PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

MONOGRAFIA JURÍDICA

A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E O DIREITO À PRIVACIDADE

ORIENTANDO: GABRIEL FUCCIOLO DE OLIVEIRA BRANDAO

ORIENTADORA: PROFª. MS. GABRIELA PUGLIESI FURTADO CALAÇA

GOIÂNIA-GO
2022

GABRIEL FUCCIOLO DE OLIVEIRA BRANDAO

A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E O DIREITO À PRIVACIDADE

Monografia Jurídica apresentada à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Prof. (a) Orientadora: Ms. Gabriela Pugliesi Furtado Calaça.

GOIÂNIA-GO
2022

LISTA DE SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
BACEN	Banco Central do Brasil
CVM	Comissão de Valores Mobiliários
GDPR	Regulamento Geral de Proteção de Dados
GPS	Sistema de Posicionamento Global
LGPD	Lei Geral de Proteção de Dados Pessoais
MP	Ministério Público
PROCON	Programa de Proteção e Defesa do Consumidor

RESUMO

A Lei Geral de Proteção de Dados Pessoais (LGPD) é um marco para a legislação brasileira. Publicada em 15 de agosto de 2018, a legislação entrou em vigor apenas em 18 de setembro de 2020, diante de uma série de adiamentos – o último devido à pandemia do novo Coronavírus. Por isso também, as sanções administrativas previstas pela LGPD só foram aplicadas a partir de agosto de 2021. O presente estudo tem como objetivo geral analisar a nova Lei Geral de Proteção de Dados (LGPD) e o direito à privacidade. Para que os objetivos mencionados sejam atingidos, utilizou-se como recurso metodológico, a pesquisa bibliográfica, executada a partir de uma análise minuciosa de materiais publicados na literatura, além de artigos científicos divulgados no meio eletrônico. Assim, conclui-se que lidar com as questões de privacidade é uma obrigação hoje em dia, porque as violações de privacidade podem resultar em consequências graves. Vários estudos lançaram luz sobre os custos de economia das violações de privacidade, deixando claro que a ausência de mecanismos de proteção de privacidade impõe enormes custos às associações, bem como custos indiretos e consequências de longo prazo. O LGPD surgiu como uma forma de facilitar o tratamento de dados com base em princípios de ética e boa fé; e suas diretrizes visam atuar em prol da segurança e privacidade dos dados dos usuários, levantando dúvidas e direcionando soluções para que associações brasileiras, públicas e/ou privadas, a implementem durante a coleta e manipulação dos dados.

Palavras-chave: Dados pessoais. GDPR. LGPD. Privacidade. Tratamento de dados.

ABSTRACT

The General Personal Data Protection Law (LGPD) is a landmark for Brazilian legislation. Published on August 15, 2018, the legislation came into force only on September 18, 2020, in the face of a series of postponements – the last one due to the new Coronavirus pandemic. For this reason, the administrative sanctions provided for by the LGPD were only applied from August 2021. The present study has the general objective of analyzing the new General Data Protection Law (LGPD) and the right to privacy. In order for the aforementioned objectives to be achieved, the bibliographic research was used as a methodological resource, carried out from a thorough analysis of materials published in the literature, in addition to scientific articles published in the electronic medium. Thus, it is concluded that dealing with privacy issues is a must nowadays because privacy violations can result in serious consequences. Several studies have shed light on the cost savings of privacy breaches, making it clear that the absence of privacy protection mechanisms imposes huge costs on associations, as well as indirect costs and long-term consequences. The LGPD emerged as a way to facilitate the processing of data based on principles of ethics and good faith; and its guidelines aim to act in favor of the security and privacy of users' data, raising doubts and directing solutions for Brazilian public and/or private associations to implement it during data collection and manipulation.

Keywords: Personal data. GPDP. GDPR. Privacy. Data processing.

SUMÁRIO

INTRODUÇÃO..... 06

1 LEI GERAL DE PROTEÇÃO DE DADOS DO BRASIL (LGPD)..... 08

1.1 ASPECTOS GERAIS DO LGPD..... 08

1.2 ÂMBITO DE APLICAÇÃO..... 09

1.3 PROTEÇÃO DE DADOS..... 10

1.4 BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS..... 13

1.4.1 Consentimento..... 14

1.4.2 Casos particulares..... 15

1.4.3 Interesse legítimo..... 16

2 DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS..... 18

2.1 RESPONSABILIDADES PARA AGENTES DE PROCESSAMENTO DE DADOS..... 18

2.1.1 Cumprimento de obrigações estatutárias ou regulamentares..... 19

2.1.2 Execução de um contrato ou procedimentos preliminares..... 20

2.1.3 Exercício regular de direitos em procedimentos..... 21

2.1.4 Proteção de crédito..... 21

2.1.5 Proteção da vida ou da segurança física..... 22

2.1.6 Proteção da saúde..... 23

2.1.7 Realização de estudos por entidades de pesquisa..... 24

2.1.8 Execução de políticas públicas..... 24

2.1.9 Particularidades dos dados pessoais sensíveis..... 25

2.2 TRANSFERÊNCIA DE DADOS INTERNACIONAIS..... 26

2.3 COMENTÁRIOS SOBRE A EFICÁCIA DA LGPD..... 30

CONCLUSÃO..... 32

REFERÊNCIAS..... 33

INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD) é um marco para a legislação brasileira. Publicada em 15 de agosto de 2018, a legislação entrou em vigor apenas em 18 de setembro de 2020, diante de uma série de adiamentos – o último devido à pandemia do novo Coronavírus. Por esse motivo, as sanções administrativas, também previstas pela LGPD só foram aplicadas a partir de agosto de 2021.

Com a LGPD, a proteção de dados pessoais no Brasil passa a contar com legislação específica, que confere segurança jurídica aos titulares de dados e agentes de processamento, sejam do setor privado ou do governo.

E, claro, a segurança jurídica é essencial para se ter um ambiente favorável ao desenvolvimento econômico, uma vez que o país adota as melhores práticas internacionais em matéria de proteção de dados. Vale ressaltar que o direito fundamental à privacidade, previsto no artigo quinto, inciso X, da Constituição Federal, é fortalecido com a LGPD.

A publicação da LGPD no Diário Oficial da União ocorreu no mesmo ano em que entrou em vigor o Regulamento Geral de Proteção de Dados (GDPR), o regulamento europeu de proteção de dados, considerado referência mundial. Mas essa não é a única característica compartilhada por essas legislações. Muito mais do que isso, pois a LGPD foi de fato inspirada no GDPR, com fundamentos, princípios e disposições em comum.

Em uma economia digital como a de hoje, com uso massivo de dados por empresas e governo, os direitos dos titulares devem ser protegidos, com regras claras que possibilitem o desenvolvimento econômico sem prejuízo à privacidade dos cidadãos.

Para que a LGPD exerça sua função, a Autoridade Nacional de Proteção de Dados (ANPD) deve estar em pleno funcionamento. No final de agosto deste ano, o Decreto 10.474/2020 estruturou a ANPD, órgão vinculado à Presidência da República com funções de regulação, fiscalização e sanção.

O trabalho da ANPD deve priorizar o engajamento construtivo com o setor privado por meio do diálogo, apoio, cooperação mútua, orientação, conscientização e informação. As sanções administrativas previstas na LGPD, que só poderão ser aplicadas a partir de agosto do próximo ano, serão a última opção – somente nos

casos de infração dolosa ou práticas exponencialmente negligentes, reiteradas ou gravíssimas.

Ressalta-se, no entanto, que embora as sanções administrativas previstas na LGPD tenham sido postergadas, as empresas têm o dever de notificar em caso de incidente envolvendo dados pessoais. Isso porque órgãos setoriais e o próprio Poder Judiciário poderão fundamentar seus atos com base na LGPD para aplicar medidas administrativas e condenações por responsabilidade civil.

O presente estudo tem como objetivo geral analisar a nova Lei Geral de Proteção de Dados (LGPD) e o direito à privacidade. Como objetivos específicos conhecer os aspectos gerais da LGPD, bem como o direito à privacidade e à proteção de dados. Em um primeiro momento, este trabalho abordará a legislação vigente, Lei nº 13.709/2018, fazendo uma análise didática e empírica por meio da qual esta Lei define sua forma de atuação. Em um segundo momento, será apresentado como ambas as leis interagem entre si devido à recente edição da LGPD, e como a doutrina analisa essa situação recente.

Para que os objetivos mencionados sejam atingidos, utilizou-se como recurso metodológico, a pesquisa bibliográfica, executada a partir de uma análise minuciosa de materiais publicados na literatura, além de artigos científicos divulgados no meio eletrônico.

1 LEI GERAL DE PROTEÇÃO DE DADOS DO BRASIL (LGPD)

Neste capítulo será elaborado o contexto histórico referente à legislação de proteção de dados pessoais e sensíveis desde a instituição dos cadastros organizacionais e do uso deles até a criação da LGPD.

1.1 ASPECTOS GERAIS DA LGPD

Tendo em vista a utilização indiscriminada de dados pessoais por parte das associações, muitos países identificaram a necessidade de implementar uma legislação específica para proteger os dados pessoais dos cidadãos. A Lei nº 13.709 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), porém, entrou em vigor em 14 de agosto de 2020, após alguns movimentos do governo que não conseguiram estender seu prazo (BRASIL, 2018).

Segundo Fernandez (2020), sua estrutura e conteúdo refletidos são o reflexo de uma legislação brasileira inspirada nas diretrizes internacionais, uma vez que 120 países já possuíam uma religião sobre o assunto, especialmente nas previsões no Regulamento Geral de Proteção de Dados da União Europeia (GDPR).

O objetivo da LGPD é proteger os direitos da personalidade, regulamentar o tratamento de dados pessoais por pessoas físicas ou jurídicas, a fim de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa física consagrados na Constituição Brasileira (BRASIL, 2018).

O LGPD entrou em vigor em 2020, durante a pandemia do Covid-19 e após uma corrida legislativa. No final de 2020, foi encontrada a entidade reguladora e publicada a sua agenda regulatória, especificando os temas para discussão e as datas em que cada um seria tratado. Levando em consideração o contexto de eficácia da LGPD e com as empresas apressadas em que adequar aos dispositivos da Lei, a Autoridade Nacional de Proteção de Dados (ANPD) tomou forma e está atuando de forma efetiva e com um primeiro plano de conscientização e educação.

Em suma, é possível dizer que a LGPD brasileira visa harmonizar o direito fundamental à proteção da privacidade e da intimidade com o interesse público e o uso e desenvolvimento de tecnologia aplicada à era da informação. Antes da LGPD ser promulgada, o direito à privacidade e intimidade já estava garantido pela

Constituição Federal Brasileira, que estabelecia claramente que tais direitos prevalecer sobre quaisquer interesses públicos, ao estabelecer restrições ao acesso a determinadas informações pessoais, tais como, mas não se limitando a, informações financeiras, correspondências, conversas telefônicas (art. 5º, X, XII). Além disso, uma Constituição Federal protege a intimidade e a privacidade, ainda que indiretamente (MACIEL, 2019).

No entanto, a promulgação da LGPD foi necessária para conferir mais segurança jurídica aos dados pessoais, enquanto expressão informativa da privacidade e intimidade das pessoas, e para regulamentar especificamente como ações relativas ao seu tratamento, atribuindo responsabilidades aos assuntos abrangidos por desde a coleta ao colégio e utilização dos dados, com base nos princípios da adequação, transparência e não discriminação. Tudo isso devido à ampla divulgação de informações, principalmente por meios digitais, bem como à tendência crescente de furto de dados, cada vez mais facilitado pelo aprimoramento da tecnologia, e utilização desses dados para fins ilícitos.

1.2 ÂMBITO DE APLICAÇÃO

No que diz respeito à aplicabilidade e extensão da LGPD, ela será aplicável e exequível no que diz respeito ao tratamento de dados realizados no Brasil, relativos à oferta de bens e serviços a pessoas físicas ou jurídicas, de direito público ou privado, no território brasileiro, caso: (i) o processamento tem por requerimento de oferta de bens ou serviços; (ii) os dados pessoais processados são de pessoas físicas que estão obrigatórias em território brasileiro; ou (iii) os dados pessoais processados foram coletados em território brasileiro. A este respeito, é perceptível que os termos de aplicação da lei se aproximam, de facto, dos resultados no GDPR (PINHEIRO, 2018).

A LGPD não é aplicável, porém, nos casos em que o tratamento de dados pessoais seja feito: (i) por uma pessoa física para fins privados exclusivamente e não econômica; (ii) exclusivamente para fins jornalísticos, artísticos e acadêmicos; (iii) pelo Poder Público, nas hipóteses de utilização para a promoção da segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; ou (iv) quando os dados têm origem fora do território nacional e não são objeto de comunicação, uso comum de dados com agentes de

processamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de origem (desde que visto que o país de origem oferece um nível de proteção de dados pessoais adequado ao estabelecido no LGPD). (BRASIL, 2018).

Observa-se que os dados anônimos não são considerados dados pessoais protegidos pela LGPD, e devem ser entendidos como dados que pertencem a pessoas não identificáveis, ou seja, dados combinados titulares dos dados não podem ser identificados.

1.3 PROTEÇÃO DE DADOS

Para efeitos da LGPD, ‘dados pessoais’ são as informações relacionadas com uma pessoa singular identificada ou identificável. Dentro deste conjunto, os ‘dados pessoais específicos’, por sua vez, determinada uma categoria específica de dados pessoais que ampliação um maior grau de proteção jurídica face ao potencial discriminatório que pode advir do seu tratamento.

Esta categoria é composta por dados pessoais de origem racial ou étnica, religião religiosa, opinião pública, filiação a sindicato ou organização religiosa, filosófica ou política, dados relativos à saúde ou vida sexual e dados genéticos ou biométricos, quando relacionado com uma pessoa singular. Neste cenário, enquanto dados pessoais são aqueles que podem identificar ou levar à identificação de alguém, os dados identificados, além de identificarem um indivíduo, é capaz de promover a discriminação contra ele. Observa-se que o processamento de dados pessoais que revelam dados confidenciais também está sujeito a proteção especial nos termos da lei (COTS, 2018).

No que se refere às obrigações de proteção de dados, destaca-se que a lei diferenciadora e classifica os assuntos por ela abrangidos, de acordo com suas responsabilidades e deveres. Dentre os assuntos expressamente contemplados em lei, além dos titulares dos dados, tem-se: agentes de processamento, responsáveis, Autoridade Nacional de Proteção de Dados e órgãos de pesquisa (PINHEIRO, 2018). Os agentes de tratamento são as pessoas singulares ou coletivas que procedem ao tratamento de dados nos termos da lei e subdividem-se em *controlador*, que se referem às decisões relativas ao tratamento de dados; e *processador*, que processa dados em nome do controlador (BRASIL, 2018).

O controlador de dados permanecerá responsável pelo processamento de dados realizado pelo processador. O controlador deve não só confirmar que as instruções são cumpridas devidamente, mas certificar que o processamento de dados está em conformidade com as regras e regulamentos aplicáveis. As empresas contratadas para processamento de bancos de dados com o objetivo de melhorar a assertividade das campanhas de *marketing* são um exemplo comum da relação controlador-processador.

O *responsável* é aquele atribuído pelo driver, que atua na comunicação entre o controlador e o *titular* dos dados, bem como com a Autoridade Nacional de Proteção de Dados (ANPD), responsável por fornecer, fiscalizar e implementar cumprimento da LGPD no território brasileiro, enviando relatório sobre o potencial de impacto do tratamento nos dados pessoais. Esse documento deve conter as seguintes informações mínimas: (i) Descrição dos dados coletados; (ii) Detalhes sobre a metodologia de coleta de dados e as medidas de valores mobiliários aplicados ao banco de dados; e (iii) Medidas, salvaguardas e sistemas adotados para mitigar riscos aos dados processados (BRASIL, 2018; COTS, 2018).

A LGPD ainda determina expressamente que a ANPD não só promulgará as regras aplicáveis ao oficial de proteção de dados, mas também pode estabelecer responsabilidades adicionais para o agente, bem como definir empresas que dispensar uma obrigação de nomeação (com base em suas atividades, porte ou volume de processamento de dados).

A LGPD, em seu art. 6º dispõe de alguns princípios para o processamento de dados pessoais que podem ser associados a cinco dos seis princípios. Esses princípios devem observar a boa-fé, o conceito brasileiro que pode ser entendido no Direito Civil como um conceito relacionado à conduta ética do cidadão não qualifica suas ideias são moldadas a partir da consciência da conduta correta e digna, além de estarem baseadas em atitudes de honestidade, princípios, boas intenções e com o propósito de não prejudicar ninguém (RODRIGUES (2003), e estão listados a seguir (BRASIL, 2018; CANEDO et al., 2020; PESSOA et al., 2021):

1. Finalidade ou Transparência: o processamento de dados pessoais deve ser um objetivo legítimo, especificado e explicitamente conhecido pelo proprietário dos dados;

2. Adequação ou limitação da forma: o processamento dos dados deve ser consistente com a forma solicitada;

3. Necessidade ou Minimização de Dados: os dados devem ser restringidos exatamente ao que é necessário para o processo;

4. Acesso gratuito: o proprietário dos dados deve poder consultar a forma e a duração do processamento, bem como os dados próprios, a qualquer momento, de forma gratuita e fácil;

5. Qualidade ou exatidão dos dados: os dados processados devem ser armazenados, organizados e manipulados à clareza, exatidão, alternativa e atualidade dos dados;

6. Transparência: as informações sobre o processamento de dados devem ser organizadas com clareza e objetividade, responsável pela sua informação;

7. Segurança ou integridade: os dados devem ser seguros técnicos e administrativamente (dados físicos e digitais);

8. Prevenção: adoção de medidas para evitar possíveis danos causados ao processamento de dados;

9. Não discriminação: proibição de processamento de dados para fins de discriminação ou abuso; e

10. Prestação de contas: demonstração dos meios utilizados para cumprir a legislação e prestação de contas pelo processamento dos dados.

Os conceitos de segurança da informação são fornecidos no LGPD desde a determinação da utilização de mecanismos como segurança física e controle de acesso, entre outros, desde a concepção do produto ou serviço até sua execução (BRASIL, 2018). As melhores práticas de governança em relação ao processamento de dados também são comuns pela LGPD como: a determinação de criar um programa de governança de privacidade, com atualização periódica que demonstra compromisso com o cumprimento da lei, adequação à natureza dos dados tratados, plano de resposta a incidentes e estabelecer relação de confiança com o proprietário dos dados, entre outros (POHLMAN, 2019).

O objetivo da criação da lei com os seus princípios, direitos dos detentores de dados e boas práticas é proporcionar meios para que o cidadão conheça o tratamento dos dados efetuado à sua própria informação e tenha uma possibilidade de encerrar o seu tratamento quando necessário.

1.4 BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS

Com o objetivo de garantir que o tratamento de dados pessoais será válido e válido, um LGPD disponibiliza uma lista de hipóteses em que essas operações podem ocorrer. Essas condições jurídicas, mais marcadas como “Bases Legais”, abrangem diversos cenários possíveis para a legitimação das operações de processamento. Para tanto, é necessário que haja uma avaliação dos agentes de processamento para identificar uma base jurídica mais relevante para cada uma de suas operações, ponderando, neste processo, fatores como o grau de segurança da base jurídica contra questionamentos futuros, o conjunto das medidas acessórias de que necessita, entre outras questões.

Nesse sentido, de acordo com o artigo 7º da LGPD, os dados pessoais só podem ser processados:

1. Com o consentimento do titular dos dados;
2. Para atender aos legítimos interesses do controlador ou de terceiro;
3. Para cumprir as obrigações legais ou regulamentares do controlador;
4. Para a execução de um contrato ou procedimentos preliminares relacionados com um contrato do qual o titular dos dados seja parte;
5. Durante o exercício regular de direitos em procedimentos judiciais, administrativos ou arbitrais;
6. Para fins de proteção de crédito;
7. Para proteção da vida ou segurança física do titular dos dados ou de terceiros;
8. Para proteção da saúde (somente por profissionais de saúde, serviços de saúde ou autoridades de saúde);
9. Para a realização de estudos por entidades de pesquisa; e
10. Para uma execução de políticas públicas (somente pela Administração Pública). (BRASIL, 2018)

Além disso, o tratamento de dados pessoais será considerado irregular quando não cumprir a legislação (ou seja, se for conduzido fora do âmbito das autorizações acima mencionadas) ou quando não fornecer a segurança que o titular dos dados pode esperar, considerando: (i) a forma como o processamento é realizado; (ii) o resultado e os riscos que dele se encontram razoavelmente; e (iii) as

técnicas de processamento de dados pessoais disponíveis no momento em que foi realizado (COTS, 2018).

Uma vez que uma operação de tratamento não se enquadre em nenhuma das bases jurídicas previstas em lei, o driver deve assegurar o fim do tratamento, o que ocorrerá quando: (i) terminar o período de processamento; (ii) houver manifestação do titular dos dados solicitando o fim do processamento; (iii) há determinação legal a esse respeito; ou (iv) se qualificar o fim que justificou o tratamento foi alcançado, ou que os dados pessoais recolhidos perderam a sua obtenção para o fim pretendido (BRASIL, 2018; PINHEIRO, 2018).

1.4.1 Consentimento

A Lei Geral de Proteção de Dados exige o consentimento dos titulares dos dados para o tratamento dos seus dados pessoais. Consentimento é a autorização direta para o tratamento de dados pessoais pelos titulares dos dados. Esta base legal é uma forma de expressão da manifestação de vontade do titular dos dados pelo qualifica-se com as operações de tratamento para os requisitos que lhe são solicitados (BRASIL, 2018).

O consentimento só é válido, por lei, se for expresso de forma (i) livre, (ii) informada e (iii) inequívoca, por escrito ou por qualquer outro meio que o dependente. A este respeito:

(i) Gratuito: o titular dos dados deve ser livre para escolher se concorda ou não com o tratamento de seus dados para uma especial, que será avaliado à luz do contexto específico em que o titular dos dados está inserido em relação ao driver;

(ii) Informado: o titular dos dados deve ter acesso fácil a todas as informações relevantes sobre o processamento de seus dados, e o responsável pelo tratamento deve apresentar (de forma clara, adequada e ostensiva) informações sobre: (a) a informática específica da operação, (b) como e por quanto ao tempo os dados serão processados, (c) quem são os agentes de processamento processados e (d) com quem eles desejam compartilhar esses dados, entre outras questões.

(iii) Unequívoco: o controlador deve minimizar de forma proativa como chances do titular dos dados ter dúvidas sobre o tratamento dos seus dados, o que

se dá por meio da adoção de técnicas como o uso de linguagem simples e direta e na linguagem titular dos dados (BRASIL, 2018).

Nesse sentido, todas as finalidades do tratamento devem ser informadas de forma clara, detalhada e separada, cabendo ao controlador o ônus de provar que adotou as ferramentas e necessárias para garantir que o consentimento foi dado de acordo com o (embora não seja necessário reunir qualquer evidência da efetiva dos titulares dos dados das informações nas quais se baseou o seu consentimento). Assim, se a informação prestada ao titular dos dados tiver conteúdo enganoso ou abusivo ou não tiver sido antecipada, de forma clara e inequívoca, o dado será considerado nulo, não autorizando, portanto, o tratamento dos dados pessoais.

É importante mencionar que o titular dos dados tem o direito de revogar o consentimento a qualquer momento, mediante manifestação expressa e por meio de procedimento gratuito e facilitado. Neste cenário, o controlador deve encerrar qualquer operação de processamento baseada exclusivamente no consentimento do titular dos dados. Observe que mesmo que não seja possível continuar a coleta de dados pessoais sem o consentimento ou outras bases legais que podem autorizá-lo, o uso dos dados antes da revogação válida, e seu armazenamento só é possível no caso de o titular dos dados também não exige a eliminação de dados ao revogar seu consentimento (POHLMANN, 2019).

Além disso, se houver qualquer alteração no tratamento de dados pessoais que não seja compatível com o consentimento original, seja em relação ao objetivo da operação com dados pessoais, sua forma e duração ou sobre o controlador e o controle deste pessoal informação, o responsável pelo tratamento deve informar a pessoa em causa, destacando especificamente o conteúdo das mudanças para que possa revogar o seu consentimento concedido caso discorde da alteração.

1.4.2 Casos particulares

A LGPD discorre sobre casos específicos em que o consentimento exigirá maior cautela quanto à sua obtenção, sendo necessário, portanto, que além de ser livre, informado e inequívoco, seja expresso de forma específica e destacada em relação a outras operações. Estas condições exigirão caso seja necessário consentimento para efeitos de processamento (i) de dados pessoais específicos; ou

(ii) dados de crianças; ou, para (iii) autorizar um *download* internacional de dados pessoais (BRASIL, 2018).

Em relação ao tratamento dos dados pessoais das crianças, algumas particularidades estão presentes, pois essas operações devem ser realizadas no melhor interesse da criança. Por este motivo, o consentimento específico e destacado não é apenas uma única base jurídica aplicável a estas operações, mas também deve ser prestado por, pelo menos, um dos responsáveis legais da criança (BRASIL, 2018).

Nesse cenário, o responsável pelo tratamento também deve manter as informações públicas sobre os tipos de dados coletados, bem como a forma de uso e o exercício dos direitos que a LGPD confere ao titular dos dados. A lei também impõe aos drivers o dever de exigir apenas as informações mínimas necessárias para a participação das crianças em jogos, aplicativos da Internet e outras atividades.

1.4.3 Interesse legítimo

A base jurídica do interesse legítimo do responsável pelo tratamento aplicar-se-á no contexto em que seja necessário justificar o tratamento de dados pessoais para fins legítimos relacionados com a sua atividade. Esta avaliação, no entanto, depende de um equilíbrio entre a necessidade do responsável pelo tratamento e a existência de direitos e liberdades fundamentais do titular dos dados que proteção de dados pessoais. Nesse sentido, se prevalecerem essas garantias fundamentais, não será possível adotar o “interesse legítimo” como base jurídica.

Nessa avaliação, a LGPD também deve ser uma lista de finalidades que pode justificar o legítimo interesse do driver, sendo necessário associá-las à análise do caso específico. São eles: (i) o apoio e a promoção das atividades do controlador; (ii) a proteção em relação ao titular dos dados do exercício regular dos seus direitos; e (iii) prestação de serviços que beneficiem o titular dos dados, desde que respeitadas as suas expectativas. No caso de tratamento de dados pessoais com base no legítimo interesse do responsável pelo tratamento, apenas podem ser utilizados nos dados estritamente tratados (no que diz respeito ao princípio da minimização). (BRASIL, 2018).

Embora limitada pelas barreiras acima mencionadas, a base jurídica do legítimo interesse dá, de fato, uma maior amplitude à autorização de procedimento de tratamento. Por esse motivo, embora seja necessário que o controlador mantenha um registro de suas operações como um todo; essa exigência é ainda mais imprescindível para aquelas atividades pautadas no interesse legítimo. É ainda possível que a Autoridade Nacional de Proteção de Dados (ANPD) exija uma apresentação de relatório sobre o impacto da proteção de dados pessoais no contexto desse funcionamento (POHLMANN, 2019).

Adicionalmente, é importante referir que a utilização do conceito de interesse legítimo como base jurídica para o tratamento de dados pessoais é feito de forma residual. Nesse processo, primeiro avalia-se em que medida outras bases jurídicas específicas podem sustentar a legitimidade da operação. Se não for o caso, e de fato o uso do "interesse legítimo" for necessário, é necessário verificar (i) em que medida os dados são processados por meios legítimos (a fim de apoiar e promover a atividade do responsável pelo tratamento, mas ainda em benefício do titular dos dados), e (ii) se o tratamento está de acordo com as expectativas legítimas dos titulares dos dados (considerando os seus direitos e liberdades fundamentais no decurso da operação). (BRASIL, 2018).

2 DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS

Sabe-se que o objetivo principal do LGPD é regular o processamento de dados e proteger os dados pessoais contra o uso não autorizado. A legislação categoriza os dados em diferentes grupos, de acordo com o potencial dano que o uso não autorizado pode causar ao titular dos dados em questão. Além disso, um LGPD também usa várias hipóteses em que tanto os drivers como os operadores podem ser responsabilizados por danos decorrentes de processamento ilícito de dados (BIONI, 2019).

Conforme descrito anteriormente, os agentes de processamento de dados são categorizados de acordo com seu poder de decisão sobre os parâmetros aplicáveis às atividades de processamento de dados. Considerando que os responsáveis pelo tratamento têm maior poder de decisão final sobre os dados e neste contexto, estão ligados a um maior grau de responsabilização perante os titulares dos dados, sendo diretamente responsáveis pelo uso indevido dos dados pessoais. Por sua vez e como regra geral, os processadores de dados são responsáveis por danos envolvendo o processamento de dados apenas nas situações em que suas ações não estejam em conformidade com a lei ou com as instruções recebidas do controlador de dados (GUTIERREZ, 2019).

2.1 RESPONSABILIDADES PARA AGENTES DE PROCESSAMENTO DE DADOS

As secções 42 a 45 da LGPD abrangem as regras aplicáveis aos drivers e configurados de dados no que diz respeito à sua responsabilidade perante o titular dos dados pessoais e à respetiva sobrecarga de danos.

De acordo com o atual quadro legal, o responsável pelo tratamento é, em regra, total e diretamente responsável pelo tratamento dos dados. O processador de dados pode ser considerado solidariamente responsável caso as atividades de processamento sejam ilegais ou não foram realizadas de acordo com as instruções dos drivers de dados (SALGADO; SAITO, 2020).

É importante destacar que se o tratamento de dados estiver vinculado a mais de um driver de dados, todos eles serão solidariamente responsáveis pelos danos decorrentes de tais atividades.

Uma LGPD define processamento ilegal de dados como qualquer atividade de processamento de dados realizada em violação da legislação de proteção de dados ou que não forneça um nível adequado de proteção aos dados pessoais. A análise da suficiência do nível de proteção compreende os elementos como a existência de risco, os meios do processamento de dados e das medidas de segurança disponíveis (DONEDA, 2019).

A responsabilidade dos agentes de processamento de dados é a especificação, o que significa que a falha do controlador ou processador deve ser demonstrada. Em consequência, a mera existência de danos para o titular dos dados é insuficiente para criar uma obrigação de compensação (exceção feita às relações de consumo).

De acordo com Camurça e Matias (2021), em algumas hipóteses, os *drivers* e ajustes de dados podem ser isentos de qualquer responsabilidade para com o titular dos dados pessoais. Em caso de exclusão de responsabilidade se LGPD:

(i) Os *drivers* / processador podem provar que não realizaram a atividade de processamento de dados relevante .

(ii) Os *drivers* / processador podem provar que o processamento dos dados é devidamente lícito e não viola qualquer acordo; ou

(iii) Os danos surgem exclusivamente devido a falhas causadas pelo próprio titular dos dados ou por terceiros.

Conforme previsto pela LGPD, como atividades de processamento de dados vinculadas às relações de consumo estão relacionadas à legislação brasileira de defesa do consumidor. Nesse sentido, são aplicáveis as disposições específicas nessas situações, como a inversão do ónus da prova e a responsabilidade objetiva dos agentes informáticos (GUNTHER et al., 2020).

2.1.1 Cumprimento de obrigações estatutárias ou regulamentares

O processamento de dados pessoais também será autorizado quando necessário para que o controlador cumpra suas obrigações estatutárias ou regulatórias de acordo com o ordenamento jurídico brasileiro. Vale ressaltar que atividades específicas são dotadas de amplos conjuntos normativos expedidos pelos órgãos públicos competentes (como a Comissão de Valores Mobiliários - CVM, o Banco Central do Brasil - BACEN, ou o Órgão de Defesa do Consumidor -

PROCON) regulamentando ainda mais o conjunto das obrigações inerentes a estes campos, que se apresentam presentes, por exemplo, nas áreas do trabalho, das relações de consumo, do mercado financeiro ou de seguros (SILVA; MELO, 2019).

Esta base jurídica confere maior segurança à legitimidade das operações de tratamento, uma vez que não envolve a necessidade de consentimento prévio do titular dos dados (que pode ou não ser dado, como nos casos com base no consentimento), nem a avaliação da viabilidade do sua aplicação (como no caso de ponderar a aplicabilidade do interesse legítimo). Desta forma, a maior clareza e certeza para fundamentar uma operação de dados de forma legítima virá de fato face à existência de uma obrigação legal ou regulamentar que requeira o tratamento de dados (FRAZÃO et al., 2019).

2.1.2 Execução de um contrato ou procedimentos preliminares

Para operacionalizar como tratamento de tratamento (nomeadamente de acesso e partilha) dos dados pessoais contidos ou que constar de contratos privados, a LGPD estipulou ainda a possibilidade de autorização legal para o tratamento de dados quando esta atividade for iniciada ponto para uma execução de um contrato ou procedimentos preliminares relacionados a um contrato do qual o titular dos dados seja parte. Neste caso, uma vez verificado que os dados pessoais são instrumentalmente instalados para uma execução de um contrato ou para uma execução dos seus termos, o driver ficará de fato autorizado a proceder à operação (OLIVEIRA; LOPES, 2019).

Para ilustrar esse cenário, é possível considerar a utilização de dados pessoais para a qualificação de pessoas físicas nos contratos dos quais farão parte. Além disso, do ponto de vista dos contratos já celebrados, é possível que a utilização de dados pessoais seja necessária para a execução do objeto do contrato, visto que através da validação de documentos fornecidos a partir da assinatura de um titular dos dados que o tenha sido contratada para supervisão setorial, função que exige o compartilhamento desses dados pessoais em diversos documentos da empresa (FINKELSTEIN; FINKELSTEIN, 2019).

Independentemente do cenário, na medida em que o tratamento de dados seja necessário para a celebração ou formação de um contrato de que o titular dos

dados faça ou venha a fazer parte, a LGPD dá de facto autorização para a continuação desta operação.

2.1.3 Exercício regular de direitos em procedimentos

Em consonância com o objetivo de avaliar não só os interesses dos titulares dos dados, mas também dos responsáveis pelo tratamento, a LGPD apresenta um cenário específico no domínio processual que pode ser defendido como uma autorização legal para o tratamento de dados pessoais. Assim, uma operação de tratamento de dados será legítima na medida em que seja necessária para assegurar o exercício regular de direitos em procedimentos judiciais, administrativos ou arbitrais (DONEDA, 2019).

Ainda que esta base jurídica possa pautar qualquer operação com tratamento de dados pessoais, a sua aplicação mais recorrente reside no âmbito das operações de acesso, partilha e armazenamento de dados pessoais que se estabelecem para cumprir como formalidades inerentes a processos específicos, que pode ocorrer dentro de processos que podem ser potenciais ou já em andamento (como lidar com qualquer notificação extrajudicial). (CARVALHO; PEDRINI, 2019).

Em se tratando de possíveis ações judiciais, será possível, portanto, que um driver de dados armazene os dados pessoais de seu cliente (após mesmo o término de sua relação jurídica) na medida em que tais informações relevantes para o desenvolvimento de seu eventual defesa judicial, o que é plausível tendo em vista que tal cliente pode acabar contra ele (CAMURÇA; MATIAS, 2021).

Ressalta-se, entretanto, que esta operação de armazenamento não será legítima se mantida por tempo indeterminado. Faz-se necessário, portanto, o cumprimento do prazo de prescrição para eventual ajuizamento de ação judicial, administrativa ou arbitral contra o controlador. Com o reconhecimento de que após esse prazo não será possível mais ajuizar a ação, a base jurídica em questão perde seu fundamento a partir deste momento.

2.1.4 Proteção de crédito

O tratamento de dados pessoais também será legítimo quando necessário para a proteção de crédito, o que deve ser feito considerando uma natureza de

interesse público que envolve o sistema de crédito. Nesse cenário, essa base legal é fortemente utilizada não só por escritórios especializados na avaliação de risco de crédito, mas também será fundamental e estratégica para os agentes de processamento que se deparam com matrizes de avaliação de risco de suas operações de crédito, o que é relevante no contexto de bancos ou seguradoras, por exemplo (DONEDA, 2019).

2.1.5 Proteção da vida ou da segurança física

Com enfoque direto no bem jurídico da vida, a LGPD apresenta-se como uma autorização específica para o tratamento de dados pessoais em qualquer operação que seja efetuada com o intuito de permitir ao controlador poder promover a proteção da vida ou da segurança física do titular dos dados ou de terceiros.

Em muitos casos, é provável que o tratamento de dados para este fim envolva inevitavelmente o tratamento de dados pessoais relativos (como dados relativos às condições de saúde dos titulares dos dados), razão pela qual esta base jurídica também é aplicável para as operações que ocorrem com esta categoria especial de dados (CARVALHO; PEDRINI, 2019).

Em meio à pandemia de COVID-19, por exemplo, a base jurídica em questão tem sido aplicada com maior recorrência, na medida em que os diferentes atores da sociedade civil passam a implementar implementadas preconizadas para o combate ao coronavírus em seus ambientes privados (como em edifícios corporativos, industriais ou técnicos comerciais).

Nesse cenário, a coleta de informações médicas dos titulares de dados que transitam por esses ambientes é vista como uma ferramenta relevante para o mapeamento desejado que podem ser potenciais transmissores do vírus, o que é feito, portanto, com o objetivo de limitar a proliferação do doença (CAMURÇA; MATIAS, 2021).

Assim, vale ressaltar que os princípios da transparência e da necessidade ainda devem ser observados como marco que delimita a utilização desses dados de forma que nenhuma coleta desnecessária ou abusiva de dados pessoais surja sob o manto que a premissa da proteção impõe da vida. É importante, portanto, que apenas o tratamento dos dados pessoais determinados.

2.1.6 Proteção da saúde

Seguindo o mesmo raciocínio que deve ser jurídica do tratamento de dados para proteção da vida ou segurança física, a LGPD alarga o âmbito desta garantia ao estabelecer que qualquer operação com dados pessoais necessários à proteção da saúde, como um todo, considerada legítima.

Existe, no entanto, uma restrição à qual os agentes de transformação podem invocar essa base jurídica como fundamento para autorizar a sua atividade. Fica estabelecida na lei, portanto, que esta hipótese será aplicável, exclusivamente, nas operações previstas por (i) profissionais de saúde, (ii) serviços de saúde ou (iii) autoridades de saúde (BRASIL, 2018).

Sobre a restrição de quais agentes podem fazer uso dessa base legal, fica claro que os principais fatores nesse contexto são, sim, hospitais, planos de saúde e demais profissionais da área de saúde. Adicionalmente, tal como a base jurídica aplicada no âmbito da proteção da vida ou da segurança física, como atividades de proteção da saúde podem exigir o tratamento de dados pessoais (neste caso, os relacionados com as condições de saúde dos titulares dos dados), razão pela qual base jurídica também é aplicável para operações envolvendo esta categoria especial de dados (CAMURÇA; MATIAS, 2021).

Observa-se, entretanto, que o escopo das operações com tais dados médicos encontra uma série de limitações prescritas na LGPD, o que restringe o que pode ser feito com essas informações, mesmo à luz do princípio da necessidade. A este respeito, é proibida a comunicação ou utilização partilhada de dados pessoais relacionados em matéria de saúde entre responsáveis pelo tratamento, sempre que estabelecido com o objetivo de obter vantagem econômica, salvo se o para nas operações relacionadas com a prestação de serviços de saúde, assistência farmacêutica e assistência à saúde (incluindo serviços auxiliares de diagnóstico e terapia), desde que sejam realizados no interesse dos titulares dos dados (GUNTHER et al., 2020).

Além disso, as operadoras de planos privados de saúde estão proibidas de processar dados de saúde para a prática de seleção de risco em qualquer modalidade de contratação.

2.1.7 Realização de estudos por entidades de pesquisa

O tratamento de dados pessoais também será autorizado quando necessário para a realização de estudos, desde que sejam realizados por entidades oficiais de pesquisa. Nesse sentido, um visto LGPD protege a produção científica do país, fazendo-se necessário, entretanto, que o órgão de pesquisa se enquadre na definição legal deste e limite sua atuação apenas à atividade de pesquisa.

Em relação aos dados coletados, é importante reiterar que não só a agência deve se limitar a coletar o mínimo necessário para o cumprimento do objetivo da pesquisa, mas também, sempre que possível, promover o anonimato dos dados pessoais coletados (ou seja, assegurar a despersonalização efetiva dos dados considerando a utilização dos meios técnicos razoáveis disponível no momento do processamento) (CAMURÇA; MATIAS, 2021).

Assim, na medida em que não seja necessária a identificação dos dados dos dados que participam da pesquisa, é recomendado por lei que a coleta de dados propriamente dita seja feita de forma anônima a partir de sua origem, de forma que a pesquisa seja trabalhando com análise dos resultados relativos a grupos diferentes, em vez de se concentrar em determinados assuntos de dados específicos (DONEDA, 2019).

2.1.8 Execução de políticas públicas

O tratamento de dados pessoais encontra na LGPD a última hipótese pública de autorização legal, que somente será aplicável às operações realizadas pela administração com o objetivo de compartilhar e usar as informações necessárias à execução de políticas públicas (publicação em leis ou regulamentos, ou com base em contratos, acordos ou instrumentos semelhantes) (PINHEIRO, 2018).

A administração pública, como agente de processamento, está também obrigada a cumprir os princípios e garantias de LGPD, devendo, pública, assim, limitar as suas operações com dados pessoais ao cumprimento da sua necessidade e à prossecução do interesse público, em para o desempenho das suas competências legais ou para o cumprimento das atribuições legais da função pública (SALGADO; SAITO, 2020).

Adicionalmente, embora os dados pessoais tratados pela administração pública devido à dependência da LGPD existem algumas regras que diferenciam os seus direitos e obrigações como controlador de dados das entidades privadas. Por exemplo, o consentimento do titular dos dados não é necessário para a concepção e implementação de políticas públicas, mas sim para outros cenários (OLIVEIRA; LOPES, 2019).

Além disso, no caso de segurança pública, defesa nacional, segurança do Estado e atividades investigativas e ações judiciais de infrações criminais e atividades de investigação e repressão de ofensas criminais, os dados pessoais serão processados de acordo com uma legislação específica que ainda será promulgada.

2.1.9 Particularidades dos dados pessoais sensíveis

De acordo com o exposto acima, os dados pessoais registrados são classificados como uma categoria especial de dados pessoais que ex. Um nível de proteção superior por parte da LGPD. Por esse motivo, algumas das bases jurídicas acima não serão aplicadas ao tratamento desses dados:

(i) Processamento com meios que atendem aos legítimos interesses do controlador ou de terceiros;

(ii) Processamento para a execução de um contrato ou procedimentos preliminares relacionados a um contrato do qual ou titular dos dados parte seja; e

(iii) Processamento para fins de proteção de crédito.

Em contrapartida, como bases jurídicas aplicáveis tanto ao tratamento de dados pessoais como aos dados pessoais à luz da LGPD são aquelas em que o tratamento é necessário:

(i) Um fim de cumprir as obrigações estatutárias ou regulamentares do controlador;

(ii) Para proteção da vida ou segurança física do titular dos dados ou de terceiros;

(iii) Para proteção da saúde (apenas por profissionais de saúde, serviços de saúde ou autoridades de saúde);

(iv) Para a realização de estudos por entidades de pesquisa; e

(v) Para a execução de políticas públicas (somente pela Administração Pública).

Neste cenário, algumas bases jurídicas já definidas para o tratamento de dados pessoais foram complementadas de forma a aumentar o seu nível de proteção e, assim, também se adequarem ao tratamento de dados pessoais:

(i) Consentimento, que deve ser não apenas livre, rede e inequívoco, mas também específico e destacado; e

(ii) O exercício regular de direitos em procedimentos judiciais, administrativos ou arbitrais, para o tratamento de dados pessoais relacionados, inclui a possibilidade de exercício regular de direitos também em contratos, o que é um análogo à base legal para uma execução de contratos (excluindo, no entanto, permissão para o tratamento de dados para procedimentos ao abrigo de procedimentos contratuais preliminares relacionados com o contrato) (BRASIL, 2018).

Por último, os dados pessoais sensíveis podem ser tratados com base na oitava e última permissão legal, que se apresenta na substituição da possibilidade de tratamento por razões de proteção de crédito e no interesse legítimo do responsável pelo tratamento (CAMURÇA; MATIAS, 2021).

Desta forma, uma operação de processamento será legítima quando necessária para garantir a prevenção de fraudes e a segurança do titular dos dados, em processos de identificação e autenticação de registo em sistemas electrónicos, o que é possível desde que seja garantido o acesso fácil às informações sobre uma operação (OLIVEIRA; LOPES, 2019).

Nota-se que o mesmo processo de ponderação de interesses em jogo estabelecido para avaliar a aplicabilidade de interesse legítimo será necessário para a autorização em análise, de forma que esta base legal não será aplicada no caso de direitos e liberdades fundamentais dos dados assuntos que ex. proteção de dados pessoais prevalecem.

2.2 TRANSFERÊNCIA DE DADOS INTERNACIONAIS

Nas últimas décadas, a fonte de dados pessoais por meio de vários serviços públicos tornou-se uma característica inevitável da era digital. Seja para participação em redes sociais, para uso de Sistema de Posicionamento Global (GPS) ou mesmo para compra de produtos e serviços online.

A sociedade global vive uma verdadeira revolução neste aspecto há muito tempo, uma vez que os obtém de ser apenas consumidores e passam a serem fornecedores de informações e dados extremamente valiosos para diversas empresas de diferentes segmentos, sejam públicos ou privados (CAMURÇA; MATIAS, 2021).

Defendido à globalização econômica, tornou-se evidente que a circulação de informações e dados pessoais em geral ultrapassaria como fronteiras territoriais dos países no mundo. Por este motivo é importante regulamentar as condições para o tratamento de dados pessoais a nível internacional (transferência de dados internacionais). (GUNTHER et al., 2020).

O legislador brasileiro inspirou-se na GDPR para editar a LGPD, publicada em 14 de agosto de 2018. Antes da LGPD, o Marco Civil da Internet (Lei nº 12.965 / 14) foi o primeiro instrumento jurídico que iniciou a abordagem dos direitos dos usuários não que se referenciou à transferência internacional de dados e foi o único ato infraconstitucional que dispositivos que tratam de dados pessoais sem redes. Seguem as disposições do artigo 11:

> Art. 11. Qualquer operação de coleta, armazenamento, armazenamento e tratamento de registros, dados pessoais ou comunicações por provedores de conexão e aplicativos de internet em que pelo menos um atos ocorra em território nacional está determinado à legislação brasileira e deve obrigatoriamente os direitos de privacidade, proteção de dados pessoais e confidencialidade de comunicações e registros privados.
> § 1 º A provisão acima mencionada aplica-se aos dados recolhidos no território nacional e o conteúdo das comunicações, desde que pelo menos um dos terminais está localizado no Brasil.
> § 2 º A provisão acima mencionada aplica-se mesmo se as atividades são realizadas por pessoa jurídica com sede no exterior, desde que oferece serviços ao público brasileiro ou pelo menos um membro do mesmo grupo econômico tenha um estabelecimento no Brasil.
> § 3 º Os provedores de conexão e aplicação de internet deve fornecer, de acordo com os regulamentos, informação que permite a verificação da conformidade com a legislação brasileira em relação à coleta, conservação, armazenamento ou processamento de dados, bem como sobre o respeito da privacidade e confidencialidade das comunicações.
> § 4º O Decreto regulará o procedimento de apuração de infração ao estudar neste artigo.

O Marco Civil da *Internet* foi a primeira legislação no Brasil a respeito da governança da Internet, visto que não existe legislação específica no país tratando do assunto até então.

A transferência internacional de dados foi abordada na LGPD, especificamente no Capítulo V, artigos 33 a 36, sendo definida como a situação em

que ocorre a transferência de dados para o país estrangeiro ou organismo internacional de que o país seja membro.

De acordo com o artigo 33 da lei, a transferência internacional só será permitida quando:

(i) para países ou associações internacionais que proporcionam um grau de proteção de dados pessoais adequado ao previsto nesta Lei;

(ii) o *driver* oferece e prova garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previsto na LGPD (na forma de: (a) cláusulas contratuais específicas para uma fornecida; (b) cláusulas contratuais padrão; (c) padrões corporativos globais e (d) selos, certificados e códigos de conduta emitidos regularmente);

(iii) a transferência é necessária para a cooperação internacional entre órgãos de inteligência, investigação e ação penal, de acordo com os instrumentos de direito internacional;

(iv) transferência é necessária para proteger a vida ou a segurança física do titular ou de terceiros;

(v) Autoridade Nacional Autorizada para Transferência;

(vi) download resultado em compromisso firmado em acordo de cooperação internacional ;

(vii) transferência para a execução de ordem pública ou público legal de serviço público;

(viii) o titular deu seu consentimento específico e destacado para a transferência, com informação prévia sobre o caráter internacional da operação, diferenciando-a de outras finalidades; ou

(ix) necessário para atender às obrigações legais ou regulamentares do controlador (BRASIL, 2018).

Quanto à autorização para transferência internacional de dados prevista no inciso I do artigo 33, a LGPD não é totalmente clara ou detalhada quando utiliza uma expressão “grau de proteção de dados pessoais adequado ao previsto nesta Lei”. A revisão do grau de proteção foi delegada ao ANDPD por meio do artigo 34, que deve considerar o seguinte na análise de um caso específico:

> (i) regras gerais e setoriais da legislação em vigor no país de destino ou na organização internacional;
> (ii) natureza dos dados;

> (iii) observância dos princípios gerais de proteção dos dados pessoais e dos direitos dos títulos de acordo com a LGPD;
> (iv) adoção de medidas de segurança previstas em regulamento;
> (v) existência de garantias judiciais e institucionais de respeito aos direitos de proteção de dados pessoais; e
> (vi) outras entidades específicas relativas a transferências (BRASIL, 2018).

Apesar da existência da existência de uma autoridade nacional de proteção de dados, não podemos negar que a campeã não é eficaz apenas por meio da padronização, mas também por meio da iniciativa privada (PINHIRO, 2018).

Também é importante destacar que existe um grande interesse econômico nos fluxos internacionais de dados, razão pela qual a transferência de dados também é objeto de vários internacionais.

Por isso, o artigo 35 da LGPD determina que a verificação das cláusulas contratuais de uma fornecida, bem como dos padrões corporativos globais, é de responsabilidade da ANPD, que considera os requisitos, condições e garantias mínimas prestadas pelos brasileiros para viabilizar soluções privadas, podendo mesmo requerer informações complementares ou realizar procedimentos de verificação das operações de tratamento, quando julgar necessário (CAMURÇA; MATIAS, 2021).

Além disso, a ANPD pode designar organismos de certificação, os quais permanecerão sob sua supervisão nos termos a serem definidos em regulamento, lembrando que os atos praticados por tais organismos serão revisados pela autoridade nacional e em caso de descumprimento da LGPD, pode ser cancelado. Qualquer alteração das garantias protegidas em conformidade com os princípios gerais da proteção de dados e dos direitos fundamentais do titular, enumerados no artigo 33, inciso II, da LGPD, deve ser comunicada à autoridade nacional (PINHEIRO, 2018).

Apesar de várias semelhanças com o GDPR, uma estrutura do padrão LGPD que trata do download internacional de dados apresenta uma diferença relevante em relação ao padrão europeu. O legislador brasileiro optou por permitir a transferência internacional de dados para o cumprimento das obrigações legais ou regulamentares por parte do controlador, contrariando as regras definidas pelo GDPR (DONEDA, 2019).

Por fim, a transferência internacional de dados no âmbito da LGPD restringe-se a enquadrar as hipóteses elencadas no artigo 33 da legislação, destacando o rigor e a semelhança entre as legislações brasileira e europeia. Tais elementos

reforçam o compromisso do Brasil com a proteção de dados pessoais e o colocam no caminho do reconhecimento pela União Europeia e outras associações internacionais como uma jurisdição com nível adequado de proteção de dados pessoais (PINHEIRO, 2018).

2.3 COMENTÁRIOS SOBRE A EFICÁCIA DA LGPD

Deve-se notar que, embora as "Disposições Substantivas" acima mencionadas digam respeito, entre outros, a questões sobre os princípios de processamento de dados, bases legais para o processamento de dados pessoais e direitos do titular dos dados, as "Disposições Penais" são limitadas àquelas relacionadas com as penalidades previstas na LGPD (ou seja, como multas e demais penalidades pelo descumprimento da LGPD que a ANPD venha a aplicar na esfera administrativa, como bloqueio de dados pessoais, suspensão temporária ou proibição de atividades de processamento de dados pessoais) (PINHEIRO, 2018).

De qualquer forma, mesmo com a LGPD em pleno vigor, deve-se destacar que a regulamentação brasileira de proteção de dados ainda está em construção, visto que maiores detalhes ainda aguardam a regularidade da ANPD para que a LGPD se torne plenamente operacional (atenuando as dúvidas que surgirem da implementação das suas disposições no dia-a-dia do mercado). Em consequência, com a Autoridade atualmente estruturada e operacional, importa referir que se tem intensificado nesta discussão honrando como suas atribuições regulamentares não apenas emitindo Orientações sobre os assuntos mais prementes (sobre o âmbito e estrutura das notificações de violação de dados, por exemplo), mas também arrecadando contribuições civis para sua futura questão de questões claras na LGPD (SALGADO; SAITO, 2020).

Para a sua futura exigência, de acordo com a Agenda Regulatória da ANPD para o biênio 2021-2022, a Autoridade deve regular as matérias relativas, por exemplo, aos processos administrativos para a aplicabilidade das Disposições Penais da LGPD; procedimentos e garantias para proteção de dados e privacidade de pequenas e médias empresas e startups; às atividades do Diretor de Proteção de Dados; à transferência internacional de dados pessoais; entre outros (CAMURÇA; MATIAS, 2021).

Nesse ínterim, no entanto, independentemente da dependência pendente da ANPD e da única entrada em vigor recente das Disposições Substantivas e Penais da LGPD, deve-se observar que a incidência e aplicação da LGPD já estão consolidadas como uma realidade na prática jurídica brasileira. O Ministério Público (MP), por exemplo, já investigou e processou ativamente como violações de dados envolvendo o vazamento de dados pessoais, o que foi feito com base na sua autoridade constitucional para impetrar ações coletivas em defesa dos interesses coletivos e difusos, especialmente quando a violação envolve consumidores (SALGADO; SAITO, 2020).

Atualmente, até a apresentação deste material (ou seja, com a LGPD em vigor há quase dois anos), já se registrou um número significativo de processos de execução na Justiça brasileira. Embora a ANPD ainda não tenha sancionado os agentes de processamento de dados, as autoridades do consumidor, tanto em âmbito federal quanto ao estadual, estão aplicando a LGPD iniciando investigações administrativas e impondo sanções com esses fundamentos legais (CAMURÇA; MATIAS, 2021).

Nesse contexto, o atual contencioso de privacidade brasileiro indica algumas tendências importantes, sendo as principais questões contestadas nos processos judiciais em relação à forma de coleta de consentimento dos titulares de dados, ao uso de dados pessoais públicos e à responsabilidade dos *drivers* e desligados devido a violações de dados (GUNHTER et al., 2020).

Com esse cenário em perspectiva, fica claro que a preferência brasileira de proteção de dados ainda está sendo desenvolvida nos níveis normativo e judicial, visto que tende a ser mais provável nos anos próximos tanto pela ANPD quanto pelos Tribunais que interpretarão a norma sobre os próximos LGPD casos. Embora as atuais dúvidas e incertezas devam ser tratadas no futuro, a LGPD já se encontra consagrada na Jurisdição brasileira como o marco normativo que trouxe mais segurança jurídica em relação à escassa regulação de proteção de dados no país, razão pela qual as normas e as disposições em vigor devem ser buscadas para a definição de objetivos comerciais não apenas como boas práticas de negócios, mas também como medida de maior segurança para a empresa no Brasil.

CONCLUSÃO

Um número crescente de sistemas atuais trata de informações pessoais (por exemplo, informações sobre cidadãos, clientes), onde as informações são protegidas por várias leis e normas de privacidade. Portanto, a privacidade se tornou uma grande preocupação para os projetistas de sistemas. Em outras palavras, lidar com as questões de privacidade é uma obrigação hoje em dia, porque as violações de privacidade podem resultar em consequências graves. Vários estudos lançaram luz sobre os custos de economia das violações de privacidade, deixando claro que a ausência de mecanismos de proteção de privacidade impõe enormes custos às associações, bem como custos indiretos e consequências de longo prazo.

A LGPD surgiu como uma forma de facilitar o tratamento de dados com base em princípios de ética e boa fé. Além disso, suas diretrizes visam atuar em prol da segurança e privacidade dos dados dos usuários, levantando dúvidas e direcionando soluções para que associações brasileiras, públicas e / ou privadas, como implementem durante a coleta e manipulação dos dados. No entanto, no decorrer da pesquisa, é possível observar que ainda faltam adequações em relação à governança e gestão de dados e à segurança das informações por parte das associações brasileiras.

Uma possível solução para essa questão pode se dar por meio da ANPD, órgão de administração pública direta, que fará a ponte entre sociedade e governo e tendo como função principal a fiscalização e regulação da LGPD, recentemente instituída. A Autoridade será fundamental para o processo de harmonia das associações brasileiras, uma vez que está em consonância com o Conselho Nacional de Proteção de Dados Pessoais e Privacidade, e irá monitorar, além de garantir que as organizações apliquem os princípios da lei de forma eficaz.

REFERÊNCIAS

ANPD. **ANPD divulga cronograma completo de reuniões técnicas sobre relatório de impacto à proteção dos dados pessoais.** 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-cronograma-completo-de-reunioes-tecnicas-sobre-relatorio-de-impacto-a-protecao-dos-dados-pessoais>. Acesso em 28 dez. 2021.

_____. Ministério da Justiça e Segurança Pública. Conselho Administrativo de Defesa Econômica. **Acordo de Cooperação Técnica nº 5/2021**. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/act-tarjado-compactado.pdf>. Acesso em 28 dez. 2021.

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

BRASIL. Casa Civil. **Lei nº 12.965**, de 23 de abril de 2018. Estabelece princípios, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 12 dez. 2021.

_____. Casa Civil. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 ago. 2021.

CAMURÇA, L. C. V.; MATIAS, J. L.N. Direito à privacidade e à proteção de dados pessoais: análise das práticas obscuras de direcionamento de publicidade consoante a Lei nº 13.709 de 14 de agosto de 2018. **Revista de Direitos Fundamentais & Democracia**, Curitiba, v. 26, n. 2, p. 6-23, mai./ago. 2021. Disponível em: <https://dspace.almg.gov.br/handle/11037/41838>. Acesso em: 28 mar. 2022.

CANEDO, E.D.; CALAZANS, A.T.S.; MASSON, E.T.S.; COSTA, P.H.T.; LIMA, F. Percepções de profissionais de TIC em relação à privacidade de *software*. **Entropy,** v. 22, n. 4, abr. 2020. Disponível em: <https://pubmed-ncbi-nlm-nih-gov.translate.goog/33286202/>. Acesso em: 28 mar. 2022.

CARVALHO, G.P.; PEDRINI, T.F. Direito à privacidade na Lei Geral de Proteção de Dados Pessoais. **Revista da ESMESC**, v. 26, n. 32, p. 363-382, 2019. Disponível em: <https://revista.esmesc.org.br/re/article/view/217/186>. Acesso em: 28 mar. 2022.

COTS, M. **Lei geral de proteção de dados pessoais comentada.** São Paulo: Revista dos Tribunais, 2018.

DONEDA, D. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei geral de proteção de dados. São Paulo: Thomson Reuters Brasil, 2019.

ERICKSON, A. Comparative analysis of the EU GDPR and the Brazilian LGPD: Law enforcement challenges with the LGPD. **Brooklyn Journal of International Law**, v. 44, n. 1, 2018. Disponível em: <https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/9>. Acesso em: 28 mar. 2022.

FINKELSTEIN, M.E.; FINKELSTEIN, C. Privacidade e Lei geral de proteção de dados pessoais. **Revista de Direito Brasileira**, v. 23, n. 9, p. 284-301, Florianópolis, SC, mai./ago. 2019. Disponível em: <https://www.indexlaw.org/index.php/rdb/article/view/5343/4545>. Acesso em: 21 mar. 2022.

FRAZÃO, A.; OLIVA, M.D.; TEPEDINO, G. **Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019.

GUNTHER, L.E.; COMAR, R.T.; RODRIGUES, L.E. A proteção e o tratamento dos dados pessoais sensíveis na era digital e o direito à privacidade: os limites da intervenção do Estado. **Revista Unicuritiba**, v. 2, n. 27, p. 1-17, 2020. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RIMA/article/view/3972/371372300>. Acesso em: 21 mar. 2022.

GUTIERREZ, A. Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. In: MALDONADO, V. N.; BLUM, R.Ó. (Coord.). **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters, 2019, p. 387-402.

MACIEL, Rafael Fernandes. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais** (Lei nº 13.709/18). Goiânia: RM Digital Education, 2019.

OLIVEIRA, M.A.B.; LOPES, I.M.P. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: TEPEDINO, G.; FRAZÃO, A.; OLIVA, M.D. (Coord.). **Lei Geral de Proteção de Dados Pessoais:** e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters, 2019, p. 53-83.

PESSOA, C.R.; NUNES, B.C.; DE OLIVEIRA, C.; MARQUES, M.E. Effects and projections of the application of the General Data Protection Law (LGPD) and the role of the DPO. In.: **Digital Transformation and Challenges to Data Security and Privacy**; IGI Global: Hershey, PA, EUA, 2021; p. 195–208. Disponível em: <https://www-igi--global-com.translate.goog/chapter/effects-and-projections-of-the-brazilian-general-data-protection-law-lgpd-application-and-the-role-of-the-dpo/271778?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc>. Acesso em: 12 mar. 2022.

PINHEIRO, P.P. **Proteção de dados pessoais.** Comentários à Lei nº 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

POHLMANN, Sérgio Antônio. **LGPD Ninja** – Entendendo e implementando a Lei Geral de Proteção de Dados nas empresas. São Paulo: Editora Fross, 2019.

RODRIGUES, S. **Direito Civil.** v. 1 São Paulo: Saraiva: São Paulo, Brasil, 2003.

SALGADO, E.D.; SAITO, V.H. Privacidade e proteção de dados: por uma compreensão ampla do direito fundamental em face da sua multifuncionalidade. **International Journal of Digital Law**, Belo Horizonte, ano 1, n. 3, p. 117-137, set./dez. 2020. Disponível em: <https://journal.nuped.com.br/index.php/revista/article/view/saito2020/25>. Acesso em: 28 fev. 2022.

SILVA, L.G.; MELO, B.L. da A. A lei geral de proteção de dados como instrumento de concretização da autonomia privada em um mundo cada vez mais tecnológico. **Revista Jurídica**, v. 3, n. 56, p. 354-377, jul. 2019. Disponível em: <https://www.researchgate.net/publication/340866889_A_LEI_GERAL_DE_PROTECAO_DE_DADOS_COMO_INSTRUMENTO_DE_CONCRETIZACAO_DA_AUTONOMIA_PRIVADA_EM_UM_MUNDO_CADA_VEZ_MAIS_TECNOLOGICO>. Acesso em: 22 mar. 2022.