Estudo objetiva a operacionalização dos art. 26 e 27 da LGPD, que tratam do compartilhamento de dados do Poder Público com pessoa de direito privado, especialmente quanto aos procedimentos a serem adotados e às informações que devem ser encaminhadas à ANPD para cumprimento do disposto na Lei (DIÁRIO OFICIAL, 2022).

Destaca-se que as serventias extrajudiciais, os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas de direito público. Sendo assim, precisam:

> "[...] executar movimentos internos e externos não somente para garantirem a sua adequação à LGPD, mas também para incorporarem em seu universo específico os fundamentos, os princípios, as bases legais e o acesso aos direitos dos titulares dos dados pessoais, os quais fazem parte da estrutura fundamental desta legislação protetiva" (LIMA, 2021, p. 33)

Passa-se à apresentação da operacionalização da LGPD nas atividades notariais e registrais, com ênfase em atividades de cartórios de protesto.

3.3 A operacionalização da LGPD nas atividades notariais e registrais: caso dos cartórios de protesto

3.3.1 Serventias extrajudiciais

As serventias extrajudiciais, também denominadas cartórios, são prestadores dos serviços notariais e de registro, que, conforme dispõe a Lei n. 8.935/94 (conhecida como Lei dos cartórios, a qual regulamenta o art. 236 da CF/88[20]), são aqueles de organização técnica e administrativa destinados a garantir a publicidade, autenticidade, segurança e eficácia dos atos e negócios jurídicos.

Quanto à natureza jurídica dos serviços notariais e de registro, Sou (2022, p. 34) afirma que o Capítulo I do Título I da Lei n. 8.935/94 trata da natureza e fins dos serviços notariais e de registro (art. 1º, 3º e 4º - o art. 2º foi vetado) e rege:

> O exercício em caráter privado por delegação do Poder Público não lhes retira o caráter público e, para que atinjam suas finalidades, são delegados a profissionais do direito dotados de fé pública (art. 3º da Lei n. 8.935/94), o que reafirma sua natureza. Os atos emanados dos serviços em questão, assim como os dos demais serviços públicos (atividades próprias prestadas diretamente pelo Estado), gozam de presunção relativa de veracidade, atributo dos atos praticados pelo Poder Público.
> São, portanto, serviços públicos exercidos em caráter privado por um profissional do direito em razão de delegação, organizados técnica e administrativamente para garantir publicidade, autenticidade, segurança e eficácia dos atos jurídicos.

---

[20] Art. 236. Os serviços notariais e de registro são exercidos em caráter privado, por delegação do Poder Público. (Regulamento)
§ 1º Lei regulará as atividades, disciplinará a responsabilidade civil e criminal dos notários, dos oficiais de registro e de seus prepostos, e definirá a fiscalização de seus atos pelo Poder Judiciário.
§ 2º Lei federal estabelecerá normas gerais para fixação de emolumentos relativos aos atos praticados pelos serviços notariais e de registro. (Regulamento)
§ 3º O ingresso na atividade notarial e de registro depende de concurso público de provas e títulos, não se permitindo que qualquer serventia fique vaga, sem abertura de concurso de provimento ou de remoção, por mais de seis meses.

No Brasil, logo após a Proclamação da República, o Poder Público instituiu a figura dos cartórios (serventias extrajudiciais), que tinham como principal efeito solucionar problemas da vida civil dos brasileiros e, desta forma, desonerar o Estado de algumas funções ligadas ao Poder Judiciário, mas que não dependem de sua chancela (escrituras, registros de imóveis, registros de nascimento, casamento, óbito, reconhecimento de assinatura, entre outros) (INSTITUTO DE PROTESTO, 2020).

De acordo com Carloto e Almirão (2021), no sistema denominado “notariado latino”, o tabelião é ao mesmo tempo um oficial público e um profissional do Direito. Consoante disposto no art. 236 , da CF/88, notários e registradores são agentes públicos delegados, ou seja, são agentes que exercem função pública em caráter privado, delegados pelo Poder Público. É, portanto, uma atividade de natureza jurídica com caráter híbrido, pois as atividades têm natureza pública, por um lado, e pela forma privado de gestão e administração das serventias extrajudiciais, por outro lado.

> Sendo a função notarial matéria de ordem pública, é obrigação do notário o atendimento aos interesses da coletividade, de modo que o acervo notarial é de livre consulta. A publicidade possui o escopo de difundir, propagar e trazer notoriedade a um fato ou acontecimento, seja ele público ou privado (LIMA et al., 2021, p. 591).

As atividades notariais e de registro são fiscalizadas pelo Poder Judiciário de cada Estado-membro e por força do art. 236 da CF/88, são exercidos em caráter privado, após delegação do poder público, por pessoa física aprovada em concurso público de provas e títulos. O delegatário recebe a denominação de tabelião (ou notário), se prestador de serviços de notas e de protesto de títulos, ou de oficial de registro (ou registrador), se prestador de serviços de registro. Como gestor em “caráter privado” (art. 236 da CF), é função do delegatário zelar pela qualidade dos serviços, buscando salvaguardar os ativos próprios de sua atividade, por meio de todas as medidas necessárias para tal fim.

Segundo a Lei nº 8.935/94, os titulares de serviços notariais e de registro são os: tabeliães de notas; tabeliães e oficiais de registro de contratos marítimos; tabeliães de protesto de títulos; oficiais de registro de imóveis; oficiais de registro de títulos e documentos e civis das pessoas jurídicas; oficiais de registro civis das pessoas naturais e de interdições e tutelas; oficiais de registro de distribuição.

Os titulares têm independência jurídica, como delegado de função pública que exige a formação de juízo e a tomada de decisões (SOU, 2022). Ainda, segundo o autor:

> A execução dos serviços exige a participação de outras pessoas e, para tanto, podem os delegatários contratar empregados, com remuneração livremente ajustada e sob o regime da legislação do trabalho.
> Os empregados são escreventes e auxiliares, ficando a critério de cada titular determinar o número a contratar. Entre os escreventes, o notário ou registrador escolherá os substitutos para, simultaneamente com o titular, praticar todos os atos que lhe sejam próprios. Entre os substitutos, um será designado pelo titular para responder pelo serviço em suas ausências ou impedimentos (§ 5º do art. 20 da Lei n. 8.935/94). (SOU, 2022, p.43).

Os serviços notariais e de registro são os de organização técnica e administrativa destinados a garantir a publicidade, autenticidade, segurança e eficácia dos atos jurídicos. De acordo com Laureano e Benfatti (2021, p. 98 [grifo dos autores]), as atividades notariais e registrais têm:

> [...] como pilar essencial o *tratamento* de dados pessoais dos usuários do serviço público, seja em formato de livros ou fichas, bem como a manutenção destes em arquivos ou *banco de dados*, armazenados em formato de papel ou eletrônico.

Como qualquer organização, o cartório possui ativos físicos e lógicos, albergam grandes bancos de dados físicos e eletrônicos, nos quais constam dados relevantes para o Poder Público e para particulares (livros e documentos oficiais, e informação armazenada em bancos de dados digitais).

As serventias extrajudiciais são, por definição, um local privilegiado para armazenamento de dados pessoais corretos e adequadamente utilizados, em respeito ao princípio da conservação. Além disso, é um dever “manter em ordem os livros, papéis e documentos de sua serventia, guardando-os em locais seguros” (art. 30, I, da Lei n. 8.935/94) e “praticar, independentemente de autorização, todos os atos previstos em lei necessários à organização e execução dos serviços” (art. 41 da Lei n. 8.935/94).

No caso do tratamento de dados pessoais realizado pelo cartório, devido a sua natureza jurídica, por meio de atos inerentes ao exercício dos respectivos ofícios e na persecução do interesse público e, ainda, executando suas competências legais, terá respaldo no cumprimento de obrigação legal ou cumprimento do dever legal, art. 7º,

II, da LGPD. Igualmente, os cartórios podem utilizar a base legal inserida no art. 7º, III, da LGPD que versa sobre o tratamento e uso compartilhado de dados necessários à execução de políticas públicas, quando fundamentada em lei, regulamentos, convênios e contratos.

> É possível observar que o cumprimento do dever legal não é a única base que dá legitimidade para tratamento de dados pessoais pelos cartórios. Em um cenário mais restritivo pode se utilizar a execução de contrato, consentimento, exercício regular de direitos, para proteção da vida, proteção de crédito e para realização de estudos por órgãos de pesquisa (LIMA et al., 2020, p. 510).

É importante salientar que, com relação aos novos contratos ou os já formalizados, entre os cartórios e colaboradores, é preciso que sejam inseridas cláusulas que versem sobre a privacidade de dados, que sejam elaborados documentos como política de privacidade de proteção de dados dentre outros e revisão para contratos elaborados antes da LGPD.

Os cartórios de protesto (um dos cartórios extrajudiciais existentes) servem para formalizar a falta de pagamento de uma dívida. Um dos movimentos é recorrer ao cartório para demonstrar à sociedade que a dívida existe e garantir que seja paga (ou incluir o nome do devedor em listas de proteção ao crédito e, caso se torne uma ação judicial, poder inabilitar, para algumas transações, o CPF ou CNPJ do inadimplente). O outro é procurar o cartório de protesto para pagamento da dívida (pagamento do título protestado) (INSTITUTO DE PROTESTO, 2020). É importante a observação de Sou (2022, p. 415) quando afirma que:

> Exerce o protesto função probatória quanto ao inadimplemento do devedor. Contudo, e evidentemente, ao se utilizarem dos serviços de protesto, não objetivam os credores a lavratura e o registro do protesto, a provar o descumprimento de obrigação originada em títulos e outros documentos de "dívida. O escopo dos credores é a solução do conflito de interesses, com o recebimento do que lhes é devido.

Desta forma, por se tratar de organização responsável por operações que gerenciam crédito (incluindo e excluindo, dentro de suas atividades cotidianas, indivíduos em listas de proteção ao crédito), os cartórios de protesto têm base legal para tratar dados baseando-se no art. 7º, X, da LGPD. A lei usa termo amplo (X - para a **proteção do crédito**, inclusive quanto ao disposto na legislação pertinente [grifo

nosso]), que pode, por sua natureza, ser aplicado a toda a cadeia de crédito. Segundo Sou (2021, p. 412): “Os serviços de protesto são prestados no interesse público, garantindo segurança às relações jurídicas que envolvem débito e crédito."

Para Lima (2020), o art. 7º, X, rege que as informações sobre adimplência e inadimplência sobre determinado titular poderão ser utilizadas, a fim de se tomar decisão acerca da concessão ou não de crédito, lembrando que, segundo §3º, o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade (deverá ser respeitada a finalidade pela qual eles foram tornados públicos, em eventual uso subsequente por terceiros) a boa-fé (não deverá haver utilização desvirtuando as legítimas expectativas dos seus titulares) e o interesse público (deve ser identificado o interesse público que embasou a disponibilização dos dados, tratando-os especificamente dentro dessas situações).

De acordo com Soler (2021, p. 87):

> [...] a aplicação extensiva desta previsão garante e valida todas as operações necessárias para a realização de um empréstimo, considerando que, embora “invisíveis”, elas são necessárias e utilizadas no mercado. [...] Tangibilizando a proteção ao crédito, podemos afirmar que para o tratamento de dados com base na proteção ao crédito, tanto a instituição financeira, quanto empresas de cobrança e outras que realizam a análise e estudo para o desenvolvimento do “score de crédito”, podem se valer deste inciso para realizar o tratamento de dados. [...] Ressalvamos as hipóteses de uso de dados além das finalidades específicas e o cumprimento de tais atividades relacionadas à proteção e à concessão de crédito, as quais não estão abarcadas nesta base legal.

Legalmente (de acordo com a Lei n. 9.492/97[21]), o protesto é o ato formal e solene pelo qual se prova a inadimplência e o descumprimento de obrigação originada em títulos e outros documentos de dívida (Art. 1º). Em art. 3º, tal lei rege que:

> Art. 3º Compete privativamente ao Tabelião de Protesto de Títulos, na tutela dos interesses públicos e privados, a protocolização, a intimação, o acolhimento da devolução ou do aceite, o recebimento do pagamento, do título e de outros documentos de dívida, bem como lavrar e registrar o protesto ou acatar a desistência do credor em relação ao mesmo, proceder às averbações, prestar informações e fornecer certidões relativas a todos os atos praticados, na forma desta Lei.

[21] Lei n. 9.492, de 10 de setembro de 1997: Define competência, regulamenta os serviços concernentes ao protesto de títulos e outros documentos de dívida e dá outras providências.

Assim, importa esclarecer que os cartórios de protesto, no exercício de suas atividades: concedem publicidade ao inadimplemento de uma obrigação originada em títulos e outros documentos de dívida, trazendo ao credor a possibilidade de dar publicidade ao descumprimento de obrigações. O tabelião de protesto (responsável por todo trâmite) ou seus prepostos devem, ao examinar um título distribuído para seu cartório, fazer a verificação de seus aspectos formais, como a presença de todos os seus requisitos essenciais (clareza nas informações, ausência de rasuras, preenchimento correto, datas de emissão e vencimento devidamente corretas, assinaturas, documentos anexados, entre outros).

Após, o tabelião (ou seus prepostos): (1) intima os devedores dos títulos para aceitá-los, devolvê-los ou pagá-los, sob pena de protesto; (2) recebe o pagamento dos títulos protocolizados, dando quitação; (3) lavra o protesto, registrando o ato em livro próprio, em microfilme ou sob outra forma de documentação; (4) acata o pedido de desistência do protesto formulado pelo apresentante; (5) averba o cancelamento do protesto ou as alterações necessárias para atualização dos registros efetuados e, por fim, (6) expede as certidões de atos e documentos que constem de seus registros e papéis (INSTITUTO DE PROTESTO, 2020).

Resta esclarecer que, para ser tabelião, é preciso ter diploma de bacharel em Direito, ser brasileiro nato e ter sido aprovado em concurso público para o cargo, que só tem validade no Estado onde foram feitas as provas.

Porém, mesmo que o objetivo seja dar publicidade à inadimplência de obrigações, os cartórios de protesto não podem, de forma indiscriminada, publicar ou difundir os dados.

> Ressalte-se que a publicidade decorrente da fé-pública tabelioa não implica, necessariamente, o acesso público geral e irrestrito ao teor dos atos notariais, de forma que não existe uma incompatibilidade apriorística com o sigilo de determinadas informações.
> Essa assertiva se reporta à distinção fundamental entre a publicidade notarial e a publicidade registral188. Nesse sentido, se por um lado os registros públicos são públicos, tanto por serem efetivados por oficiais públicos quanto por serem cognoscíveis, em princípio, a todos189, os atos notariais, por seu turno, são públicos apenas no primeiro sentido190. Não são necessariamente abertos, muito embora possam ser. (LIMA et al., 2021, p. 594)

Por dever ético e legal, o tabelião deve guardar e operacionalizar suas atividades tendo como base a LGPD, observando os regramentos nela contidos.

Assim, passa-se à operacionalização da LGPD em serventias extrajudiciais, mediante análise do caso de cartórios de protesto.

3.3.2 A LGPD nas serventias extrajudiciais: caso de cartórios de protesto

Primeiramente, é importante que se entenda a interseção da temática LGPD e cartórios, ou seja o porquê de ser importante a proteção de dados e privacidade no âmbito das atividades notariais. Há três aspectos básicos, segundo Lima et al. (2021, p. 59), que são: (1) é uma decorrência dos termos da LGPD, por previsão implícita (art. 5o, VI, VII e IV, da LGPD) e expressa (art. 23, § 4o, da LGPD); (2) pelos seus acervos, os cartórios acabam sendo organizações que demandam muita proteção de ativos; e (3) a proteção de informações é inerente à função notarial e de registro, como instituição cuja função é garantir a segurança jurídica.

Nos termos da lei, a primeira interseção se aplica às serventias extrajudiciais já que os agentes delegados são agentes de tratamento de dados pessoais e, sobremaneira, a LGPD expressa em art. 23, §º, igualdade à Administração Pública. Trata-se, portanto, do princípio da legalidade, que incide nos cartórios (art. 37 da CF/88). Em uma perspectiva pragmática, entende-se a segunda interseção, pois os cartórios, enquanto organizações com ativos físicos (livros e documentos oficiais, além de bancos de dados eletrônicos), devem salvaguardar os ativos de sua atividade.

> As serventias extrajudiciais são, por definição, um local privilegiado para armazenamento de dados pessoais corretos e adequadamente utilizados, em respeito ao princípio da conservação [...]. Ademais, é um dever “manter em ordem os livros, papéis e documentos de sua serventia, guardando-os em locais seguros” (art. 30, I, da Lei n. 8.935/94) e “praticar, independentemente de autorização, todos os atos previstos em lei necessários à organização e execução dos serviços” (art. 41 da Lei n. 8.935/94). (LIMA, 2021, p. 62)

Assim, por ter acesso a acervo valioso e volumoso (grande parte composto por dados pessoais), os cartórios precisam boas práticas de segurança, ou seja, a aplicação da LGPD é decorrência inerente à atividade notarial.

Mais sutil, a terceira interseção ultrapassa o objetivo das leis (LGPD e Lei dos Cartórios). Fruto da Antiguidade, ainda na Idade Média há registros de profissionais encarregados de guardar o que fosse digno de conservação. Após evolução constante, chegou-se à autonomia e ao rol de competências dos notários e

registradores como conhecidas atualmente (profissionais independentes, com fé pública e capacitação de títulos). No Brasil, os delegatários tem como função de administrar uma serventia em caráter privado e, assim a “[...] prestação de serviço público (notarial e registral) é delegada a uma pessoa física, que recolhe emolumentos com natureza de taxa, mas não é remunerada pelos cofres públicos, podendo auferir lucros da atividade” (LIMA et al., 2021, p. 63). Há, desta forma, interesse e criar e manter ambiente seguro para dados pessoais.

A LGPD atribui aos serviços notariais, de registro e de protesto, o mesmo tratamento legal dispensado às pessoas jurídicas de direito público, encontrando perfeita harmonia com o art. 173[22], da CF/88 e artigo 24 da LGPD, a *contrario sensu*, que prevê o regime público às empresas públicas e sociedade de economia mista que não desempenhem atividade concorrencial, mas de monopólio (TASSO, 2020).

A LGPD inclui os serviços notariais e registrais em seu rol de obrigações, nos parágrafos 4º e 5º, do artigo 23:

> § 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.
> § 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

---

[22] Art. 173. Ressalvados os casos previstos nesta Constituição, a exploração direta de atividade econômica pelo Estado só será permitida quando necessária aos imperativos da segurança nacional ou a relevante interesse coletivo, conforme definidos em lei.
§ 1º A lei estabelecerá o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias que explorem atividade econômica de produção ou comercialização de bens ou de prestação de serviços, dispondo sobre:
I - sua função social e formas de fiscalização pelo Estado e pela sociedade;
II - a sujeição ao regime jurídico próprio das empresas privadas, inclusive quanto aos direitos e obrigações civis, comerciais, trabalhistas e tributários;
III - licitação e contratação de obras, serviços, compras e alienações, observados os princípios da administração pública;
IV - a constituição e o funcionamento dos conselhos de administração e fiscal, com a participação de acionistas minoritários;
V - os mandatos, a avaliação de desempenho e a responsabilidade dos administradores.
§ 2º As empresas públicas e as sociedades de economia mista não poderão gozar de privilégios fiscais não extensivos às do setor privado.
§ 3º A lei regulamentará as relações da empresa pública com o Estado e a sociedade.
§ 4º - lei reprimirá o abuso do poder econômico que vise à dominação dos mercados, à eliminação da concorrência e ao aumento arbitrário dos lucros.
§ 5º A lei, sem prejuízo da responsabilidade individual dos dirigentes da pessoa jurídica, estabelecerá a responsabilidade desta, sujeitando-a às punições compatíveis com sua natureza, nos atos praticados contra a ordem econômica e financeira e contra a economia popular.

Assim, os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas de direito público (art. 23, § 4°, da LGPD).

Rocha (2020) afirma que é verossímil a preocupação dos notários e registradores, vista a grande quantidade de dados pessoais diariamente tratada pelos cartórios extrajudiciais.

> A atividade notarial é, em nosso país, um serviço intimamente ligado ao Estado que, em certa medida, o representa como agentes políticos e sociais, exercida por particular. Extrai-se dessa atividade, em regra, credibilidade em todas as suas práticas, por meio das declarações escritas, denotando veracidade e a autenticidade daquilo que lhe foi apresentado (FUJITA; MATHEUS, 2021, p. 480).

Cabe destacar que:

> Quanto aos serviços notariais e de registro, o CNJ editou o Provimento n. 74, de 31 de julho de 2018, que dispõe sobre padrões mínimos de tecnologia da informação para a segurança, integridade e disponibilidade de dados para a continuidade da atividade pelos serviços notariais e de registro do Brasil. Esse provimento se adequa às pretensões da LGPD, na medida em que impõe aos serviços notariais e de registro que tenham disponíveis as informações claras sobre o tratamento de dados que realizam, devendo na forma do § 5º fornecer à Administração Pública os dados por meio eletrônico (TEIXEIRA; GUERREIRO, 2022, s/p).

O Instituto de Protesto (IEPTB) de São Paulo lançou cartilha própria para orientar a operacionalização da LGPD nas atividades do tabelionato de protesto. Tal cartilha afirma que o Provimento n. 74/2018 estabelece que os cartórios devem adotar políticas de segurança de informação que garantam: confiabilidade, disponibilidade, autenticidade, integridade e mecanismos preventivos de controle físico e lógico da informação. Ainda, as orientações salientam que o descumprimento das medidas previstas no Provimento n. 74/2018 “[...] ensejará a instauração de procedimento administrativo disciplinar, sem prejuízo de responsabilização cível e criminal e das sanções previstas na LGPD.” (INSTITUTO DE PROTESTO, 2021).

Fica estabelecido que o Comitê de Gestão da Tecnologia da Informação dos Serviços Extrajudiciais (Cogetise) é o responsável pela atualização anual dos pré-requisitos mínimos, além de ser responsável por divulgar, estimular, apoiar e detalhar a implementação das diretrizes do Provimento nº 74/2018. O Cogetise é formado Corregedoria Nacional de Justiça, na condição de presidente; Corregedorias de

Justiça dos Estados e do Distrito Federal; Associação dos Notários e Registradores do Brasil (Anoreg/BR); Colégio Notarial do Brasil – Conselho Federal (CNB/CF); a Associação Nacional dos Registradores de Pessoas Naturais do Brasil (Arpen/BR); o Instituto de Registro Imobiliário do Brasil (Irib/BR); o Instituto de Estudos de Protesto de Títulos do Brasil (IEPTB/BR); e o Instituto de Registro de Títulos e Documentos e de Pessoas Jurídicas do Brasil (IRTDPJ/BR) e é responsável pela fixação de prazos para adequação dos cartórios às obrigações previstas no Provimento n. 74/2018.

Em 11 de setembro de 2019, por meio do Provimento n. 87, o CNJ apresentou as normas gerais de procedimentos para o protesto extrajudicial de títulos e outros documentos de dívida, regulamentou a implantação da Central Nacional de Serviços Eletrônicos dos Tabeliães de Protesto de Títulos (CENPROT[23]) e deu outras providências.

Por meio do provimento n. 87/2019 o protesto tornou-se "[...] a primeira atividade extrajudicial 100% digital do País, incentivando a redução do custo do crédito no Brasil, promovendo a desjudicialização de conflitos e a integração eletrônica dos tabelionatos com sistema financeiro." (LIMA et al., 2021, p. 142). Segundo Lima et al. (2021, p. 142):

> É importante destacar que o Provimento n. 87/2019 não prejudica a arrecadação; na verdade facilita, uma vez que visa ao aumento do volume de títulos que podem ser levados aos cartórios de Protesto, possibilitando conceder parcelamento de emolumentos. Esse parcelamento pode ser feito por meio de cartão de crédito. Também é aceito pagamento por meio de cartão de débito. Tais possibilidades elevam as chances de o usuário quitar esses valores integralmente.

Segundo os autores, o Provimento n. 87/2019 foi um marco para a inovação e um estímulo para que as serventias extrajudiciais se adaptem às boas práticas e normas de segurança tecnológica.

Em 26 de maio de 2020, o CNJ estabeleceu, em Provimento n. 100, a prática de atos notariais eletrônicos utilizando o sistema e-Notariado, criou a Matrícula Notarial Eletrônica-MNE e deu outras providências. Esse provimento possibilitou a lavratura de todos os atos físicos que normalmente são feitos, presencialmente, nas

---

[23] A CENPROT é uma central de escrituração e emissão de duplicatas, que oferta: acesso ao instrumento de protesto eletrônico, consulta pública e gratuita de um título protestado, declaração de anuência eletrônica, pedido de cancelamento de protesto, pedido de certidão digital e confirmação de autenticidade e, por fim, recepção e distribuição de títulos (CRA).

Serventias Notarias, tais como: procurações, escrituras, testamentos, reconhecimento de firma e, até mesmo, autenticação, por meio eletrônico. De forma única e válida em todo o território nacional, o provimento estabeleceu para todos os Estados um mesmo procedimento. Anteriormente, cada um ao seu modo, os Estados usavam procedimentos de atos notariais eletrônicos diversos (o que gerava certa insegurança jurídica).

Outro provimento, publicado em 24 de agosto de 2022, pelo CNJ, estabelece medidas a serem adotadas pelas serventias extrajudiciais em âmbito nacional para o processo de adequação à LGPD. Especificamente no que tange os cartórios de protesto, o Provimento n. 134, de 24 de agosto de 2022, rege, em seu Capítulo XV – Do protesto de títulos e outros documentos de dívida, em seu art. 51, que das certidões individuais de protesto deverão constar, sempre que disponíveis, os dados enumerados no art. 17, parágrafo único, do Provimento 87, da Corregedoria Nacional de Justiça, excetuados endereço completo, endereço eletrônico e telefone do devedor.

Em art. 52, o provimento rege que as certidões em forma de relação sobre inadimplementos por pessoas naturais serão elaboradas pelo nome e CPF dos devedores, devidamente identificados, devendo abranger protestos por falta de pagamento, de aceite ou de devolução, vedada exclusão ou omissão, espécie do título ou documento de dívida, data do vencimento da dívida, data do protesto da dívida e valor protestado.

O art. 53 afirma que nas informações complementares requeridas em lote ou em grande volume poderão constar CPF dos devedores, espécie do título ou documento de dívida, número do título ou documento de dívida, data da emissão e data do vencimento da dívida, valor protestado, protocolo e data do protocolo, livro e folha do registro de protesto, data do protesto, nome e endereço do cartório.

No art. 54, fica estabelecido que o fornecimento de cópias ou certidões de documentos arquivados na serventia se limita ao documento protestado propriamente dito, nos termos do art. 31 da Lei n. 9.492/1997[24], enquanto perdurar o protesto, e dentro do prazo máximo de 10 (dez) anos, nos termos do art. 36 Lei n. 9.492/1997[25],

[24] Art. 31. Poderão ser fornecidas certidões de protestos, não cancelados, a quaisquer interessados, desde que requeridas por escrito.
[25] Art. 36. O prazo de arquivamento é de três anos para livros de protocolo e de dez anos para os livros de registros de protesto e respectivos títulos.

não devendo ser fornecidas cópias dos demais documentos, salvo para as partes ou com autorização judicial. Parágrafo único. Tratando-se de documento de identificação pessoal, a cópia arquivada somente deve ser fornecida ao próprio titular.

Além disso, o art. 55 estabelece que o tabelião de protesto poderá devolver ou eliminar documentos apresentados para protesto/ cancelamento que forem considerados desnecessários à prática do ato almejado, após adequada qualificação. Ainda, (1) § 1º O documento cujo original não precise ser guardado por imposição legal deve ser eliminado de maneira segura quando for digitalizado, evitando-se a duplicidade (art. 35, § 2º, Lei n. 9.492/1997[26]); (2) § 2º Fica o tabelião de protesto autorizado a eliminar o documento após o término do prazo da tabela de temporalidade prevista no Provimento 50, da Corregedoria Nacional de Justiça, ou superada a necessidade de sua guarda por outras circunstâncias, tais como prescrição civil, tributária e penal.

O art. 56 esclarece que, antes da expedição do edital para intimação do devedor, o tabelião poderá buscar outros endereços em sua base de dados, endereços em que outros tabeliães realizaram a intimação, desde que na mesma base da sua competência territorial, ou endereços eletrônicos, a serem compartilhados por meio da Central Nacional de Serviços Eletrônicos Compartilhados (CENPROT), bem como endereços constantes de bases de natureza jurídica pública e de acesso livre e disponível ao tabelião.

Em parágrafo único, o Provimento n. 134, estabelece que a CENPROT deverá compartilhar entre os tabeliães os endereços em que foi possível a realização da intimação de devedores, acompanhado do CNPJ ou CPF do intimado, bem como da data de efetivação.

Finalizando o capítulo, o art. 57 rege que a declaração eletrônica de anuência para fins de cancelamento de protesto, recebida na forma prevista no art. 17, inciso V, do Provimento 87, da Corregedoria Nacional de Justiça, poderá ser comunicada ao interessado por meio dos Correios, empresas especializadas, portador do próprio tabelião ou correspondência eletrônica, via internet ou qualquer outro aplicativo de mensagem, ficando autorizado o encaminhamento de boleto bancário, outro meio de

[26] Art. 35. O Tabelião de Protestos arquivará ainda: [...] § 2º Para os livros e documentos microfilmados ou gravados por processo eletrônico de imagens não subsiste a obrigatoriedade de sua conservação.

pagamento ou instruções para pagamento dos emolumentos e despesas relativos ao cancelamento do protesto (Adaptado de CNJ, 2022).

Em suas considerações gerais, o Provimento n. 134/22 estabelece que as disposições previstas na LGPD deverão ser cumpridas, tendo como base o art. 55-J (aqui já apresentado) e as diretrizes, regulamentos, normas, orientações e procedimento da ANPD. Ainda, estabelece que os responsáveis pelas delegações dos serviços extrajudiciais são os titulares das serventias, portanto controladores a quem compete as decisões referentes ao tratamento de dados pessoais. Em nome e por ordem do controlador, o operador é a pessoa natural ou jurídica, de direito público ou privado, externa ao quadro funcional da serventia – contratada, pois, para serviço que envolva o tratamento de dados pessoais.

Laureano e Benfatti (2021, p. 99) afirmam que o operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais, já o controlador é a pessoa natural ou jurídica, de direito público ou privado, que recebe os dados do titular e detém o controle sobre como, por que e para qual fim serão aplicados estes dados, "[...] considerando uma estrutura na qual esteja legal ou contratualmente autorizado ou obrigado a compartilhar, divulgar ou torná-lo público (por exemplo, os bancos, as corretoras de saúde, etc.)".

Há a necessidade implícita – igual ocorre em cada uma das mudanças vivenciadas pelo amplo uso das TIC's – de treinamento e capacitação, tanto de operadores, quanto de tabeliões titulares das serventia (e seus prepostos), para que seja operacionalizada a LGPD em cartórios, o que inclui os cartórios de protesto. Porém, extra subjetividade, há, previsto em texto legal, a obrigação de treinamento.

Segundo a LGPD, em seu artigo 41, cabe ao controlador indicar um encarregado pelo tratamento de dados pessoais e, entre as atribuições do encarregado está a de orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais. Além disso, cabe ao controlador, segundo art. 50 da LGPD [grifo nosso]:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão **formular regras de boas práticas e de governança** que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, **as ações educativas**, os mecanismos

> internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Algumas das ações educativas do controlador, para que se estabeleça a boa gestão de um cartório seriam: (1) avaliar a participação em atividades de treinamento em privacidade e proteção de dados (por exemplo, número de participantes, pontuação); (2) fornecer educação e treinamento contínuos para o *Privacy Office* e / ou DPOs[27] (por exemplo, conferências, seminários on-line, palestrantes convidados); (3) conduzir *walk-throughs* (treinamentos/ orientações) periódico; (4) incorporar a privacidade e proteção dos dados ao treinamento operacional, como RH, segurança, call center; (5) oferecer treinamento / conscientização em resposta a questões / tópicos que vierem a surgir oportunamente; (6) manter e disponibilizar material de conscientização de privacidade e proteção de dados (por exemplo, pôsteres e vídeos); (7) conduzir treinamento em privacidade e proteção de dados e dados sensíveis; (8) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; entre outras (YUN, 2020).

Lima et al. (2020) reforça que a boa gestão e a correta operacionalização da LGPD baseia-se no tripe tecnologia-processos-pessoas, pois dependem de boa tecnologia (investimento constantes em equipamentos adequados e modernos), ordenação adequada de tarefas e treinamento da equipe. A tecnologia e as inovações tecnológicas têm papel de destaque nesta tríade, já que garantem o processo básico de proteção e gerenciamento de riscos.

Além disso, para os autores, é importante o planejamento das ações educativas e de conscientização para operacionalização da LGPD em cartórios, além de garantir acesso facilitado ao treinamento e o uso de linguagem acessível. Ainda, o conteúdo e a carga horária de treinamento varia conforme três aspectos: (1) natureza dos dados tratados: por apresentar maiores riscos, a orientação sobre o tratamento de dados sensíveis difere da orientação sobre o tratamento de dados comuns e quem tem acesso a dados sensíveis deve possuir maior carga horária de treinamento; (2) tipo de tratamento realizado: difere o treinamento conforme a complexidade do tratamento realizado, assim as pessoas que efetuam processamento dos dados executam atividades mais complexas em relação a quem apenas os armazena; (3) nível

[27] Encarregado pela privacidade e proteção dos dados a um indivíduo (por exemplo: Privacy Officer, Privacy Counsel, DPO).

hierárquico: o treinamento deve ser direcionado conforme o poder de decisão da pessoa na organização, portanto, em ordem crescente: funcionários terceirizados; auxiliares do cartório; escreventes; substitutos; operadores de dados (externos) (LIMA et al., 2021). Salienta-se que:

> Engana-se o delegatário que entender que é suficiente tomar apenas uma medida (por exemplo, fornecer um treinamento apenas). A esperada adesão de todos às políticas de tratamento de dados pessoais só ocorre por meio das ações educacionais constantes e diversificadas. Portanto, transcorrida a etapa de conscientização ou sensibilização inicial, é preciso constante aprofundamento e rememoração (LIMA et al., 2021, p. 86).

Em cartilha, o IEPTB estabelece como principais responsabilidades dos controladores as seguintes atribuições, citando os artigos a que coaduna cada uma delas: (1) obter consentimento, quando necessário, assim como demonstrar, em caso de necessidade, como o consentimento foi obtido (art. 7°, §5°; art. 8°, §6°); (2) informar e prestar contas; garantir a portabilidade (art. 9°; art. 18; art. 20); (3) garantir a transparência no tratamento de dados baseado em legítimo interesse (art. 10, §2°); (4) manter registro das operações de tratamento de dados pessoais, especialmente quando baseado no legítimo interesse (art. 37); (5) elaborar relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, com observância dos segredos comercial e industrial (art. 10; §3°; art. 38); (6) indicar o encarregado pelo tratamento de dados (art. 41); (7) reparar danos patrimoniais, morais, individuais ou coletivos causados por violação à legislação de proteção de dados pessoais (art. 42); (8) comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (art. 48); (9) salvaguardar os direitos dos titulares mediante a adoção de providências, divulgação do fato em meios de comunicação; medidas para reverter ou mitigar os efeitos do incidente (art. 48, §2°); (10) observar as boas práticas e padrões de governança (art. 50) (INSTITUTO DE PROTESTO, 2021).

Na prática das atividades cotidianas, para que se possa fornecer adequadamente os serviços do cartório de protesto, na persecução do interesse público, há a coleta de dados pessoais, que são armazenados em sistemas próprios ou contratados. Sendo assim, no cotidiano de um cartório de protesto, quanto aos dados sensíveis sob proteção da LGPD que um cartório de protesto processa, tem-se

garantia de proteção para todos dados e informações relacionados à identificação da pessoa, seja natural ou jurídica. Dentre os dados protegidos, observam-se o nome, seja civil, denominação ou fantasia. Mesmo que esta informação fique velada em virtude da roupagem da PJ, os nomes dos representantes legais também têm essa proteção, assim como os endereços, as referências, os telefones e as atividades que podem servir de substrato para identificação e individualização da informação.

Mesmo que seja função do cartório de protesto tornar pública uma dívida, deve-se, na prática, proteger e tutelar o banco de dados que o cartório possui (natureza pública da atividade), sendo sua publicidade mitigada, mediante requerimento e identificação documental do requerente. Assim, o cartório pode publicizar e divulgar a informação requerida. Por exemplo, no site www.pesquisaprotesto.com.br, com a inserção de CPF/CNPJ, é possível verificar o valor e local de protesto da dívida, não necessitando qualquer identificação do requerente, nem os motivos da consulta, anonimizando todo o restante sensível da informação restritiva: nome, endereço, telefone, data do protesto, natureza da dívida, entre outros.

Nem mesmo um contrato protestado que contenha dados pessoais – que não façam diferença para a publicidade do crédito – pode ser divulgado na íntegra, pois a natureza dos cartórios de protesto é pública e de tutela do bem jurídico econômico como fonte de circulação saudável e de confiança do crédito, não constituindo mero meio de publicidade de informações. Assim, todas as informações irrelevantes ao tráfego econômico e jurídico da informação deve ser igualmente protegido. Ressalta-se, por oportuno, que é o típico caso das informações creditícias e restritivas com mais de cinco anos, ou seja, elas "desaparecem" do sistema ao cabo do quinquídio.

Além disso, para que se cumpra a função do cartório de protesto, todas as publicações cumprem a legislação de proteção ao consumidor, tendo consentimento informado, e estrito cumprimento do dever legal e prestação de informações seguras, úteis e qualificadas juridicamente. Há transferência de dados para empresas de proteção de crédito, por expressa previsão legal. Os birôs de crédito[28], notadamente

[28] Birôs de crédito são empresas que reúnem dados sobre o histórico financeiro das pessoas. Essas informações são verificadas por diversas empresas e instituições financeiras quando elas precisam decidir se vão ou não liberar um pedido de crédito, por exemplo. Os birôs de crédito (a palavra vem do francês "bureau") são empresas que registram o histórico de pagamentos de uma pessoa. Na prática, funcionam como grandes bancos de dados. Se o consumidor atrasa o pagamento de uma conta ou faz uma nova dívida, por exemplo, essa informação é registrada nos birôs. O contrário também ocorre: se você quita uma dívida atrasada ou negativada, essa informação também vai para os birôs. Por isso, os

SERASA e CDL Brasil, adquirem essas informações e tratam esses dados para a melhor e mais justa concessão de crédito no mercado. O cartório de protesto assina termo de conduta e o cumprimento imperativo da lei, também cogente para as referidas instituições.

Sob pena de responsabilização pela LGPD, o cartório de protestos, do ponto de vista de condutas comissivas, não pode publicar indiscriminadamente a relação de credores e devedores, não pode promover editais públicos de maus pagadores sem o filtro legal, não pode publicar cobranças públicas e vexatórias, entre outras ações; já do ponto de vista da omissão, não pode deixar de efetuar o *backup* de seus dados, não pode deixar de qualificar juridicamente as relações de crédito e débito que lhe são expostas, não deve deixar de proteger os dados constantes de seus acervos, seja por meio de prevenção cibernética e/ou física, entre outras ações.

O Instituto de Protestos-BR (2022) estabelece as categorias e descreve o motivo e a forma de tratamento destes dados. O Quadro 8 apresenta resumidamente tais fatores.

Quadro 8 – Dados tratados e descrição do motivo do tratamento

CATEGORIA DE DADOS TRATADOS	DESCRIÇÃO E MOTIVO DO TRATAMENTO
Dados pessoais fornecidos pelo Cliente para cadastro nos sistemas, utilização de nossos Serviços e cumprimento de obrigação legal ou regulatória previstas nas Leis nº 9.492/97, 8.935/94, Lei nº 13.775/18 e Provimento nº 87/19 do CNJ e Resolução nº 01/19 do Conselho Gestor da CENPROT	A partir do seu cadastro nas plataformas do o Instituto de Estudos de Protesto de Títulos do Brasil - IEPTB e/ou do seu acesso aos nossos Serviços por meio de login e senha ou certificado digital, podemos tratar os seguintes dados: (1) dados cadastrais: (a) Representantes dos Cartórios: nome do Tabelião e CPF; quando os dados do cartório estiverem em nome do Tabelião, também podemos tratar dados bancários; (b) Usuário administrador: nome, telefone, e-mail e CPF; (c) Usuário da plataforma/ Escreventes/ Preposto: nome, CPF, telefone, função, e-mail e senha; (2) dados de título (instrumento de protesto): nome, data e número de protocolização, nome do apresentante e endereço, reprodução ou transcrição do documento ou das indicações feitas pelo apresentante e declarações nele inseridas, certidão das intimações feitas e das respostas eventualmente oferecidas, indicação dos intervenientes voluntários e das firmas por eles honradas, aquiescência do portador ao aceite por honra, nome, número do documento de identificação do devedor e endereço, data e assinatura do Tabelião de Protesto, de seus substitutos ou de Escrevente autorizado; (3) documentos de identidade; (4) dados bancários. Esses dados são coletados somente quando

birôs também são chamados de empresas de proteção ao crédito: porque se uma pessoa pedir crédito a uma instituição (como um empréstimo a um banco ou um parcelamento a uma varejista), os birôs serão consultados para que a instituição tenha mais informações sobre o histórico de pagamento do solicitante. A partir dos dados dos birôs, as empresas que oferecem crédito podem fazer suas análises para conceder ou não empréstimos, cartões de crédito, financiamento etc. (ORTIZ, 2022).

	necessários para o fornecimento de nossos Serviços por meio do cadastro do Cliente na Central Nacional de Serviços Eletrônicos Compartilhados - CENPROT, gestão do instrumento de protesto, prestação e operacionalização dos Serviços prestados, manutenção do seu cadastro em nossas bases, acompanhamento e gestão de pagamento das custas, emolumentos e do instrumento de protesto.
Dados de fornecedores e prestadores de serviço	O IEPTB pode coletar dados de fornecedores ou prestadores de serviços contratados e de seus sócios, tais como: nome, número de celular, CPF, CNPJ, endereço e e-mails funcionais. Esses dados são coletados somente quando necessários para o controle interno da ordem de serviço executada, cadastro dos parceiros, acompanhamento dos serviços executados no/para o IEPTB, elaboração de contratos, avaliar as documentações regulatórias aplicáveis disponíveis, emitir a nota fiscal, bem como garantir a relação de confiança entre as partes.
Dados de uso e navegação na plataforma de Clientes	Coletamos informações sobre as atividades realizadas através do uso de nossos websites e nossas plataformas como as CENPROTs (Cartórios, Empresas, Estadual e Pública) e CRA, como datas, duração e frequência das sessões do Cliente e acesso por qualquer meio ao Serviço e geolocalização do dispositivo, tablets ou computadores por meio dos quais o Serviço é acessado e utilizado; endereço de IP da conexão, data, horário, duração e frequência do acesso à Plataforma e informações gerais, de caráter estatístico, anonimizadas, que incluem informação técnica sobre o Seu dispositivo, sistema operacional e ID. Também poderemos utilizar ferramentas, próprias ou de terceiros, para monitoramento das atividades realizadas enquanto Você acessa o nosso site, tais como cookies e ferramentas de *analytics* e performance.
Dados para comunicação informativa com CRAs Estaduais, Cartórios, empresas e clientes conveniados	Podemos coletar nome, comarca do título, e-mail e número do cartório para fins de realizar comunicações informativas por e-mail ou plataformas internas com os cartórios, CRAs Estaduais, empresas e clientes conveniados, sem o intuito de captação de clientes ou leads.
Dados tratados para exercício regular de direitos pelo IEPTB em processos judiciais, administrativos ou arbitrais	Podemos tratar dados pessoais para que possamos analisar e comprovar fatos e questões sob a perspectiva jurídica, de modo a atuar e instruir demandas judiciais, administrativas ou arbitrais das quais o IEPTB figure como parte ou, de alguma forma, seja parte interessada, bem como quando necessário para responder, de boa-fé, a ordens judiciais ou demais intimações encaminhadas por órgãos competentes e cumprimento de obrigação legal ou regulatória prevista no âmbito do protesto. Dessa forma, podemos manter seus dados para estrito cumprimento desta finalidade.

Fonte: Adaptados de Instituto de Protestos-BR (2022).

Destaca-se que o uso da primeira pessoa do discurso é proposital, pois, segundo o Instituto de Protestos-BR (2022), a política apresentada é destinada ao cliente, fornecedor ou prestador de serviço, mantendo informações e linguagem clara e objetiva, para garantir a transparência sobre como os dados são coletados, como são tratados e como são compartilhados.

Sobre o compartilhamento de dados pessoais, realizados dentro dos limites da legislação aplicável ao IEPTB, para fins de cumprimento das atividades do cartório de

protesto, com objetivo de melhor atender ao público, pode-se compartilhar os dados dos clientes com terceiros para a realização e prestação de nossos

Serviços regulados por lei, com garantia da mesma proteção aos dados pessoais conferida pela Política de Privacidade e Cookies do IEPTB (que inclui: (1) envio de títulos a protesto; (2) consulta eletrônica de informações de existência ou inexistência de protesto; (3) disponibilização para impressão ou download de instrumento eletrônico de protesto; (4) recepção de declaração eletrônica de anuência para fins de cancelamento do protesto, bem como de solicitação eletrônica de cancelamento de protesto; (5) recepção de pedidos de certidão de protesto e disponibilização de certidão eletrônica de protesto.

É importante apresentar, da mesma forma, os direitos dos clientes em relação ao processamento dos dados pessoais quando envolvidos em atividades de cartórios de protesto. Os clientes, de forma gratuita, após comprovada a titularidade, podem exercer os direitos referentes ao processamento, conforme estabelecido na LGPD. Ainda, nos termos do art. 20[29] do Provimento CNJ nº 134/2022, a gratuidade do livre acesso dos titulares de dados (art. 6º, IV, da LGPD) será restrita aos dados pessoais constantes nos sistemas administrativos da serventia, não abrangendo os dados próprios do acervo registral e não podendo, em qualquer hipótese, alcançar ou implicar a prática de atos inerentes à prestação dos serviços notariais e registrais dotados de fé-pública.

Ainda, aos clientes de serviços de cartórios de protesto, é apresentado e explicado um rol de direitos, no que tange a política de privacidade. Sobre o Direito à informação (Art. 9 e 18, VII e VIII da LGPD), é informado que existe o direito de ser

---

[29] CAPÍTULO IX DAS MEDIDAS DE TRANSPARÊNCIA E ATENDIMENTO A DIREITOS DE TITULARES
Art. 20. A gratuidade do livre acesso dos titulares de dados (art. 6º, IV, da LGPD) será restrita aos dados pessoais constantes nos sistemas administrativos da serventia, não abrangendo os dados próprios do acervo registral e não podendo, em qualquer hipótese, alcançar ou implicar a prática de atos inerentes à prestação dos serviços notariais e registrais dotados de fé-pública.
§ 1º Todo documento obtido por força do exercício do direito de acesso deverá conter em seu cabeçalho os seguintes dizeres: "Este não é um documento dotado de fé pública, não se confunde com atos inerentes à prestação do serviço notarial e registral nem substitui quaisquer certidões, destinando-se exclusivamente a atender aos direitos do titular solicitante quanto ao acesso a seus dados pessoais".
§ 2º A expedição de certidões deverá ser exercida conforme legislação específica registral e notarial e taxas e emolumentos cobrados conforme regulamentação própria.
§ 3º Mantém-se o disposto quanto aos titulares beneficiários da isenção de emolumentos, na forma da lei específica.
§ 4º O notário e/ou registrador coletarão as informações necessárias para identificação segura do solicitante, com o objetivo de garantir a confidencialidade.

informado sobre: (1) a finalidade, a forma e a duração do tratamento; (2) a identificação e as informações de contato do IEPTB; (3) as informações acerca do compartilhamento dos dados com entidades públicas e privadas, a finalidade desse compartilhamento e as responsabilidades dos agentes de tratamento envolvidos; e (4) como exercer outros direitos previstos na Lei, como os direitos do art. 18 da LGPD.

Sobre o direito de confirmação ao tratamento e direito de acesso (Art. 18, I e II da LGPD), há o direito de confirmar se o cartório de protesto trata os dados pessoais, assim como o cliente poderá solicitar acesso a essas informações. Sobre o direito à retificação dos seus dados (Art. 18, III da LGPD), é informado que existe o direito de requisitar a correção de dados incompletos, inexatos ou desatualizados na base de dados do IEPTB, de acordo com a LGPD e da Lei do *Habeas Data*.

O IEPTB fará esforços para informar seus parceiros e terceiros a respeito da necessidade de atualização dos dados (art. 18, § 6º), exceto quando essa comunicação for comprovadamente impossível ou implicar em esforço desproporcional. Destaca-se que, em caso de documentos ou informações apresentadas ou distribuídas no para fins de protesto são de responsabilidade do apresentante, não possuindo o IEPTB ingerência por estes dados ou possibilidade de atualização/correção de instrumentos de protesto, conforme previsto no art. 5, § único da Lei nº 9.492/97[30].

Quanto ao direito à anonimização, ao bloqueio, à eliminação de dados desnecessários (Art. 18, IV da LGPD) e à oposição (Art. 18, § 2º da LGPD), o cliente é informado de que, quando os dados pessoais tratados forem desnecessários, excessivos ou tratados em desconformidade com a Política do IEPTB ou com a legislação aplicável, existe o direito de solicitar, caso aplicável: (1) a anonimização; (2) o bloqueio; (3) a eliminação, de seus dados pessoais; ou (4) a oposição ao tratamento, mesmo que tais dados sejam tratados mediante outra base legal que não o consentimento - salvo em caso de protestos decorrentes da Lei nº 9.492/97 e 8.935/94.

Cumpre destacar que todos os títulos e documentos de dívida protocolizados serão examinados em seus caracteres formais e terão curso se não apresentarem vícios, não cabendo ao Tabelião de Protesto ou ao IEPTB investigar a ocorrência de

---

[30] Parágrafo único. Ao apresentante será entregue recibo com as características essenciais do título ou documento de dívida, sendo de sua responsabilidade os dados fornecidos.

prescrição ou caducidade ou alterar dados pessoais decorrentes dos títulos recebidos em seus sistemas - nestes casos, os pedidos devem ser realizados nos respectivos Cartórios. O IEPTB recomenda que o pedido indique as razões pelas quais o cliente entende que os dados estão sendo tratados em desconformidade com a legislação de proteção de dados pessoais.

Diante disso, o cartório retorna ao cliente com informações e respostas mais precisas a respeito dos fatos questionados. O pedido é registrado e caso seja verificada e diagnosticada alguma dessas hipóteses, é compromisso dos cartórios de protesto excluir os dados questionados. Caso não seja possível verificar qualquer irregularidade, os cartórios de protesto deverão informar ao cliente a respeito e procurar resolver eventuais dúvidas relacionadas às atividades de tratamento.

Há, expresso em comunicado de direitos, o direito de revogação do consentimento e eliminação dos dados pessoais tratados com o consentimento do titular (Art. 18, VI e IX da LGPD), explicado ser possível que o cliente, de forma livre e a qualquer momento, revogue seu consentimento a determinado tratamento de dados mediante manifestação expressa, gratuita e facilitada, sempre que esta for a base legal utilizada. Dá mesma forma, é explicado que não está assegurado o direito de portabilidade (Art. 18, V, da LGPD), já que se trata de dados utilizados no serviço de protesto regulado pela Lei 9.492/97, em razão da insubstitutividade do protesto, e do regime de territorialidade do serviço, não havendo possibilidade de portabilidade dos dados pessoais. Contudo, mais esclarecimentos sobre a implementação e concretização deste direito estão pendentes de regulamentação pela Autoridade Nacional de Proteção de Dados – ANPD.

O direito de revisão ou explicação de tomada de decisão automatizada (Art. 20, da LGPD) é garantido ao cliente o direito de solicitar revisão das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais quando estas decisões afetam diretamente os seus interesses e de receber uma explicação acerca dos critérios e procedimentos que levaram a ela, observados os segredos comercial e industrial (Adaptados de Instituto de Protestos-BR, 2022).

Ressalta-se que os operadores devem operacionalizar dados pessoais estritamente após instruções do controlador, além de fornecer garantias de que foram implementadas as medidas técnicas e organizacionais adequadas para manter os dados pessoais protegidos.

4 CONCLUSÕES

As últimas décadas – principalmente os últimos anos, pelo aumento exponencial do uso da internet em consequência do enfrentamento da pandemia da Covid-19 e da necessidade de isolamento social – viu-se um acréscimo da exposição de dados pessoais e um aumento exponencial do fluxo de transações com dados pessoais. A quantidade de dados e informações geradas, a cada ano, pela humanidade, e o uso de tecnologias como smartphones, redes móveis de internet, Wi-Fi, a internet das coisas (IoT), o uso de *Big Data* e algoritmos de inteligência artificial transformaram radicalmente a economia e as relações sociais. Na Era da Informação, como comumente se nomeia o que contemporaneamente se vive, a informação é o elemento base para o desenvolvimento econômico, tornando-se um bem tão valioso quanto o dinheiro.

A discussão sobre a proteção de dados pessoais é uma tendência mundial, observada nas últimas quatro décadas, enraizada em diversos ordenamentos jurídicos, e com uma evolução natural, condizente com os avanços tecnológicos. A problemática apresenta diversos desdobramentos, incluindo o que tange aos direitos fundamentais. A busca por proteção jurídica dos dados pessoais é um movimento global (com maior ou menor intensidade, variando de país para país). A complexidade das relações sociais leva a discussões sobre o respeito à privacidade, liberdade de expressão, inviabilidade da intimidade, da honra e da imagem, livre iniciativa, direitos humanos, livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais, pois são fundamentos que vêm à tona e forçam a sociedade moderna a integrá-los no contexto das novas legislações.

Porém, não é o acesso à informação o maior entrave à privacidade, mas sim sua geração, seu processamento e sua transmissão. Dados são coletados (acessados) e são armazenados, organizados, categorizados (tratados) e convertidos em algo decifrável: a informação. A interpretação dessas informações (por organizações econômicas, de bens e/ou serviços) agrega conhecimento, suscita vantagem competitiva e gera a problemática do acesso à informação, pois os dados (lá do início do processo) são obtidos, comumente, sem o consentimento do indivíduo.

Diante do exposto, era de se esperar que, tendo em vista a grande quantidade de dados e velocidade com que estes dados podem trafegar pela rede mundial de computadores, uma legislação específica fosse criada para regulamentara proteção dos dados pessoais. A LGPD dispõe sobre o tratamento de dados pessoais, “inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (Art. 1º).

Assim, em uma sociedade que vivencia, cada vez mais frequentes, profundas e aceleradas transformações, sobretudo ligadas às inovações tecnológicas, no Brasil surge a Lei 13.709/2018 – a LGPD, cujo objetivo principal é criar um âmbito legal de proteção para a privacidade e operacionalização dos dados pessoais dos indivíduos, sem, no entanto, impedir o direito à informação ou ser contrária à transparência de ações. Aprovada em 14 de agosto de 2018, com vigência a partir de 18 de setembro de 2020, e muito ainda para evoluir, sendo assim, segue sendo modificada, o que indica que há um longo e árduo caminho a ser percorrido na busca por garantir efetivamente proteção jurídica aos direitos fundamentais de liberdade e de privacidade.

A legislação brasileira, mesmo antes da promulgação da LGPD já contava com alguns dispositivos legais que, de alguma forma, regiam o direito à privacidade e davam proteção jurídica aos dados pessoais (tais como: a Constituição Federal (CF/88), o Código de Defesa do Consumidor (Lei n. 8.078/1990), o Decreto do Comércio Eletrônico (Lei n. 9.507/1997), a Lei de Acesso à Informação (Lei n. 12.527/2011), a Lei do *Habeas Data* (Decreto n. 7.962/2013), o Marco Civil da Internet (Lei n. 12.965/2014), o Código Civil (CC). Em 10 de fevereiro de 2022, a EC 115/22 foi promulgada, alterando a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Além de aprofundar e dar maior visibilidade às normas existentes, a LGPD buscou seu arcabouço na lei da UE (RGPD), fazendo proposital uso de várias de suas premissas, o que permite a análise simultânea e comparativa dos ordenamentos brasileiro e europeu. A similaridade dos textos é proposital, já que o bloco econômico europeu é um forte parceiro comercial do Brasil e ter ordenamentos gêmeos facilita as negociações, pois a EU exige rigor na proteção de dados pessoais. Outros países,

à exemplo do Brasil, também redigiram suas leis de proteção de dados com base na RGPD.

Sendo assim, a LGPD – enquanto base legal mais completa sobre o tema, sendo um exponencial na legislação sobre proteção de dados – impactou todas as áreas da sociedade. Sua promulgação proporcionou uma maior estabilidade e segurança jurídica para os diversos ramos de negócios existentes, afetando, inclusive e de sobremaneira, as atividades notariais e registrais e modificando a operacionalização dos dados regulados pelos cartórios de protesto.

A promulgação, em 14 de agosto de 2018, da LGPD, originada do PL n. 53/2018, pelo então presidente Michel Temer, e a entrada em vigor, em todo território nacional, em 18 de setembro de 2020 foi um marco legal de grande impacto, tanto para as instituições privadas quanto para as públicas, pessoas jurídicas ou pessoas físicas. Foi imperativa a mudança no modelo de tratamento de dados pessoais.

Os cartórios são, por excelência e atribuição, repositórios de dados pessoais. As atividades notariais têm natureza jurídica com caráter híbrido, pois têm natureza pública, por um lado, e administração privada, por outro lado. Notários e registradores são agentes públicos delegados, ou seja, são agentes que exercem função pública em caráter privado, delegados pelo Poder Público. Os cartórios de protesto devem, no exercício de suas atividades, conceder publicidade ao inadimplemento de uma obrigação originada em títulos e outros documentos de dívida. Assim, é função dos cartórios de protesto dar publicidade ao descumprimento de obrigações, à inadimplência.

A promulgação da LGPD trouxe aos cartórios de protesto especial mudança, pois não se pode, de forma indiscriminada, publicar ou difundir os dados que deveriam ser tornados públicos. Por dever ético e legal, o tabelião deve guardar e operacionalizar suas atividades tendo como base a LGPD, observando os regramentos nela contidos e usando a publicidade de dados pessoais o mínimo necessários para a execução fim. A proteção de dados pessoais tem como fundamentos: o respeito à privacidade, à autodeterminação informativa, à liberdade de expressão, de informação, de comunicação e de opinião, à inviolabilidade da intimidade, da honra e da imagem e da proteção aos direitos humanos.

O Provimento n. 74, de 31 de julho de 2018, dispôs sobre os padrões mínimos de tecnologia da informação para a segurança, integridade e disponibilidade de dados

para a continuidade da atividade pelos serviços notariais e de registro do Brasil e o Provimento n. 134, de 24 de agosto de 2022, em seu Capítulo XV – Do protesto de títulos e outros documentos de dívida, estabelece medidas a serem adotadas pelas serventias extrajudiciais em âmbito nacional para o processo de adequação à LGPD.

É obrigação dos notários e registradores repensarem as atividades de armazenamento e tratamento dos dados coletados para que haja mais governança e monitoramento eficaz contínuo das informações pelas quais são responsáveis. Devem, caso ainda não tenham feito, iniciar a capacitação dos colaboradores, por meio de palestras, cursos e treinamentos. Deve ser realizado o mapeamento e redigido o relatório de impacto, além de alocar investimento em segurança da informação, impostos pelo provimento 74 do CNJ, para garantir controle efetivo do arquivo de dados gerados nos serviços do cartório.

Apesar das mudanças normativas e das dúvidas quanto à implementação da LGPD às atividades dos serviços extrajudiciais, é fundamental que a confiança habitual depositada nos serviços notariais e de registro, o que inclui os serviços de tabelionato de protesto de títulos, não seja abalada. Deve haver a adequação à nova legislação, caso contrário, haverá pena a ser imposta, sendo tão mais severa quanto o grau de desídia e incúria do administrador público, uma vez ciente da operação de tratamento potencialmente danosa e das medidas passíveis de conter ou mitigar os danos.

REFERÊNCIAS

ALMEIDA, S. do C. D. de; SOARES, T. A. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital **Perspectivas em Ciência da Informação**, v. 27, n. 3, p. 26-45, jul/set 2022.

AMARAL, F. **Introdução à ciência de dados**. Rio de Janeiro: Alta Books, 2016.

ARAÚJO, V. S.; GOMES, M. L. **Inteligência Artificial**. E aplicabilidade prática no Direito. Conselho Nacional de Justiça, 2022.

BARDIN, L. **Análise de conteúdo**. São Paulo: Edições 70, 2011.

BARROSO, L. R. **Curso de Direito Constitucional Contemporâneo**. 10. ed. São Paulo: Saraiva, 2022. E-book.

BASTOS, F. A. de; BASSI, M. C. P. C.; CASSI, G. H. G. Legítimo interesse como excludente de responsabilidade civil à luz da lei geral de proteção de dados. **Brazilian Journal of Development**, v. 7, n. 7, p. 71582-71607, 2021.

BIONI, B. R. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2019.

BOFF, S. O.; FORTES, V. B. A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil. **Seqüência** (Florianópolis), n. 68, p. 109-127, jun. 2014.

BORTALI, H. P. **Limites da atividade do provedor**: o gerenciamento de dados e a responsabilidade sobre conteúdo de terceiros. 2020. 134 f. Dissertação (Mestrado em Direito) - Programa de Estudos Pós-Graduados em Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2020.

BOTELHO, M. C. A proteção de dados pessoais enquanto direito fundamental: considerações sobre a Lei Geral de Proteção de Dados Pessoais. **Argumenta Journal Law**, n. 32 p. 191-207, jan./jun. 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 13 jun. 2021.

BRASIL. **Lei dos cartórios**. Lei Federal nº 8.935, de 18 de novembro de 1994. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8935.htm>. Acesso em: 10 jun. 2022.

BRASIL. **Lei n. 9.492**, de 10 de setembro de 1997. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9492.htm>. Acesso em: 28 fev. 2023.

BRASIL. **Código civil de 2002**. Lei Federal nº 10.406, de 10 de janeiro de 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/ L10406compilada.htm. Acesso em 20 jun. 2022.

BRASIL. **Lei de acesso à informação**. Lei Federal nº 12.527, de 18 de novembro de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 3 maio 2022.

BRASIL. **Lei geral de proteção de dados pessoais (LGPD)**. Lei Federal nº 13.709, de 14 de agosto de 2018. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei /l13709.htm. Acesso em 12 jan. 2022.

CÂMARA DOS DEPUTADOS. **Acesso à informação não pode ser prejudicado por conta de Lei de Proteção de Dados**, dizem especialistas. Agência Câmara de Notícias, publicado em 18/11/2021. Disponível em: <https://www.camara.leg.br/noticias/828370-acesso-a-informacao-nao-pode-ser-prejudicado-por-conta-de-lei-de- -protecao-de-dados-dizem-especialistas/>. Acesso em: 15 fev. 2023.

____. **Promulgada lei que transforma Autoridade Nacional de Proteção de Dados em autarquia**. Agência Câmara de Notícias, publicado em 26/10/2022. Disponível em: <https://www.camara.leg.br/noticias/915858-PROMULGADA-LEI-QUE-TRANSFORMA-AUTORIDADE-NACIONAL-DE-PROTECAO-DE-DADOS-EM-AUTARQUIA>. Acesso em 18 abr. 2023.

CARDOSO, O. V. **Introdução à Lei Geral de Proteção de Dados Pessoais**. E-book, 2020.

CARLOTO, S.; ALMIRÃO, M. **Lei geral de proteção de dados comentada**: com enfoque nas relações de trabalho. São Paulo: LTr, 2021.

CASTELLS, M. **A sociedade em rede**. A era da informação: economia, sociedade e cultura. São Paulo: Paz e Terra, 2011.

CONSELHO DA JUSTIÇA FEDERAL. Enunciado 531. Disponível em: < https://www.cjf.jus.br/enunciados/enunciado/142>. Acesso em 12 dez. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Provimento n. 74**, de 31 de julho de 2018. DJe/CNJ nº141/2018, de 01/08/2018, p. 44. Disponível em: < https://atos.cnj.jus.br/atos/detalhar/2637 >. Acesso em 25 jan. 2023.

CONSELHO NACIONAL DE JUSTIÇA. **Provimento n. 87**, de 11 de setembro de 2019. DJE/CNJ nº 191/2019, de 12/09/2019, p. 4. Disponível em: <https://atos.cnj.jus.br/files//provimento/provimento_87_11092019_12092019113253.pdf>. Acesso em: 28 fev. 2023.

CONSELHO NACIONAL DE JUSTIÇA. Provimento n. 100, de 26 de maio de 2020. DJE Edição nº 100/2020,de 26/05/2020, p. 2. Disponível em: <https://atos.cnj.jus.br/files/original222651202006025ed6d22b74c75.pdf>. Acesso em: 28 fev. 2023.

CONSELHO NACIONAL DE JUSTIÇA. **Provimento n. 134**, de 24 de agosto de 2022. DJe/CNJ nº 203/2022, de 24 de agosto de 2022, p. 18-25. Disponível em: < https://atos.cnj.jus.br/files/original141307202208256307837 3a0892.pdf >. Acesso em: 25 jan. 2023.

COMISSÃO EUROPEIA. **Comunicação da Comissão ao Parlamento Europeu e ao Conselho**: Intercâmbio e proteção de dados pessoais num mundo globalizado. Bruxelas: Bélgica. 2017.

COMISSÃO EUROPEIA. **Decisão de Execução** (UE) 2019/419. [S.l.]: [s.n.]. 2019.

COSTA, I.; DALLEDONE, R. Direito à privacidade X Direito à informação: novos aportes para o debate brasileiro. **Revista Jurídica da Escola Superior do Ministério Público de São Paulo**, v. 18, n. 2, 2020, p. 131-145.

CRESWELL, J. W.; CRESWELL, J. D. **Projeto de pesquisa**: métodos qualitativo, quantitativo e misto. 5. ed. Porto Alegre: Artmed, 2021.

CURY, P. M. N. **Métodos de Direito Comparado**: desenvolvimento ao longo do século XX e perspectivas contemporâneas. Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD). UNISINOS. Julho-setembro/2014, p. 176-185.

DA SILVA, S. de A. A. et al. Herança da informação digital e direito ao esquecimento em redes sociais on-line: uma revisão sistemática de literatura. **Em Questão**, Porto Alegre, v. 26, n. 1, p. 375-401, jan/abr. 2020.

DIÁRIO OFICIAL. PORTARIA ANPD n. 35, de 4 de novembro de 2022. **Torna pública a Agenda Regulatória para o biênio 2023-2024**. 2022. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885>. Acesso em: 27 fev. 2023.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Revista Espaço Jurídico Journal of Law**. Joaçaba/SC, vol. 1, n. 2, p. 91-108, jul/dez.

2011.

EDUCACAO, S. **Lei Geral de Proteção de Dados (LGPD) e Marco Civil da Internet.** São Paulo: Saraiva, 2022. E-book.

ESQUÁRCIO, A. T; ESQUARCIO, D. T. **Reflexão sobre a Lei Geral de Proteção de Dados Pessoais na atual sociedade informatizada e virtualizada**. In: Estado, Governança, Democracia e Virtualidades [Recurso eletrônico on-line] organização XI Congresso RECAJ/UFMG: UFMG – Belo Horizonte, 2020, p. 14-20

FUJITA, J.; MATHEUS, R. Atividade notarial frente às transformações de uma sociedade digitalizada: fé pública na sociedade da informação. **Argumenta Journal Law**, n. 35, 2021, p. 478-501.

GARCIA, L. R. **Lei Geral de Proteção de Dados Pessoais (LGPD)**: guia de implantação. São Paulo: Blucher, 2020.

GÓIS, J. A. de O. **A intimidade e a vida privada em face de biografias não autorizadas**. Avanços da esfera pública sobre a esfera privada. e-Book: Dialética, 2020.

GONÇALVES, T. C. N. M.; VARELLA, M. D. Os desafios da Administração Pública na disponibilização de dados sensíveis. **Revista Direito FGV**. São Paulo, v. 14, n. 2, p. 513-536, maio/ago. 2018.

GONÇALVES, C. R.; LENZA, P. **Direito Civil Esquematizado®**. 12. ed. São Paulo: Saraiva, 2022. E-book.

GREENLEAF, G. **Asian Data Privacy Laws**: Trade & Human Rights Perspectives. Oxford: Oxford University Press, 2014. E-book/Kindle Edition.

GRESSLER, I.C.; BACHINSKI, F. L.; SILVA, R. L. **A divulgação indevida de informações pessoais em site de universidade gaúcha**: resposta jurisdicional entre a óptica constitucional e os princípios da lei n. 13.709/2018. X Congresso Internacional de Direito e Contemporaneidade: mídia e direitos da sociedade em rede. UFSM, 2019.

GUERRA, E.; CARLOTO, S. **Manual prático de adequação à LGPD**: com enfoque nas relações de trabalho. São Paulo: Ltr, 2021.

HARARI, Y. N. **SAPIENS** – Uma Breve História da Humanidade. L&PM, 2017.

HOFFMANN, W. A. M. **Gestão do conhecimento**: desafios de aprender. São Carlos: Compacta, 2009.

HOUNSLOW, D. **Japan - Data Protection Overview**. OneTrust – Data Guidance, 2021. Disponível em: <https://www.dataguidance.com/notes/japan-data-protection-overview. Acesso em: 13 de nov. de 2022.

INSTITUTO DE PROTESTO – IEPTB-BR. **O que é e para que serve um cartório de protestos**. 2020. Disponível em: <https://blog.protestodedivida.org.br/o-que-e-e-para-que-serve-um-cartorio-de-protestos/>. Acesso em: 27 fev. 2023.

INSTITUTO DE PROTESTO – IEPTB-SP. **LGPD Lei Geral de Proteção de Dados**. Cartório de Protesto de São Paulo. 2021. Disponível em: < https://www.anoreg.org.br/site/wp-content/uploads/2021/10/LGPD_-_Cartilha_-_IEPTB-SP_1.pdf >. Acesso em 10 dez. 2022.

INSTITUTO DE PROTESTO – IEPTB-BR. **Política de privacidade e cookies**. Versão 1.0. 2022. Programa de governança em privacidade e proteção de dados pessoais. Disponível em: <https://www.protestodetitulos.org.br/arquivos/politica-privacidade.pdf>. Acesso em 10 dez. 2022.

IRAMINA, A. RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 12, n. 2, p. 91-117, outubro de 2020.

KEINERT, T. M. M.; CORTIZO, C. T. Dimensões da privacidade das informações em saúde. **Cad. Saúde Pública**, v. 34, n. 7, p. e00039417, 2018.

KITCHIN, R. **The data Revolution**: big data, open data, data infrastructure & their consequences. Thousand Oaks: Sage Publications, 2014.

LAUREANO, J. C.; BENFATTI, F. F. N. A Lei Geral de Proteção de Dados Pessoais e os impactos nos serviços notariais e registrais brasileiros: uma análise a partir da proteção de valores e princípios constitucionais. **Revista Brasileira de Direitos e Garantias Fundamentais**, v. 7, n. 2, p. 88-106, jul./dez. 2021.

LEONARDI, M. **Fundamentos de Direito Digital**. São Paulo: Editora Revista dos Tribunais, 2019.

LIMA, A. C. D. et al. **LGPD e Cartórios: implementação e questões práticas**. São Paulo: Saraiva, 2021. E-book.

LIMA, C. C. C. **Capítulo II – Do Tratamento de Dados Pessoais**. In: MALDONADO, V. N.; BLUM, R. O. LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico] / coordenadores. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020, p. 201-241.

LIMA, A.; SAMANIEGO, D.; BARONOVSKY, T. (org.) **LGPD para contratos**. Adequando contratos e documentos à Lei Geral de Proteção de Dados. São Paulo: Expressa, Saraiva Educação S. A., 2022.

MALHOTRA, N. K. **Pesquisa de marketing**: uma orientação aplicada. 6. ed. Porto Alegre: Bookman, 2012.

MARMELSTEIN, George. **Controle Judicial dos Direitos Fundamentais**. Currículo Permanente – Caderno de Direito Constitucional – TRF 4ª Região, Porto Alegre, mod. 5, p. 59, 2008.

MARQUES, A. V. C. de C. **A relação entre a lei brasileira 13.709/18 e o arcabouço jurídico para proteção de dados pessoais do Japão e da Coreia do Sul a partir do modelo TLICS**. 2021. Monografia Final de Curso, Faculdade de Direito, Universidade de Brasília, Brasília/DF, 129 p.

MARTINS, G. D. A.; THEÓFILO, C. R. **Metodologia da Investigação Científica para Ciências Sociais**. 2. ed. São Paulo: Atlas, 2009.

MAYER-SCHÖNBERGER, V.; CUKIER, K. **Big data**: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Rio de Janeiro: Elsevier, 2013.

MENDES, G. F. **Curso de direito constitucional**. 13. ed., São Paulo: Saraiva, 2018.

MENDES, L. S. **A Lei Geral de Proteção de Dados Pessoais**. In: SOUZA, C. A. (coord). Lei Geral de Proteção de Dados – Caderno Especial. São Paulo: Revista dos Tribunais, n. 1, 2019.

MICHELETTI, M.; BORGES, T. T. **LGPD**. O abismo entre a teoria e a prática. Lei comentada. Paulínia, SP: Ed. Do Autor, 2021.

MIYASHITA, H. **The Evolving Concept of Data Privacy in Japanese Law**. Oxford: Oxford University Press, International Data Privacy Law, v. 1, n. 4, 2011.

MIRANDA, J. **Manual de direito constitucional**: Tomo IV. 4. ed. Coimbra: Coimbra Editora, 1990.

MORAES, A. de. **Direito constitucional**. São Paulo: Atlas, 2002.

MONTEIRO, C. V. A. Direito à privacidade versus direito à informação. Considerações sobre a possibilidade de órgãos públicos fornecerem a terceiros informações pessoais de agentes públicos. **Revista de Informação Legislativa**, Brasília, a. 44, n. 173, jan./mar. 2007, p. 27-40.

MOZZATO, A. R.; GRZYBOVSKI. Análise de conteúdo como técnica de análise de dados qualitativos no campo da Administração: Potencial e Desafios. **RAC**, Curitiba, v. 15, n. 4, p. 731-747, jul./ago. 2011. MULHOLLAND, C. **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020.

MULHOLLAND, C. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado**. São Paulo, n. 144, nov. 2019.

____. **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020.

NASCIMENTO, H. J. C. A. do. **Políticas públicas para preservação digital**: um panorama das inter-relações conceituais da legislação brasileira. 2021. 150 f. Dissertação (Mestrado em Ciência da Informação) – Universidade Federal de Pernambuco. Recife, 2021.

ORTIZ, E. **O que é birô de crédito e como esse tipo de empresa funciona**. Disponível em: https://www.serasa.com.br/score/blog/o-que-e-biro-de-credito-e-como-esse-tipo-de-empresa-funciona/. Acesso em: 08 maio 2023.

PATEL, N. K. et al. **The American Data Privacy and Protection Act: Is Federal Regulation of AI Finally on the Horizon?** Perspectives & Events. oct. 2022.

PINHEIRO, P. P. **Proteção de Dados Pessoais**. 3. ed. São Paulo: Saraiva Educação, 2021.

REPORT nº 117-669. **RH 8152**. Disponível em: <https://www.congress.gov/bill/117th-congress/house-bill/8152/text#toc-H0299B60817D742978DC3C447CD110A88>. Acesso em 03 jan. 2023.

ROCHA, W. L. Tratamento de dados pessoais pelo poder público: uma análise da aplicação da LGPD no registro empresarial. **Revista Brasileira de Catalogação na Publicação**. Rio de Janeiro, jan. jun. 2020, p. 191-224.

RODOTÀ, S. **A vida na sociedade da vigilância** – a privacidade hoje. Rio de Janeiro: Renovar, 2009.

RUSSO, R. A. **A tutela da privacidade de dados na era do *Big Data***. 2019. 136 f. (Mestrado em Direito) – Pontifícia Universidade Católica, São Paulo, 2019.

SARLET, I. W. et al. **Curso de direito constitucional**. 8. ed. São Paulo: Saraiva. 2019.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada**: uma visão jurídica da sexualidade da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998.

SCHREIBER, A. **Direito da personalidade**. São Paulo: Atlas, 2013.

SERPRO. Serviço Federal de Processamento de Dados. **Lei que cria a ANPD é sancionada com vetos**. 2019. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/lei-que-cria-a-autoridade-nacional-de-protecao-de-dados-e-sancionada-com-vetos>. Acesso em: 27/02/2023.

____. **A empresa**. 2022. Disponível em: <https://www.serpro.gov.br/menu/institucional/quem-somos>. Acesso em: 10 dez. 2022a.

____. **Mapa da proteção de dados**. 2022. Disponível em: <https://www.serpro.gov.br/lgpd/menu/a-lgpd/mapa-da-protecao-de-dados-pessoais>. Acesso em: 10 dez. 2022b.

____. **Como as empresas devem tratar os dados pessoais sensíveis e não sensíveis?** 2023. Disponível em: <https://www.serpro.gov.br/menu/noticias/noticias-2023/dados-pessoais-sensiveis-e-nao-sensiveis>. Acesso em: 20 jan. 2023.

SILVA, J. A. da. **Curso de direito constitucional positivo**. 39. ed., São Paulo: Malheiros, 2016.

SOLER, F. G. **Proteção de Dados**: Reflexões Práticas e Rápidas Sobre a LGPD. São Paulo: Saraiva, 2021. E-book.

SOU, E. P. R. D. **Série Direito Registral e Notarial** - Noções Fundamentais de Direito Registral e Notarial. 3. ed. São Paulo: Saraiva, 2022. E-book.

TASSO, F. A. Capítulo IV – Do Tratamento de Dados Pessoais pelo Poder Público. In: MALDONADO, V. N.; BLUM, R. O. LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico] / coordenadores. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020, p. 275-325.

TAVARES, A. R. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2002.

TEIXEIRA, T.; GUERREIRO, R. M. **Lei Geral de Proteção de Dados Pessoais**: comentada artigo por artigo. 4. Ed. São Paulo: SaraivaJur, 2022.

VENOSA, S. de S. **Direito Civil**. Parte Geral. 13. ed. São Paulo: Atlas, 2013.

VERGARA, S. **Projetos e relatórios de pesquisa em administração.** 10. ed. São Paulo: Atlas, 2009.

WACHOWICZ, M. (org). **Proteção de dados pessoais em perspectiva**: LGPD e RGPD na ótica do direito comparado. Curitiba, PR: Gedai, 2020.

YUN, R. (coord.). **LGPD Acadêmico Comparativo**. Disponível em: <https://observatoriolgpd.com/wp-content/uploads/2020/02/Comparativo-17022020.pdf.pdf.pdf >. Acesso em: 10 jan. 2022.

ANEXOS

ANEXO 1

PORTARIA ANPD Nº 35, DE 4 DE NOVEMBRO DE 2022

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 08/11/2022 | Edição: 211 | Seção: 1 | Página: 6

Órgão: Presidência da República/Autoridade Nacional de Proteção de Dados

PORTARIA ANPD Nº 35, DE 4 DE NOVEMBRO DE 2022

Torna pública a Agenda Regulatória para o biênio 2023-2024.

O DIRETOR-PRESIDENTE DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, no exercício das atribuições que lhe confere o art. 3º, §2º, do Decreto nº 10.474, de 2020,

CONSIDERANDO que a Agenda Regulatória é um instrumento de planejamento que agrega as ações regulatórias consideradas prioritárias e que serão objeto de estudo ou tratamento pela Autoridade durante sua vigência;

CONSIDERANDO a deliberação tomada pelo Conselho-Diretor no Circuito Deliberativo nº 10/2022; e

CONSIDERANDO o constante dos autos do processo nº 00261.001286/2022- 93, resolve:

Art. 1º Tornar pública a Agenda Regulatória da Autoridade Nacional de Proteção de Dados - ANPD para o biênio 2023-2024, na forma do Anexo a esta Portaria.

Art. 2º As iniciativas da Agenda Regulatória para o biênio 2023-2024 são classificadas em fases, por ordem de priorização:

I - Fase 1 - itens cujo processo regulatório foi iniciado durante a vigência da Agenda Regulatória para o biênio 2021-2022, aprovada pela Portaria nº 11, de 27 de janeiro de 2021;

II - Fase 2 - itens cujo início do processo regulatório acontecerá em até 1 ano;

III - Fase 3 - itens cujo início do processo regulatório acontecerá em até 1 ano e 6 meses;

IV - Fase 4 - itens cujo início do processo regulatório acontecerá em até 2 anos.

Parágrafo Único: As iniciativas a que se refere o inciso I do caput deste artigo terão prevalência sobre os demais itens constantes da Agenda Regulatória.

Art. 3º A ANPD deverá considerar como prioritários os temas constantes da Agenda Regulatória para o biênio 2023-2024 quando do planejamento e da execução de ações educativas.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

WALDEMAR GONÇALVES ORTUNHO JUNIOR

ANEXO I

AGENDA REGULATÓRIA - 2023-2024

Item	Iniciativa	Descrição	Priorização
1	Regulamento de Dosimetria e Aplicação de Sanções Administrativas	A LGPD determina que a ANPD definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, as metodologias que orientarão o cálculo do valor-base das sanções de multa e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos na lei.	Fase 1
2	Direitos dos titulares de dados pessoais	A LGPD estabelece os direitos dos titulares de dados pessoais, mas diversos pontos merecem regulamentação, que tratará desses direitos, incluindo, mas não limitado aos artigos 9º, 18, 20 e 23.	Fase 1

3	Comunicação de incidentes e especificação do prazo de notificação	De acordo com o art. 48 da LGPD, o controlador deverá comunicar à Autoridade Nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações.	Fase 1
4	Transferência Internacional de Dados Pessoais	O art. 33, inciso I da LGPD, prevê que a transferência internacional de dados pessoais somente é permitida para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na referida lei. Por sua vez, o art. 34 explica que o nível de proteção de dados do país estrangeiro ou do organismo internacional poderá ser avaliado pela ANPD. O art. 35 da lei determina, ainda, que a definição do conteúdo de cláusulas-padrão contratuais, dentre outros, será realizada pela ANPD. Assim, é necessário regulamentar os arts. 33, 34 e 35 da LGPD, sem prejuízo dos demais temas tratados pelos artigos não mencionados neste texto.	Fase 1
5	Relatório de Impacto à Proteção de Dados Pessoais	De acordo com as competências estabelecidas pelo art. 55-J, inciso XIII, cabe a ANPD editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais.	Fase 1
6	Encarregado de proteção de dados pessoais	Nos termos do art. 41, § 3º da LGPD, a ANPD pode estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.	Fase 1
7	Hipóteses legais de tratamento de dados pessoais	Documento orientando o público sobre as bases e hipóteses legais de aplicação da LGPD sobre diversos temas, incluindo as hipóteses legais descritas no art. 7º mas não restritas a ele.	Fase 1
8	Definição de alto risco e larga escala	Obrigação legal disposta no § 3º do art. 4º do Regulamento de aplicação da Lei 13.709, de 14 de agosto de 2014, Lei Geral de Proteção de Dados Pessoais (LGPD) para agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, dispôs sobre os critérios para definição do tratamento de alto risco ao titular de dados.	Fase 1
9	Dados Pessoais Sensíveis - Organizações religiosas	Documento com finalidade de disseminar as medidas básicas para adequação ao disposto na LGPD pelas organizações religiosas.	Fase 1
10	Uso de dados pessoais para fins acadêmicos e para a realização de estudos por órgão de pesquisa	Documento com finalidade de fornecer aos agentes de tratamento recomendações e orientações que possam incentivar a adoção de boas práticas e respaldar o tratamento de dados pessoais realizado para fins acadêmicos e de estudos e pesquisas de forma compatível com a LGPD.	Fase 1
11	Anonimização e pseudonimização	Documento com objetivo de orientar e esclarecer a utilização das técnicas de anonimização e de pseudonimização previstos na LGPD.	Fase 1
12	Regulamentação do disposto no art. 62 da LGPD	O art. 62 da LGPD determina a edição de regulamento específico pela ANPD para acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004.	Fase 1
13	Compartilhamento de dados pelo Poder Público	O capítulo IV da LGPD dispõe sobre o tratamento de dados pessoais pelo Poder Público. A lei determina que a ANPD disponha sobre as formas de publicidade das operações de tratamento, bem como que contratos e convênios estabelecidos entre o Poder Público e entidades privadas que tenham acesso a dados pessoais constantes de bases de dados deverão ser comunicadas à ANPD. Estudo objetiva a operacionalização dos art. 26 e 27 da LGPD, que tratam do compartilhamento de dados do Poder Público com pessoa de direito privado, especialmente quanto aos procedimentos a serem adotados e às informações que devem ser encaminhadas à ANPD para cumprimento do disposto na Lei.	Fase 2

14	Tratamento de dados pessoais de crianças e adolescentes	A ANPD elaborou Estudo Preliminar sobre o tema, o qual teve por objetivo analisar as possíveis hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes. No entanto, o estudo não teve pretensão de ser exaustivo, em razão de limitações de escopo e de tempo, que buscou promover a discussão pública e coletar contribuições da sociedade, a fim de, em um momento posterior, estabelecer interpretações e orientações mais conclusivas. Cumpre enfatizar que não foram consideradas as possíveis técnicas para aferição do consentimento ou para a aferição de idade de usuários de aplicações de internet. Além disso, observa-se necessidade de analisar os impactos de plataformas e jogos digitais na Internet na proteção de dados de crianças e de adolescentes. Embora relevantes para o tratamento de dados pessoais de crianças e adolescentes, a discussão sobre esses temas correlatos demanda uma abordagem mais ampla, levando em consideração outros contextos e aspectos técnicos e jurídicos.	Fase 2
15	Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade	Em atenção a determinação legal disposta no art. 55-J, III, da LGPD, para elaboração de Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, a iniciativa faz-se necessária para direcionar a atuação de todos os atores envolvidos no ecossistema de proteção de dados, inclusive a ANPD. A Política deve considerar as demais políticas públicas publicadas, como por exemplo, Estratégia Digital, Plano Nacional de IoT, dentre outros.	Fase 2
16	Regulamentação de critérios para reconhecimento e divulgação de regras de boas práticas e de governança	O art. 50 da LGPD dispõe que os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. Ao estabelecer regras de boas práticas, o controlador e o operador deverão considerar, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular. A LGPD determina que as regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela Autoridade Nacional.	Fase 2
17	Dados Pessoais Sensíveis - Dados biométricos	A coleta da biometria é de fundamental importância para se evitar fraudes e uma salvaguarda relevante para a segurança do titular. A despeito da importância do assunto, a LGPD não supriu integralmente a necessidade de disciplina do tema. Neste sentido, torna-se necessária a intervenção da ANPD, seja mediante regulamentação ou documentos de caráter orientativo sobre os contextos nos quais a coleta de dados sensíveis seria legítima.	Fase 3
18	Medidas de segurança, técnicas e administrativas (incluindo padrões técnicos mínimos de segurança)	Nos termos do art. 46 da 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. O § 1º do referido artigo estabelece que a ANPD poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no citado dispositivo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos na lei.	Fase 3
19	Inteligência artificial	Para além da determinação legal de regulamentar o disposto na LGPD, em especial o disposto no art. 20 da Lei, que trata do direito do titular de solicitar revisão de decisões automatizadas, a ANPD pode endereçar melhor o tema por meio de documentos orientativos, como guias e estudos técnicos, uma vez que o assunto está sendo bastante utilizado pelos agentes de tratamento, frente à vulnerabilidade do titular que não possui conhecimento avançado sobre o tema. Torna-se fundamental que a ANPD estude e acompanhe o tema sob a perspectiva da proteção de dados pessoais e, em particular, da aplicação da LGPD. Tais diretrizes servirão de base para o desenvolvimento de outras regras que venham a ser necessárias para a disciplina de sistema de IA.	Fase 3

20	Termo de Ajustamento de Conduta - TAC	Em atenção ao disposto no art. 55-J, XVII da LGPD e no art. 44 da Resolução CD/ANPD Nº 1, de 28 de outubro de 2021, o Termo de Ajustamento de Conduta - TAC é instrumento que compõe o Processo de Fiscalização e o Processo Administrativo Sancionador da ANPD, possibilitando ao agente interessado a apresentação de proposta de acordo como alternativa ao regular andamento do processo sancionador.	Fase 4