Revista de Direito, Governança e Novas Tecnologias

Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 15.02.2025
Aprovado em: 16.02.2025

ANÁLISE COMPARADA DA NORMAS DE PROTEÇÃO DE DADOS DO BRASIL, DA UNIÃO EUROPEIA E DO ESTADO DA CALIFÓRNIA - EUA: LGPD X GDPR X CCPA

COMPARATIVE ANALYSIS OF DATA PROTECTION RULES IN BRAZIL, THE EUROPEAN UNION AND THE STATE OF CALIFORNIA - USA: LGPD X GDPR X CCPA

Marcos Martins de Oliveira[1]

Daniel Barile da Silveira[2]

Maria das Graças Macena Dias de Oliveira[3]

[1] Defensor Público do Estado do Piauí, titular da 2ª Defensoria Pública de Floriano, Estado do Piauí. Coordenador do Núcleo de Defesa da Mulher de Floriano-PI. Professor efetivo-assistente da Universidade Estadual do Piauí. Coordenador do Núcleo de Práticas Jurídicas da Universidade Estadual do Piauí, campus de Floriano-PI. Mestre em Direito Internacional pela Universidade Católica de Santos – UNISANTOS. Doutorando em Direito pela UNIMAR/UNIFIP.

[2] Pós-Doutor em Direito pela Universidade de Coimbra; Doutor em Direito pela Universidade de Brasília (UnB). Professor do PPGD da Unimar (Universidade de Marília).

[3] Doutora e Mestre em Direito pela Universidade de Marília - UNIMAR

RESUMO

Esse artigo faz uma análise comparativa das normas de proteção de dados pessoais vigentes no Brasil (LGPD), na União Europeia (GDPR) e no estado da Califórnia, EUA (CCPA). A metodologia utilizada envolveu uma revisão bibliográfica das legislações mencionadas e a comparação detalhada de seus principais aspectos, conceitos, âmbito territorial de cada normativa, autoridades governamentais de proteção de dados, como é tratada a coleta e o tratamento de dados de menores de idade, e quais direitos as normativas asseguram aos titulares dos dados, principalmente, acesso, retificação e apagamento dos dados coletados. O objetivo da pesquisa foi identificar semelhanças e diferenças entre as três normativas e avaliar sua eficácia na proteção dos dados pessoais. Os resultados indicam que, apesar das divergências culturais e legais entre as regiões, há uma tendência crescente à padronização de normas de proteção de dados, visando maior segurança e transparência no tratamento das informações pessoais. Conclui-se que a CCPA enseja punições consideradas leves em comparação com a LGPD e o GDPR, que são mais abrangentes e rigorosos em suas sanções. A harmonização dessas normas pode facilitar o comércio internacional e promover a proteção de dados em escala global, embora desafios significativos permaneçam na implementação dessas políticas.

Palavras-chave: Proteção de Dados, LGPD, GDPR, CCPA, Direito Comparado

ABSTRACT

This article makes a comparative analysis of the personal data protection standards in force in Brazil (LGPD), the European Union (GDPR) and the state of California, USA (CCPA). The methodology used involved a bibliographical review of the aforementioned legislations and a detailed comparison of their main aspects, concepts, territorial scope of each regulation, governmental data protection authorities, how the collection and processing of data from minors is handled, and which rights the regulations guarantee to data holders, mainly access, rectification and erasure of collected data. The objective of the research was to identify similarities and differences between the three regulations and evaluate their effectiveness in protecting personal data. The results indicate that, despite cultural and legal divergences between regions, there is a growing trend towards standardization of data protection standards, aiming for greater security and transparency in the processing of personal information. It is concluded that the CCPA entails punishments considered light in comparison to the LGPD and GDPR, which are more comprehensive and stricter in their sanctions. Harmonization of these standards can facilitate international trade and promote data protection on a global scale, although significant challenges remain in implementing these policies.

Keywords*: Data Protection, LGPD, GDPR, CCPA, Comparative Law.*

SUMÁRIO

INTRODUÇÃO

O primeiro instrumento normativo sobre proteção de dados surgiu no âmbito da União Europeia. Conforme o site da Comissão Europeia, o *General Data Protection Regulation* (GDPR) – regulamento 679, de 23.05.2016 do conselho e do parlamento europeu, que foi publicado em 24.05.2016, cujo texto retificado no Jornal Oficial da União Europeia de 23 de maio de 2018, e que se tornou aplicável desde 25 de maio de 2018 (Comissão Europeia, 2024). A GDPR versa sobre a proteção de pessoas físicas e jurídicas no que diz respeito ao tratamento de dados pessoais e sobre a livre circulação de tais dados (Portugal: Centro Nacional de Cibersegurança, 2020).

O GDPR constituiu esforço governamental essencial para maior proteção dos direitos fundamentais das pessoas na era digital e facilitar a atividade empresarial, mediante a padronização das normas aplicáveis às empresas e aos organismos públicos no mercado único digital, aplicando-se a empresas e organismos estatais que operem no âmbito dos países integrantes da União Europeia, configurando ato legislativo único que encerrou a coexistência de sistemas nacionais diversos, díspares e dispersos (Comissão Europeia, 2024).

Inspirada na GDPR, a LGPD do Brasil - Lei geral de proteção de dados (BRASIL, 2018). Embora a lei tenha sido publicada no DOU (diário oficial da união) de 15.8.2018, trouxe previsão de *vacatio legis* no artigo 65, de modo que entrou em vigor em sua integralidade 24 meses depois de sua publicação. Na forma do art. 1º, esta Lei 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/física.

Vale lembrar aqui a distinção entre lei federal e lei nacional[4]. A Lei n.º 13.709/2018, no parágrafo único do art. 1º, indica que as normas gerais contidas nesta Lei são de interesse

[4] A lei nacional é aquela que atinge os três entes federados: União, Estados e Municípios. Já a lei federal é aquela que tem aplicação restrita ao âmbito federal, como é o caso paradigmático da lei que incide sobre o funcionário federal. Ambas são de competência do Congresso Nacional e, formalmente, identificam-se. (Brasil: Câmara Dos Deputados, 2024).

nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios, disposição que a qualifica como lei nacional.

Diversamente do Brasil e da União Europeia, os Estados Unidos da América ainda buscam unificar a legislação sobre a Proteção de Dados Pessoais, dada a variedade de leis estaduais e federais que regem o tema, na maioria das vezes por setor: saúde, finanças, telecomunicações (Gatefy, 2020) e criança e adolescente.

Uma pesquisa feita nos Estados Unidos mostrou que 87% (oitenta e sete por cento) das pessoas acreditam que a privacidade de dados é um direito humano e que 56% (cinquenta e seis por cento) dos cidadãos estadunidenses querem ter mais controle sobre os seus dados pessoais, além de que metade da população não confia nas empresas para coletar e proteger seus dados pessoais (JUNQUEIRA, 2020). Isso mostra a importância do tema, que se reputa mundial/global.

O *California Consumer Privacy Act* de 2018 (CCPA) foi promulgada em 1º de janeiro de 2020, mas só entrou em vigor em 1º de julho de 2020 marcou a primeira lei abrangente de privacidade estadual dos Estados Unidos da América e vale frisar que vários outros Estados do país publicaram leis de proteção de dados, entre eles, Virgínia, Colorado, Texas, Indiana, Minesota, Nebrasca, Nova Jersey e Oregan, as quais serão mencionadas e referenciadas no desenvolvimento do presente artigo (Onetrust DataGuindance, 2024).

Objetiva-se compreender os principais conceitos, princípios, âmbito territorial, autoridade nacional de proteção de dados, sujeitos envolvidos (controlador, encarregado e operador de dados) e responsabilidade civil, penal e administrativa pelos vazamentos de dados, na lei brasileira, confrontando com normas internacionais que regem o tema, em especial a Resolução da União Europeia e leis estadunidenses que versam sobre o mesmo tema, abordando criticamente as normas indicando eventuais pontos fracos e/ou de não efetividade.

Para tal desiderato, consultar-se-á a lei brasileira, a resolução da União Europeia, e se fará consulta a julgado do Tribunal de Justiça Europeu que aplicou normas relativas ao sigilo e tratamento de dados, bem como do STF-Supremo Tribunal Federal (tema 786 de repercussão geral que buscou compatibilizar, nesses casos, os princípios constitucionais da liberdade de

expressão e do direito à informação com aqueles que protegem a dignidade da pessoa humana e a inviolabilidade da honra e da intimidade).

Buscar-se-á apoio nos textos originais e nos comentários aos artigos das normas confrontadas, do estudo de casos, e da revisão bibliográfica especializada, consulta aos sites do Tribunal de Justiça Europeu, do STF, da União Europeia, do planalto, do CCPA, entre outros.

2 ÂMBITO TERRITORIAL DAS NORMAS ANALISADAS:

A LGPD em seu artigo 3º dispõe que se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, mas: I - a operação de tratamento tem que ser realizada no território nacional, excetuados os dados 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 na aludida Lei; II - a atividade de tratamento tem que ter por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tem que ter sido coletados no território nacional.

O § 1º, do art. 3º afirma que se consideram coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

Já a *GDPR* é aplicada a empresas que atuam na União Europeia, independentemente de o tratamento ocorrer dentro ou fora da União Europeia. O art. 3º dispõe que se aplica ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União. O item 2 afirma que o regulamento se aplica ao tratamento de dados pessoais de titulares residentes no território da União, mesmo que efetuado por agente de tratamento não estabelecido na UE, quando as atividades de tratamento estejam relacionadas com a oferta de bens ou serviços a titulares de dados na UE, mediante pagamento ou não, e o controle do seu comportamento, desde que esse comportamento tenha lugar na União Europeia.

Prevê ainda o item 3, do art. 3º, da GDPR que o regulamento se aplica ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido no território da União Europeia, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público.

Aplicando o critério da especialidade a União Europeia editou Diretiva (UE) 2016/680, a qual objetiva garantir proteção de dados pessoais das vítimas, testemunhas e dos suspeitos de

crimes, bem como facilitar a cooperação transnacional na luta contra a criminalidade e o terrorismo, possuindo como destinatários os responsáveis pela aplicação do direito penal, assim como as autoridades policiais ou judiciárias e entrou em vigor em 5 de maio de 2016, tendo estabelecido a obrigação de os países do bloco incorporar ao direito interno até 6 de maio de 2018 (Parlamento Europeu, 2024).

Nos Estados Unidos da América, não há uma legislação federal específica que corresponda diretamente à LGPD (Lei Geral de Proteção de Dados), sendo comum a existência de leis federais que regem temas por setor (saúde, finanças e telecomunicações) e criança e adolescente. Por exemplo, a *Children's Online Privacy Protection Rule* (*COPPA*) regulamenta o uso e a coleta de informações relacionadas a crianças menores de 13 anos sem consentimento dos pais (Federal Trade Commission, 2024). Essa lei será melhor detalhada abaixo que se fará a comparação das regras que detalham a coleta de dados de incapazes no Brasil, União Europeia e nos Estados Unidos da América.

Em face da ausência de norma federal abrangente, como se fez no Brasil por meio da LGPD, nos Estados Unidos da América a regulamentação da privacidade acabou sendo feita pelos Estados. A promulgação do *California Consumer Privacy Act* de 2018 (*CCPA*) em 1º de janeiro de 2020 com data de aplicabilidade em 1º de julho de 2020 marcou a primeira lei abrangente de privacidade estadual dos EUA (Onetrust DataGuidance, 2024).

A lei da Califórnia (*CCPA*) não se limita a entidades que possuem operações físicas na Califórnia, pois se aplica a entidades que "façam negócios" no estado e que: a) A receita bruta anual é superior a US $ 25 milhões ou; b) Anualmente compre, receba para fins comerciais, venda ou compartilhar para fins comerciais informações pessoais de 50.000 ou mais consumidores, famílias ou dispositivos ou; c) obtenha 50% ou mais de suas receitas anuais da venda de informações pessoais de consumidores da Califórnia ou; d) A CCPA também se aplica a qualquer entidade que (1) controle, ou é controlada por uma empresa que atende aos critérios acima, e (2) compartilha uma marca comum com essa empresa (Bakerlaw, 2020).

Somente residentes da Califórnia têm direitos tutelados pela CCPA, de modo que um residente da Califórnia, pessoa física, pode se opor a uma corporação ou outra entidade empresarial com base no Estado que colete e faça o tratamento dos dados pessoais desse

cidadão, mesmo que este esteja temporariamente fora do estado" (Departamento de Justiça Do Estado da Califórnia, 2024).

A lei da Califórnia tem destinatários restritos a um porte financeiro definido, enquanto que o Regulamento Europeu e a lei brasileira se aplicam a todas as pessoas e empresas, independente do porte econômico, que façam o tratamento de dados pessoais que possa refletir/prejudicar pessoas localizadas em seu território (URUPÁ, 2020). Após o CCPA, vários estados publicaram suas leis, como indicado no quadro abaixo:

Datas de entrada em vigor **(Onetrust DataGuindance, 2024)**

Estado	Lei	Entrada em vigor
Califórnia	Lei de Privacidade do Consumidor da Califórnia de 2018, conforme alterada (CCPA, conforme alterada)	Vigente
Virgínia	Lei de Proteção de Dados do Consumidor (CDPA)	Vigente
Colorado	Lei de Privacidade do Colorado (CPA)	Vigente
Connecticut	Lei de Connecticut sobre privacidade de dados pessoais e monitoramento on-line (CTDPA)	Vigente
Utah	Lei de Privacidade do Consumidor (UCPA)	Vigente
Texas	Lei de Privacidade e Segurança de Dados do Texas (TDPSA)	Vigente
Flórida	Declaração de Direitos Digitais da Flórida (FDBR)	Vigente
Oregon	Lei de Privacidade do Consumidor do Oregon (OCPA)	Vigente
Montana	Lei de Privacidade de Dados do Consumidor (MCDPA)	1 de outubro de 2024
Iowa	Lei de Proteção de Dados do Consumidor de Iowa (ICDPA)	1 de janeiro de 2025
Delaware	Lei de Privacidade de Dados Pessoais de Delaware (DPDPA)	1 de janeiro de 2025
Nebrasca	Lei de Privacidade de Dados (NEDPA)	1 de janeiro de 2025
Nova Hampshire	Uma Lei relativa à expectativa de privacidade (NHCDPA)	1 de janeiro de 2025
Nova Jersey	Uma lei relativa a sites comerciais da Internet, serviços online, consumidores e informações de identificação pessoal (NJDPA)	15 de janeiro de 2025
Tennessee	Lei de Proteção de Informações do Tennessee (TIPA)	1 de julho de 2025
Minnesota	Lei de Privacidade de Dados do Consumidor de Minnesota (MCDPA)	31 de julho de 2025
Maryland	Lei de Privacidade de Dados Online de Maryland (MODPA)	1 de outubro de 2025
Indiana	Lei de Proteção de Dados do Consumidor (ICDPA)	1 de janeiro de 2026
Kentucky	Lei de Proteção de Dados do Consumidor de Kentucky (KCDPA)	1 de janeiro de 2026

Rhode Island	Lei de Transparência de Dados e Proteção de Privacidade de Rhode Island (RIDTPPA)	1 de janeiro de 2026

Como regra geral, as normativas continuam aplicáveis caso a empresa que coleta e trata e os dados pessoais esteja sediada fora do âmbito territorial da norma, mas possa afetar cidadãos brasileiros, europeus ou californianos.

3 CONCEITOS ESPECÍFICOS DAS TRÊS NORMAS DE PROTEÇÃO DE DADOS

As normas de proteção de dados pessoais procuram determinar a maneira como empresas e organizações devem tratar dados pessoais, as quais normatizam como empresas devem coletar, processar, compartilhar e fazer uso das informações pessoais naturais com quem tiveram relação jurídica. De acordo com o Ibi Jus:

> A Proteção de Dados Pessoais é a área do direito que mais se desenvolve no mundo na atualidade. A transformação digital é realidade cada vez mais presente nas vidas das pessoas e das empresas. Os dados são o novo petróleo. A proteção da privacidade e dos dados pessoais é tema que ocupará a sociedade com importância crescente nas próximas décadas (Instituto Brasileiro de Direito, 2020).

A Lei n.º 13.709, de 14.08.2018 – Lei Geral de Proteção de Dados do Brasil, teve vigência fragmentada, na forma do Art. 65: I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos.

O Art. 2º da lei de proteção de dados do Brasil dispõe que a disciplina da proteção de dados pessoais tem como fundamentos: a - o respeito à privacidade; b - a autodeterminação informativa; c - a liberdade de expressão, de informação, de comunicação e de opinião; d - a inviolabilidade da intimidade, da honra e da imagem; e - o desenvolvimento econômico e tecnológico e a inovação; f - a livre iniciativa, a livre concorrência e a defesa do consumidor; e g - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

> O direito à proteção de dados pessoais, por sua vez, origina-se posteriormente ao direito à privacidade. É resultado da sociedade da informação. Com o surgimento de computadores e, em seguida, bancos de dados, o controle sobre a informação – e, em especial, dados pessoais – passa a ser visto como uma forma de poder. A preocupação com a proteção de dados pessoais deriva da percepção da amplitude e potencialidade de controle e manipulação sobre a sociedade e o mercado que este tipo de dado oferece (VERGILI, 2019).

A lei preserva os direitos da personalidade das pessoas físicas titulares dos dados/informações, mas tenta harmonizar com as atividades econômicas desenvolvidas por pessoas e empresas ligadas ao setor de informação e comunicação (LGPD, art. 2º, III - a liberdade de expressão, de informação, de comunicação e de opinião); do setor de TI (LGPD, art. 2º, V - o desenvolvimento econômico e tecnológico e a inovação; e do setor empresarial em geral (LGPD, art. 2º, VI - a livre iniciativa, a livre concorrência e a defesa do consumidor).

A "ARTICLE 19", Organização não governamental (ONG) atuou em favor do GOOGLE no julgamento perante o Tribunal de Justiça da União Europeia (TJUE), relacionado ao "**Direito ao esquecimento**", propôs um rigoroso filtro/teste de sete partes para balancear os direitos dos titulares dos dados e o dos provedores, buscadores, operadores (de acordo com o conceito do art. 5º, VII, da LGPD do Brasil): a) Se a informação em questão é de natureza privada; b) se o requerente tinha uma expectativa razoável de privacidade, incluindo a consideração de questões como a conduta anterior, autorização para publicação ou prévia existência da informação em domínio público; c) Se as informações em causa são de interesse público; d) se as informações em causa se referem a uma figura pública; e) se a informação é parte do registro público; f) se o requerente demonstrou danos substanciais; g) o quão recente é a informação e se mantém o valor de interesse público (Article 19, 2016, p. 02);

Essa publicação da ONG sustenta que o direito não tem incidência quando a informação tiver natureza pública, interesse público, for parte de registro público, partir de autorização do requerente ou de banco de dados de domínio público que restou apenas impulsionado pelo "motor de busca" (Article 19, 2016, p. 02) e que são informações de natureza privada, entre outras: a) detalhes de sua vida íntima ou sexual; b) informação sobre a sua saúde; c) informações bancárias ou detalhes de pagamento de contas (tais como números de cartão); d) contato privado ou informações de identificação, incluindo PINs ou senhas, passaporte ou números de segurança social; e) outras informações sensíveis, tais como a filiação sindical, origem racial

ou étnica, opiniões políticas ou crenças religiosas ou filosóficas também poderiam ser consideradas privadas (Article 19, 2016, p. 23-25).

As informações são tidas como de natureza pública quando se referirem a política, saúde e segurança pública; aplicação da lei e da administração da justiça; dos consumidores e dos interesses sociais; meio ambiente; questões econômicas; os exercícios de poder; arte e cultura (Article 19, 2016, p. 23-25).

Seguindo a inspiração da GDPR da União Europeia (art.4º), a lei brasileira destaca dispositivo (art. 5º) em que as expressões são conceituadas e delimitadas, de modo a trazer segurança jurídica e facilidades ao intérprete.

Dessa forma, segue definições trazidas pelo legislador brasileiro - LGPD, nos incisos do art. 5º, comparado com a GDPR, que traz as definições no art. 4º, e com o CCPA, que traz as definições n.º 1798.140:

I - **dado pessoal**: informação relacionada a pessoa natural identificada ou identificável. Conceito idêntico ao da GDPR (art. 4º, item 1). Entretanto, vale ressaltar que a GDPR também protege os dados de pessoa jurídica. A doutrina alude a visão reducionista (pessoa identificada) ou expansionista (pessoa não identificada), que nas duas normativas é igual.

> Na linha expansionista, ambas as informações de uma pessoa identificada e identificável seriam consideradas dados pessoais, e estariam assim abarcadas pelos institutos legais que visam a proteger esse bem jurídico. A pessoa relacionada ao dado pode ser indeterminada, e o vínculo com seus dados pode ser "mediato, indireto, impreciso ou inexato", nas palavras de Bruno Bioni.
> Já na linha reducionista, os dados pessoais seriam apenas as informações de uma pessoa identificada. Ela se torna, portanto, uma pessoa específica e determinada por essas informações, com as quais se estabelece um vínculo "imediato, direto, preciso ou exato" (GOMES, 2022).

Na forma do CCPA, informações pessoais são informações que identificam uma pessoa ou permita identificação da pessoa ou sua família. Nesse conceito se enquadram seu nome, número de previdência social, endereço de e-mail, registros de produtos comprados, histórico de navegação na internet, dados de geolocalização, impressões digitais e inferências de outras informações pessoais que podem criar um perfil sobre suas preferências e características (Departamento de Justiça do Estado da Califórnia, 2024).

II – **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. Esse conceito incorpora conceitos trazidos no art. 4º, da GDPR, nos incisos 13 (dados genéticos), 14 (dados biométricos), 15 (dados relativos à saúde).

No CCPA, as "informações pessoais sensíveis" são espécies de informações pessoais que incluem certos identificadores governamentais (como números de previdência social); um login de conta, conta financeira, cartão de débito ou número de cartão de crédito com qualquer código de segurança, senha ou credenciais necessárias que permitam acesso a uma conta; geolocalização precisa; conteúdo de correspondência, e-mail e mensagens de texto; dados genéticos; informações biométricas processadas para identificar um consumidor; informações sobre a saúde, vida sexual ou orientação sexual de um consumidor; ou informações sobre origem racial ou étnica, crenças religiosas ou filosóficas ou filiação sindical (Departamento de Justiça do Estado da Califórnia, 2024).

III - **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.

A GDPR chama de "pseudonimização" no item 5, do art. 4º e conceitua como o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

Tanto no CCPA, quanto na GDPR, o processo de anonimizar dados é chamado de "pseudominização" e tem como produto o dado pseudominizado, chamado no Brasil de "dado anonimizado".

De acordo com o CCPA, (aa) "Pseudonimizar" ou "Pseudonimização" significa o processamento de informações pessoais de uma maneira que as torne não mais atribuíveis a um consumidor específico sem o uso de informações adicionais, desde que as informações

adicionais sejam mantidas separadamente e estejam sujeitas a medidas técnicas e organizacionais para garantir que as informações pessoais não sejam atribuídas a um consumidor identificado ou identificável.

IV - **banco de dados**: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico. A GDPR chama de "ficheiro" (item 6 do art. 4º).

No CCPA n.º 1798.140. Definições: (b) "Informações agregadas do consumidor" significa informações que se relacionam a um grupo ou categoria de consumidores, dos quais identidades individuais do consumidor foram removidas, que não estão vinculadas ou razoavelmente vinculáveis a nenhum consumidor ou domicílio, inclusive por meio de um dispositivo. "Informações agregadas do consumidor" não significa um ou mais registros individuais do consumidor que foram desidentificados.

V - **titular**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular (art. 4º, 1, GDPR). No CCPA, o titular dos dados é chamado de "consumidor", pois a lei tem o fim de proteger os dados dentro de relações de consumo.

VI - **controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O item 7 do art. 4º, da GDPR chama de "responsável pelo tratamento".

VII - **operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O item 8 do art. 4º, da GDPR chama de "subcontratante".

IX - **agentes de tratamento**: o controlador e o operador;

X - **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.

Na forma do item 2 do art. 4º, do Regulamento Europeu, entende-se por «**Tratamento de Dados**», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

De acordo com a GDPR, em seu considerando n.º 24, uma atividade de tratamento de dados é considerada "controle de comportamento" dos titulares de dados, se eles são seguidos na Internet e se as técnicas de tratamento de dados pessoais implicarem na definição de perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes.

No CCPA, item (z), a "Criação de perfil" significa qualquer forma de processamento automatizado de informações pessoais, conforme definido por regulamentos de acordo com o parágrafo (16) da subdivisão (a) da Seção 1798.185, para avaliar certos aspectos pessoais relacionados a uma pessoa física e, em particular, para analisar ou prever aspectos relativos ao desempenho dessa pessoa física no trabalho, situação econômica, saúde, preferências pessoais, interesses, confiabilidade, comportamento, localização ou movimentos.

Ainda na CCPA no setor relacionado às definições a coleta de dados é apresentada do seguinte modo: (f) "Coleta", "coletado" ou "coleta" significa comprar, alugar, reunir, obter, receber ou acessar qualquer informação pessoal pertencente a um consumidor por qualquer meio. Isso inclui receber informações do consumidor, ativa ou passivamente, ou observando o comportamento do consumidor.

XI - **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. A GDPR chama de Pseudonimização (item 5 do art. 4º), mesma nomenclatura utilizada no CCPA.

XII - **consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. O consentimento para o tratamento de dados só pode ser dado no Brasil por aqueles que tenha plena capacidade civil (18 anos ou mais).

Corresponde ao art. 7º, da GDPR (Condições aplicáveis ao consentimento). No regulamento europeu o consentimento para o tratamento de dados pode ser dado a partir dos 16 anos de idade.

No CCPA, há um extenso conceito de consentimento, no qual traz as condições gerais de sua validade: (h) "Consentimento" significa qualquer indicação livremente dada, específica, informada e inequívoca dos desejos do consumidor pela qual o consumidor, ou o responsável legal do consumidor, uma pessoa que tenha procuração, ou uma pessoa agindo como conservador do consumidor, incluindo por uma declaração ou por uma ação afirmativa clara, significa concordância com o processamento de informações pessoais relacionadas ao consumidor para um propósito específico estritamente definido. A aceitação de termos de uso gerais ou amplos, ou documento semelhante, que contenha descrições de processamento de informações pessoais junto com outras informações não relacionadas, não constitui consentimento. Passar o mouse sobre silenciar, pausar ou fechar um determinado conteúdo não constitui consentimento. Da mesma forma, o acordo obtido por meio do uso de padrões escuros não constitui consentimento.

XIII - **bloqueio**: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados. O Artigo 18, da GDPR traz o direito à limitação do tratamento de dados pessoais e o art. 21, o direito à oposição ao tratamento de dados por parte de seu titular.

Na CCPA, você pode solicitar que as empresas parem de vender ou compartilhar suas informações pessoais (*opt-out*) (Departamento de Justiça do Estado da Califórnia, 2024).

XIV - **eliminação**: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado. Corresponde ao art. 17, da GDPR (Direito ao apagamento dos dados - direito a ser esquecido).

No CCPA, o consumidor pode solicitar que as empresas excluam as informações pessoais que coletaram e que informem aos seus provedores de serviço para que tomem a mesma providência. No entanto, há muitas exceções (veja FAQ D.5) que permitem que as empresas mantenham suas informações pessoais (Departamento de Justiça do Estado da Califórnia, 2024).

XV - **transferência internacional de dados**: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro. Corresponde ao item 23 do art. 4º, da GDPR, chamado de tratamento transfronteiriço.

XVI - **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;

XVII - **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;

XVIII - **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. Se assemelha aos serviços da sociedade da informação (art. 4º, item 25, da GDPR).

XIX - **autoridade nacional**: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. A GDPR chama de autoridade de controle (art. 4º, item 21) e este ponto será abordado especificamente a seguir.

4 AUTORIDADES GOVERNAMENTAIS DE PROTEÇÃO DE DADOS NA LGPD, GDPR E NO CCPA

A lei brasileira, em seu art. 5º, inciso XIX esclarece que a autoridade nacional é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

De acordo com o Decreto n.º 10.474, de 26 de agosto de 2020, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança, dentre outras competências, caberá à Autoridade Nacional de Proteção de Dados (art. 2º): a) Regulamentar a Lei Geral de Proteção de Dados; b) Fiscalizar o cumprimento da legislação de proteção de dados pessoais, com vistas a proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural; c) Elaborar as diretrizes do Plano Nacional de Proteção de Dados com a finalidade de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural; e d) Aplicar sanções administrativas, após os respectivos dispositivos entrarem em vigor em agosto de 2021 e a matéria ser regulamentada, considerando as contribuições de consulta pública (Brasil, 2020).

A ANPD é uma autarquia de natureza especial, vinculada ao Ministério da Justiça e Segurança Pública. A estrutura do órgão foi estabelecida no decreto mencionado supra e adveio de: a) Remanejamento de 16 cargos em comissão e 20 funções comissionadas do Poder Executivo (FCPE) da Secretaria de Gestão (SEGES) para a ANPD; b) Organização da ANPD como órgão da Presidência, de acordo com a LGPD; c) Estabelecimento de competências da

ANPD, de acordo com a LGPD; e d) Fixação dos órgãos da ANPD com respectivas competências, de acordo com a LGPD (Brasil, 2020);

O Comitê Europeu para a Proteção de Dados (CEPD) é um organismo europeu independente que assegura a aplicação coerente das regras de proteção de dados em toda a União Europeia e os países da União Europeia criaram organismos nacionais responsáveis pela proteção de dados pessoais, em conformidade com o artigo 8.º, n.º 3, da Carta dos Direitos Fundamentais da União Europeia (Comissão Europeia, 2024).

O enfrentamento interno nos países componentes da União Europeia do tratamento indevido de dados pessoais foi o objetivo do regulamento ao criar as "autoridades de controle independentes" nos artigos 51, 55 e 56. Dentro dos países, cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação do regulamento, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União (autoridade de controle), conforme artigo 51.

Sem prejuízo do disposto no artigo 55.º, da Resolução 679/2016 da EU, a autoridade de controle do estabelecimento principal ou do estabelecimento único do responsável pelo tratamento ou do subcontratante é competente para agir como autoridade de controlo principal para o tratamento transfronteiriço efetuado pelo referido responsável pelo tratamento ou subcontratante nos termos do artigo 60º (art. 55, item 1).

As autoridades de controle na União Europeia dispõem de **poderes de investigação**, indicado no item 1 do Art. 58: a) Ordenar que os responsáveis lhe forneçam as informações de que necessite para o desempenho das suas funções; b) Realizar investigações sob a forma de auditorias sobre a proteção de dados; c) Rever as certificações emitidas nos termos do artigo 42º, n.º 7; d) Notificar o responsável pelo tratamento ou o subcontratante de alegadas violações do presente regulamento; e) Obter acesso a todos os dados pessoais e a todas as informações necessárias ao exercício das suas funções; f) Obter acesso a todas as instalações do responsável pelo tratamento e do subcontratante, incluindo os equipamentos e meios de tratamento de dados, em conformidade com o direito processual da União ou dos Estados-Membros.

Cada autoridade de controlo dos países membros da União Europeia dispõe dos seguintes **poderes de correção**: a) fazer advertências ao responsável pelo tratamento de dados ou ao subcontratante quando as operações de tratamento forem suscetíveis de violar as disposições do presente regulamento; b) fazer repreensões ao responsável pelo tratamento ou ao subcontratante sempre que as operações de tratamento tiverem violado as disposições do presente regulamento; c) Ordenar ao responsável pelo tratamento ou ao subcontratante que satisfaça os pedidos de exercício de direitos apresentados pelo titular dos dados nos termos do presente regulamento; d) Ordenar aos agentes de tratamento de dados que tome medidas para que as operações de tratamento cumpram as disposições do presente regulamento e, se necessário, de uma forma específica e dentro de um prazo determinado; e) Ordenar ao responsável pelo tratamento que comunique ao titular dos dados uma violação de dados pessoais; f) Impor uma limitação temporária ou definitiva ao tratamento de dados, ou mesmo a sua proibição; g) Ordenar a retificação ou o apagamento de dados pessoais ou a limitação do tratamento nos termos dos artigos 16º, 17º e 18º, bem como a notificação dessas medidas aos destinatários a quem tenham sido divulgados os dados pessoais nos termos do artigo 17º, n.º 2, e do artigo 19º; h) Retirar a certificação ou ordenar ao organismo de certificação que retire uma certificação emitida nos termos dos artigos 42º e 43º, ou ordenar ao organismo de certificação que não emita uma certificação se os requisitos de certificação não estiverem ou deixarem de estar cumpridos; i) Impor uma coima nos termos do artigo 83º, para além ou em vez das medidas referidas no presente número, consoante as circunstâncias de cada caso; j) Ordenar a suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais.

Ainda de acordo com o item 3, do art. 58, da GDPR, as autoridades nacionais e controle de dados possuem **competências consultivas e de autorização**: a) Aconselhar o responsável pelo tratamento, pelo procedimento de consulta prévia referido no artigo 36º; b) Emitir, por iniciativa própria ou se lhe for solicitado, pareceres dirigidos ao Parlamento nacional, ao Governo do Estado-Membro ou, nos termos do direito do Estado-Membro, a outras instituições e organismos, bem como ao público, sobre qualquer assunto relacionado com a proteção de dados pessoais; c) Autorizar o tratamento previsto no artigo 36º, n.º 5, se a lei do Estado-Membro exigir tal autorização prévia; d) Emitir pareceres e aprovar projetos de códigos de

conduta nos termos do artigo 40º, n.º 5; e) Acreditar organismos de certificação nos termos do artigo 43º; f) Emitir certificações e aprovar os critérios de certificação nos termos do artigo 42º, n.º 5; g) Adotar as cláusulas-tipo de proteção de dados previstas no artigo 28º, n.º 8, e no artigo 46º, n.º 2, alínea d); h) Autorizar as cláusulas contratuais previstas no artigo 46º, n.º 3, alínea a); i) Autorizar os acordos administrativos previstos no artigo 46º, n.º 3, alínea b); j) Aprovar as regras vinculativas aplicáveis às empresas nos termos do artigo 47º.

Na forma do item 5 do art. 58, da GDPR, os Estados-Membros estabelecem por lei que as suas autoridades de controle estão habilitadas a levar as violações de seus preceitos ao conhecimento das autoridades judiciais e, se necessário, a intentar ou de outro modo intervir em processos judiciais, a fim de fazer aplicar as disposições do presente regulamento.

Frise-se que sem prejuízo das autoridades nacionais ainda existe a autoridade no âmbito do Bloco (UE). A AEPD - Autoridade Europeia para a Proteção de Dados - é um organismo independente da União Europeia, responsável pelo controle da aplicação das regras no que diz respeito à proteção de dados no interior das instituições europeias e pela investigação de reclamações, enquanto que o "Encarregado da proteção de dados na Comissão Europeia" é responsável pelo controle da aplicação interna das regras em matéria de proteção de dados, em cooperação com a Autoridade Europeia para a Proteção de Dados (Comissão Europeia, 2024).

De agora em diante, buscar-se-á indicar o papel instituído pela Lei brasileira para a autoridade nacional de proteção de dados.

Na forma do art. 4º, III e § 3º, a autoridade nacional emitirá opiniões técnicas ou recomendações referentes ao tratamento de dados relativos a segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais. Vale ressaltar que os dados relativos aos temas mencionados serão objetos de legislação específica e não podem ser tratados por pessoas físicas como determinam os § § 1º e 2º, da LGPD.

A autoridade nacional tem importantes funções regulamentadoras: a) dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais (§ 3º, do art. 12); b) o acesso aos dados necessários a realização de estudos na área da saúde pública será objeto

de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências (§ 3º, do art. 13); c) regulamentação da portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, observados os segredos comercial e industrial (art. 18, V, da LGPD).

Dentre as funções da autoridade nacional de proteção de dados estão a determinação do encerramento do tratamento de dados (art. 15, IV) e o recebimento de petições do titular dos dados contra o controlador (§ 1º, do art. 18).

Sem dúvida, que o papel mais destacado da autoridade nacional é a aplicação de sanções aos agentes de tratamento de dados, quais sejam (art. 52): I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; VII – IX – vetados; X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

No CCPA, há previsão de uma Agência Estadual de Proteção de dados no número 1798.155. Execução Administrativa, onde restou disposto que (EUA: Califórnia, 2018): (a) Qualquer empresa, prestador de serviços, empreiteiro ou outra pessoa que viole este título será responsável por uma multa administrativa de não mais de dois mil e quinhentos dólares (US$ 2.500) por cada violação ou sete mil e quinhentos dólares (US$ 7.500) para cada violação intencional ou violações envolvendo informações pessoais de consumidores que a empresa, prestador de serviços, contratante ou outra pessoa tenha conhecimento real têm menos de 16 anos de idade, conforme ajustado de acordo com o parágrafo (5) da subdivisão (a) da Seção

1798.185, em ação administrativa movida pela **Agência de Proteção à Privacidade da Califórnia**. (b) Qualquer multa administrativa aplicada por violação deste título, e o produto de qualquer resolução de uma ação movida de acordo com a subdivisão (a), serão depositados no Fundo de Privacidade do Consumidor, criado dentro do Fundo Geral de acordo com a subdivisão (a) da Seção 1798.160 com a intenção de compensar totalmente quaisquer custos incorridos pelos tribunais estaduais, pelo Procurador-Geral e pela Agência de Proteção à Privacidade da Califórnia em conexão com este título.

5 DADOS DE CRIANÇAS E ADOLESCENTES NO CCPA, LDPD E GDPR

Nos Estados Unidos, a *Children's Online Pivacy Protection Act* (COPPA), lei federal que regulamenta o uso e a coleta de informações relativas a menores de 13 anos sem o consentimento dos pais (ConectaJá.Proteste, 2024).

Acerca dessa lei se encontra no site do INC.com (Inc., 2020): a) O *Children's Online Privacy Protection Act (COPPA)* é uma lei federal dos EUA criada para limitar a coleta e o uso de informações pessoais sobre crianças – menores de 13 anos de idade - pelos operadores de serviços de Internet e sites; b) aprovada pelo Congresso dos EUA em 1998, a lei entrou em vigor em abril de 2000; c) ela é implementada pela Federal Trade Commission (FTC); d) A COPPA é "a primeira lei de privacidade dos EUA escrita para a Internet"/ e) ela foi escrita especificamente para profissionais de marketing da Internet que operam sites visitados por crianças menores de 13 anos e coletam informações pessoais dessas crianças; f) Seu propósito é regular essa coleta; g) Ao determinar se um site é direcionado a crianças, a FTC considerará, entre outras coisas, o conteúdo do site, a linguagem, a publicidade e o público-alvo, bem como o uso de gráficos ou recursos voltados para crianças; h) a COPPA exige que os operadores desses tipos de sites incluam um aviso de privacidade claramente escrito em sua página inicial e em qualquer lugar do site onde os dados do usuário são coletados; i) a política de privacidade deve revelar quem está coletando e mantendo as informações que as crianças fornecem ao site e fornecer informações sobre como contatá-las; explicar como as informações pessoais das crianças serão usadas; e declarar se serão disponibilizadas a terceiros; j) exige que os operadores

de sites obtenham "consentimento parental verificável" antes de coletar ou usar informações pessoais de crianças; k) mesmo quando o consentimento parental foi concedido uma vez, os operadores do site devem buscar o consentimento novamente sempre que fizerem alterações em suas políticas de privacidade; m) exceções aos requisitos de consentimento parental da COPPA são permitidas para a coleta de endereços de e-mail para buscar consentimento, proteger a segurança de uma criança ou responder a uma solicitação única de uma criança (desde que o endereço de e-mail seja excluído imediatamente depois); n) a FTC aplica penalidades por não conformidade que variam até US$ 11.000 por incidente.

A Lei brasileira dispõe em seu artigo 14, caput, § 1º que: O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse e deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. O controlador de dados deve realizar todos os esforços razoáveis para verificar que o consentimento foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis (§5º).

O § 2º, do art. 14, da LGPD, dispõe que no tratamento de dados de crianças e adolescente, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 (informação sobre a existência de tratamento, acesso aos dados, correção de dados, anonimização, bloqueio ou eliminação de dados, portabilidade, quais as entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa, revogação do consentimento).

O § 3º, do art. 14, da LGPD, assevera que poderão ser coletados dados pessoais de crianças sem consentimento quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º do mesmo artigo.

Os controladores não deverão condicionar a participação de crianças e adolescentes em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade, como regulamenta o § 4º, do art. 14, da LGPD.

Na forma do § 6º, do art. 14, da LGPD indica que as informações sobre o tratamento de dados de crianças e adolescente deverão ser fornecidas de maneira simples, clara e acessível, de acordo com as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, através da utilização de recursos audiovisuais quando couber, da forma mais eficiente para manter pais e responsáveis legais cientes e proporcionar a compreensão da criança.

Na GDPR, o tratamento de dados de incapazes é regulado no artigo 8º: a) quando o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas, no que respeita à oferta direta de serviços da sociedade da informação às crianças, o consentimento para o tratamento dos dados pessoais de incapazes é lícito se elas tiverem pelo menos 16 anos; b) Caso a pessoa tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança; c) os Estados-Membros da União Europeia podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos; d) o responsável pelo tratamento dos dados deve envidar todos os esforços adequados para verificar que o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais da criança, tendo em conta a tecnologia disponível; e) essas disposições não afetam o direito contratual geral dos Estados-Membros, como as disposições que regulam a validade, a formação ou os efeitos de um contrato em relação a um incapaz (entende-se que decorre da aplicação do princípio da especialidade, critério de solução de antinomia de regras-legais.

6 DIREITOS DO TITULAR DOS DADOS: ACESSO, RETIFICAÇÃO, APAGAMENTO

A LGPD tenta sintetizar os direitos do titular dos dados no art. 18: a) confirmação da existência de tratamento; b) acesso aos dados; c) correção de dados incompletos, inexatos ou

desatualizados; d) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; e) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; f) eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei; g) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; h) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; i) revogação do consentimento, nos termos do § 5º do art. 8º da Lei;

A lei brasileira – LGPD – traz ainda em seu artigo 19 o direito ao acesso às informações coletadas pelo operador acerca da pessoa do requerente dispondo que: a) a confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: a1) em formato simplificado, imediatamente; ou a2) por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

Dispõe ainda o artigo 19 da LGPD que os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso e serão fornecidos, a critério do titular, por meio eletrônico, seguro e idôneo para esse fim; ou na forma impressa.

Vale frisar que o Supremo Tribunal firmou precedente vinculante (tema 786 de repercussão geral) considerando inconstitucional o direito ao esquecimento, dando realce para os princípios da harmonização dos princípios constitucionais da liberdade de expressão e do direito à informação em detrimento da dignidade da pessoa humana e a inviolabilidade da honra e da intimidade (arts. 1º, III, 5º, caput, III e X, e 220, § 1º, da Constituição Federal).

Já a GDPR (EU) assegura aos titulares dos dados pessoais em detrimento das empresas que coletam, tratam e compartilham esses dados: a) Artigo 15º - Direito de acesso do titular dos dados; b) Artigo 16º - Direito de retificação; c) Artigo 17º - Direito ao apagamento dos dados («direito a ser esquecido»); d) Artigo 18º - Direito à limitação do tratamento; e) Artigo 19º -

Obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento; f) Artigo 20º - Direito de portabilidade dos dados; g) Artigos 21-22 – direito de se opor a decisões individuais automatizadas, definições de perfis.

No regulamento da União Europeia, conforme o item 1 do art. 15, o titular dos dados tem o direito de obter do responsável pelo tratamento as seguintes informações (direito de obter informações) sobre: a) as fins do tratamento dos dados; b) as categorias dos dados pessoais coletados; c) os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais; d) na medida do possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;

No regulamento da União Europeia, ainda de acordo com o item 1 do art. 15, o titular dos dados tem o direito de: a) solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento; b) O direito de apresentar reclamação a uma autoridade de controlo; c) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados; d) saber da existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22., n. 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

O direito ao esquecimento veio tratado no Regulamento da UE no art. 17. O item 1 do art. 17 dispõe que o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, tendo a empresa que fez a coleta dos dados a obrigação de apagar os dados pessoais, sem demora injustificada, quando presentes um dos seguintes motivos: a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6º, n.º 1, alínea a), ou do artigo 9º, n.º 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento; c) O titular opõe-se ao tratamento nos termos do artigo 21º, n.º 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2; d)

Os dados pessoais foram tratados ilicitamente; e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da UE ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º 1.

Na forma do item 3., do artigo 17, do Regulamento Europeu, não incide o direito ao esquecimento nas seguintes hipóteses: a) Ao exercício da liberdade de expressão e de informação; b) Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento; c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9., n.2, alíneas h) e i), bem como do artigo 9., n. 3; d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89., n.1 [pseudonimização], quando o "direito ao apagamento" seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

O titular dos dados na União Europeia tem o sagrado de direito oposição delineado no art. 21. No item 1. se lê que o titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.º, n.º 1, alínea e) ou f), ou no artigo 6.º, n.º 4, incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento deve cessar o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

O item 1 do art. 89, do Regulamento assevera que "o tratamento para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, está sujeito a garantias adequadas voltadas para a preservação dos direitos e liberdades do titular dos dados. Essas garantias asseguram a adoção de medidas técnicas e organizativas a fim de

assegurar, nomeadamente, o respeito do princípio da minimização dos dados. Essas medidas podem incluir a **pseudonimização**, desde que os fins visados possam ser atingidos desse modo. Sempre que esses fins possam ser atingidos por novos tratamentos que não permitam, ou já não permitam, a identificação dos titulares dos dados, os referidos fins são atingidos desse modo.

O CCPA assegurou aos consumidores os seguintes direitos, conforme número do item legislativo e respectivo direito assegurado: a) 1798.105. direito de excluir informações pessoais; b) 1798.106. Direito dos consumidores de corrigir informações pessoais imprecisas; c) 1798.110. Direito dos consumidores de saber quais informações pessoais estão sendo coletadas. Direito de acessar informações pessoais; d) 1798.115. Direito dos consumidores de saber quais informações pessoais são vendidas ou compartilhadas e para quem; e) 1798.120. Direito dos consumidores de cancelar a venda ou compartilhamento de informações pessoais; f) 1798.121. Direito dos Consumidores de Limitar o Uso e Divulgação de Informações Pessoais Sensíveis; g) 1798.125. Direito dos Consumidores de Não Retaliação Após *Opt Out* ou Exercício de Outros Direitos.

O item 1798.100 (direito de acesso) do CCPA conferiu ao consumidor os seguintes direitos relacionados aos seus dados pessoais: A) solicitar que uma empresa que coleta informações pessoais informe ao consumidor as categorias e peças específicas de informações pessoais que a empresa coletou; B) direito de informação advinda de uma empresa que coleta informações pessoais dos consumidores, antes da coleta, sobre as categorias de informações pessoais a serem coletadas e os fins para os quais as categorias de informações pessoais devem ser utilizadas; C) direito de evitar coleta adicional de informações pessoais ou usar informações pessoais coletadas para finalidades adicionais sem fornecer ao consumidor um aviso compatível com esta seção da lei; D) uma empresa deve fornecer as informações especificadas somente após o recebimento de uma solicitação verificável do consumidor. E) a empresa que recebe uma solicitação verificável de um consumidor para acessar informações sobre a pessoa dele deve prontamente tomar medidas para divulgar e entregar, gratuitamente a ele, as informações pessoais exigidas por esta seção (EUA: Califórnia, 2024).

CONSIDERAÇÕES FINAIS

A lei geral de proteção de dados do Brasil, LGPD, teve clara inspiração no Regulamento 679/2016 do Conselho e Parlamento Europeu, GDPR, e se trata de lei nacional, vez que aplicável em todo o território nacional e a todas as esferas de poder e a todos os entes federativos, tendo entrado em vigor em sua plenitude e totalidade 15 de agosto de 2020, 24 meses após sua publicação no diário oficial da União.

O direito à privacidade é relevante direito da personalidade e projetado internacionalmente é direito humano fundamental reconhecido como carecedor de tutela adequada ante ao forte anseio das empresas com atuação na grande rede de deter informações das pessoas naturais e com a definição de perfis fomentar atividades econômicas e práticas lucrativas.

Os cidadãos querem ter mais controle sobre os seus dados pessoais e não confiam nas empresas para coletar e proteger seus dados pessoais, os quais são constantemente tratados/reorganizados e impulsionados/cedidos para terceiros, na maioria das vezes sem o conhecimento e a autorização expressa de seus titulares.

Na forma do artigo 2º, da LGPD foram mencionados seus fundamentos, os quais possuem claramente a intenção de promover o equilíbrio entre os interesses das pessoas físicas, titulares dos dados, e das pessoas que exercem atividades ligadas à liberdade de expressão, de informação, de comunicação e de opinião, de desenvolvimento econômico, tecnológico e de inovação. O ideal do legislador é buscar um ponto de equilíbrio, em que os princípios sejam sopesados de modo a coexistirem e terem a máxima efetividade, como se faz na harmonização de princípios.

A normas explicam o que se considera tratamento de dados, a saber, 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 e diz que o controlador, responsável por essas

operações responde perante o titular, perante a autoridade nacional de controle de dados e perante o Judiciário pelos danos que vier a causar, bem como pela violação das regras de confidencialidade.

Vale frisar, por oportuno, que a Suprema Corte brasileira considerou o direito ao esquecimento (*right to be forgotten*) inconstitucional em ponderação de princípios normalmente opostos liberdade de expressão e do direito à informação *versus* dignidade da pessoa humana e a inviolabilidade da honra e da intimidade (tema 786 de repercussão geral).

Nos Estados Unidos da América, como exposto no decorrer do texto, possui legislação focada em temas/setores (saúde, relações de consumo, criança e adolescente, etc) e fragmentada entre os entes federativos (leis federais e estaduais sobrepostas). No estado da Califórnia, entrou em vigor no primeiro dia de 2020, a CCPA, a primeira Lei Estadual voltada a assegurar de privacidade dos dados do consumidor, que não se aplica a todas as empresas que realizam coleta e tratamento de dados e que traz punições tidas como leves, pela doutrina, especialmente se comparadas com a lei brasileira e o regulamento europeu que, além de trazerem tratamento unificado e completo do tema, preveem punições severas aos infratores de suas regras e princípios (v.g. LGPD prevê multa de até 50 milhões de reais no art. 52, II).

A harmonização dessas normas pode facilitar o comércio internacional e promover a proteção de dados em escala global, embora desafios significativos permaneçam na implementação dessas políticas.

REFERÊNCIAS

ARTICLE 19. **Direito ao esquecimento: Lembrando da Liberdade de Expressão**. 2016. p.02. Disponível em https://www.article19.org/data/files/medialibrary/38318/The_right_to_be_forgotten_A5_44pp_report_portuguse-pdf.pdf. Acesso em: 14 jul. 2024.

BAKERLAW. **The California Consumer Privacy Act: Frequently Asked Questions**. Disponível em https://bakerlaw.com/webfiles/Privacy/2019/Briefs/California-Consumer-Privacy-Act-FAQs.pdf. Acesso em 12.11.2020.

BRASIL. **DECRETO Nº 10.474, DE 26 DE AGOSTO DE 2020.** DOU de 27/08/2020 | Edição: 165 | Seção: 1 | Página: 6. Disponível em https://www.in.gov.br/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226. Acesso em 11.11.2020.

BRASIL. **Lei geral de proteção de dados**. Lei número 13.709 (14/08/2018), acessível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018 / Lei / L13709.htm. Acesso em 14 jul 2024.

BRASIL: CAMARA DOS DEPUTADOS. COMISSÃO DE CONSTITUIÇÃO E JUSTIÇA E DE CIDADANIA - **Projeto de Lei nº 4476, de 1994**. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=314211#:~:text=A%20lei%20nacional%20%C3%A9%20aquela,%2C%20formalmente%2C%20identificam%2Dse. Acesso em: 14 jul. 2024.

BRASIL: Secretaria-Geral da Presidência da República. **Governo Federal publica a estrutura regimental da Autoridade Nacional de Proteção de Dados**. Disponível em https://www.gov.br/secretariageral/pt-br/noticias/2020/agosto/governo-federal-publica-a-estrutura-regimental-da-autoridade-nacional-de-protecao-de-dados. Acesso em 11.11.2020.

COMISSÃO EUROPEIA. **Proteção de dados na UE**. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt#:~:text=O%20regulamento%20entrou%20em%20vigor,as%20empresas%20e%20os%20cidad%C3%A3os. Acesso em: 14 jul. 2024.

CONECTAJÁ.PROTESTE. **Veja como são as leis de proteção de dados nos Estados Unidos.** Disponível em https://conectaja.proteste.org.br/veja-como-sao-as-leis-de-protecao-de-dados-nos-estados-unidos/#:~:text=Nos%20EUA%2C%20n%C3%A3o%20existe%20uma,privacidade%20dos%20cidad%C3%A3os%3B%20saiba%20mais.&text=Al%C3%A9m%20disso%2C%20existem%20leis%20espec%C3%ADficas,intuito%20de%20garantir%20a%20privacidade. Acesso em 12.11.2020.

DEPARTAMENTO DE JUSTIÇA DO ESTADO DA CALIFÓRNIA. **Lei de Privacidade do Consumidor da Califórnia (CCPA)**. 2024. Disponível em: https://oag.ca.gov/privacy/ccpa. Acesso em: 14 jul. 2024.

DEPARTAMENTO DE JUSTIÇA DO ESTADO DA CALIFÓRNIA. **Lei de Privacidade do Consumidor da Califórnia (CCPA).** 2024. Disponível em: https://oag.ca.gov/privacy/ccpa#sectiona. Acesso em: 14 jul. 2024.

EUA: Califórnia. **CALIFORNIA CONSUMER PRIVACY ACT OF 2018**. Disponível em: https://cppa.ca.gov/regulations/pdf/cppa_act.pdf. Acesso em: 16 jul. 2024.

FEDERAL TRADE COMMISSION. **Children's Online Privacy Protection Rule ("COPPA").** Disponível em: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa. Acesso em: 16 jul. 2024.

GATEFY. **Como funcionam as leis de proteção de dados nos Estados Unidos**. 2021. Disponível em https://gatefy.com/pt-br/blog/como-funcionam-leis-protecao-dados-estados-unidos/. Acesso em 12.11.2020.

GOMES, Maria Cecília. **Você sabe o que são os dados pessoais? Compreenda o conceito!** 2022. Disponível em: https://mariaceciliagomes.com.br/voce-sabe-o-que-sao-os-dados-pessoais-compreenda-o-conceito/ Acesso em: 14 jul. 2024.

INC. **Lei de Proteção à Privacidade Online de Crianças (COPPA)**. 2020. Disponível em: https://www.inc.com/encyclopedia/childrens-online-privacy-protection-act-coppa.html. Acesso em: 14 jul. 2024.

INSTITUTO BRASILEIRO DE DIREITO (IBIJUS). **LGPD do Zero: Método prático para conquistar clientes advogando com proteção de dados**. Disponível em https://www.ibijus.com/curso/301-lgpd-do-zero?a=3&utm_source=gads&utm_medium=cpc&utm_content=palavrachave&utm_campaign=traf_lgpdzeronov20&utm_term=gads-cpc-palavrachave-traf_lgpdzeronov20&gclid=CjwKCAiAtK79BRAIEiwA4OskBvCqvNgPBy4wDNLT6Lows9SKktYa2gbFGA8aQsJMRlhQuqA4l1dYERoCZxIQAvD_BwE. Acesso em 11.11.2020.

JUNQUEIRA, Daniel. Nos EUA, 87% consideram a privacidade de dados como um direito humano. Disponível em https://olhardigital.com.br/noticia/nos-eua-87-consideram-a-privacidade-de-dados-como-um-direito-humano/104819. Acesso em 12.11.2020.

ONETRUST DATAGUINDANCE. **US Privacy Laws**. 2024. Disponível em: https://www.dataguidance.com/comparisons/usa-privacy-laws?gclid=EAIaIQobChMItIP0k8ymhwMVJ1NIAB1vvwIZEAAYASAAEgKZFPD_BwE&ef_id=EAIaIQobChMItIP0k8ymhwMVJ1NIAB1vvwIZEAAYASAAEgKZFPD_BwE:G:s&s_kwcid=AL!17820!3!703187697735!e!!g!!california%20privacy%20regulations!14822529341!130706372871&utm_source=google&utm_medium=cpc&utm_campaign=G|LATAM|Search|Non-

Brand|OneTrust_DataGuidance|Brazil&utm_content=US_Privacy_Laws&utm_term=california%20privacy%20regulations&gad_source=1. Acesso em: 16 jul. 2024.

PARLAMENTO EUROPEU. **DIRETIVA (UE) 2016/680 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680. Acesso em: 16 jul. 2024.

PORTUGAL: CENTRO NACIONAL DE CIBERSEGURANÇA. **REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016.** Disponível em https://www.cncs.gov.pt/content/files/regulamento_ue_2016-679_-_protecao_de_dados.pdf. Acesso em 05.09.2020.

URUPÁ, Marcos. **Lei de privacidade da Califórnia começa a valer e é a mais abrangente dos EUA**. Disponível em https://teletime.com.br/13/01/2020/lei-de-privacidade-da-california-comeca-a-valer-e-e-a-mais-abrangente-dos-eua/. Acesso em 12.11.2020.

VERGILI, Gabriela Machado. **Análise comparativa entre direito à privacidade e direito à proteção de dados pessoais e relação com o regime de dados públicos previsto na Lei Geral de Proteção de Dados.** 2019. Disponível em https://dataprivacy.com.br/analise-comparativa-entre-direito-a-privacidade-e-direito-a-protecao-de-dados-pessoais-e-relacao-com-o-regime-de-dados-publicos-previsto-na-lei-geral-de-protecao-de-dados/. Acesso em: 11 nov. 2020.