Revista
(RE)DEFINIÇÕES
DAS FRONTEIRAS

www.journal.idesf.org.br

A REGULAÇÃO DO TRATAMENTO DOS DADOS PNR PELA ANAC, SOB A PERSPECTIVA DA LGPD: A PROTEÇÃO DOS DADOS ALÉM DA FRONTEIRA

Aicha de Andrade Quintero Eroud[1]
Erika Patrícia de Souza Davies[2]
Manuel David Masseno[3]

Resumo
Diante da maior crise mundial, na área da saúde, do século XXI, devido à pandemia do Coronavírus (COVID-19), que ocasionou o fechamento das fronteiras terrestres do Brasil com os 10 países da América do Sul, com quem faz divisa de território, além do distanciamento social que gerou uma série de problemas econômicos, era esperado uma redução na criminalidade transfronteiriça, o que não ocorreu. O Brasil que é um país de dimensões continentais, acaba sendo rota do contrabando com os países com quem faz fronteira, e, com o trancamento destas, a criminalidade acabou se reinventando para escoar estes ilícitos que fazem girar a economia informal. Correndo maiores riscos de serem apreendidos pelos órgãos de segurança pública, que investem, cada vez mais, na área de inteligência, e, em consequência das dificuldades logísticas, gerada pelo trancamento das fronteiras terrestres, não houve redução desse tipo de criminalidade, o que demanda o estudo dos seus motivos.

Palavras-chave: Crime; contrabando; fronteira; pandemia.

INTRODUÇÃO

Considerando a globalização e a facilidade de locomoção dos viajantes, sob uma perspectiva global, as viagens internacionais ocorrem, cada vez mais, a trabalho, estudo ou turismo. Esse cenário proporciona um aumento no fluxo de

[1] Advogada especialista em privacidade e proteção de dados (OAB/PR 102.358). Especialista em Gestão, Estratégia e Planejamento em Fronteiras pelo Instituto de Desenvolvimento Econômico e Social de Fronteiras - IDESF. Presidente da Comissão de Direito Digital e Proteção de Dados da OAB Subseção Foz do Iguaçu (triênio 2022-2024). Membro Correspondente da Comissão Especial de Privacidade, Proteção de Dados e Inteligência Artificial da OAB Seção São Paulo (triênio 2022-2024). Coordenadora do Curso de Direito e do Núcleo de Práticas Jurídicas do Centro de Ensino Superior de Foz do Iguaçu - CESUFOZ. Professora do Curso de Direito do CESUFOZ e UNIFOZ (Faculdades Unificadas de Foz do Iguaçu). Co-founder do Direito Talks. Membro Titular do Comitê de Proteção de Dados do Instituto Brasileiro de Consumidores e Titulares de Dados - IBCTD. Diretora de Direitos Humanos do Instituto de Desenvolvimento Econômico e Social de Fronteiras - IDESF. Mestranda em Literatura Comparada pela Universidade Federal da Integração Latino-americana - UNILA. Escritora e palestrante.

[2] Advogada. Graduada em Direito pela UNIFOZ. E-mail erikadaviesadv@gmail.com.

[3] Professor Adjunto e Encarregado da Proteção de Dados do I. Politécnico de Beja, em Portugal, onde também integra as Coordenações do Laboratório UbiNET _ Segurança Informática e Cibercrime e do MESI - Mestrado em Engenharia de Segurança Informática.

passageiros internacionais e, consequentemente, um aumento na coleta de dados PNR – *Passenger Name Record* / Registro de Número de Passageiro.

No Brasil, as empresas de transportes aéreos públicos, nacionais ou oriundas de outros países, devem fornecer os dados PNR dos viajantes advindos de voos internacionais com destino, escala, conexão ou origem no Brasil. Dessa maneira, é importante a legislação pátria conferir proteção ao tratamento dos dados em comento, dando ênfase à LGPD.

Nesse sentido, a LGPD trouxe inovações legislativas, com a capacidade de impor a regulação dos dados PNR pela ANAC, e, dessa forma, protegê-los com maior efetividade. Verificar-se-á o repasse de tais dados para a Polícia Federal, designadamente quanto à legitimidade desta em face da LGPD.

O problema de pesquisa formulado para o presente estudo cumpre a seguinte pergunta: Quais são os reflexos da LGPD no tratamento dos dados PRN pela ANAC? A hipótese provisória para essa indagação demonstra que, com o advento da LGPD, há a conferência de uma maior proteção aos dados em questão, com a finalidade de resguardar a privacidade dos passageiros, seguindo o modelo europeu.

O objetivo geral centra-se na verificação das alterações legislativas, decorridas com a vigência da LGPD no ordenamento jurídico pátrio, no tocante ao tratamento dos dados PNR. É pertinente ressaltar a relevância da proteção dos dados dos viajantes, nacionais ou estrangeiros, pois a exploração econômica de tais dados não poderia ser feita pela ANAC; no entanto, o que fazem as companhias aéreas com estes seria objeto de outro estudo, por questões de privacidade.

Os objetivos específicos são: a) constatar as alterações provocadas pela LGPD, pertinente à proteção dos dados PNR; b) identificar a importância da proteção dos dados PNR; c) verificar a regulação do tratamento dos dados PNR pela ANAC.

A partir dessas premissas, com base no critério metodológico que compõe a investigação de abordagem, o método dedutivo, cuja premissa maior é identificar os

efeitos produzidos pela LGPD no tocante à regulamentação do tratamento de dados PNR pela ANAC. Elegem-se como técnicas utilizadas a pesquisa bibliográfica[4] e a documental.

O ATUAL VALOR DOS DADOS E A LGPD, COMO INSTRUMENTO DE PROTEÇÃO

Atualmente – e cada vez mais – o compartilhamento de dados pessoais se torna mais evidente. Com a advinda de novos recursos tecnológicos e com a globalização, os dados são compartilhados em grande escala e possuem valor econômico no mercado. Segundo Rochfeld (2018, p. 73) "os dados pessoais são elementos de personalidade de cada um; emanam dos indivíduos e revelam sua identidade e seus comportamentos, tal como tem elaborado o Tribunal Constitucional alemão desde 1983". Nessa mesma linha, no Brasil, também foi esse o entendimento do Supremo Tribunal Federal[5].

A utilização inadequada dos dados pessoais, no entanto, pode acarretar violação à privacidade – direito fundamental protegido pela Constituição Federal de 1988 (art 5º, inc. X, CF) –, bem como pode gerar danos morais e materiais aos seus titulares. Nesse sentido, a proteção dos dados pessoais decorre do princípio constitucional da dignidade da pessoa humana, e reside, implicitamente, no artigo 5º, IV, X e XII, da Constituição Federal, constituindo, assim, o interesse do Brasil na tutela desses dados (FALK, 2020, p. 163).

Para seus próprios fins, as empresas de transporte aéreo recolhem e armazenam dados pessoais, fornecidos pelos viajantes – dados PNR – e se

[4] "[...] Técnica de investigação em livros, repertórios jurisprudenciais e coletâneas legais". PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica**: teoria e prática. p. 215.

[5] "Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos". Acórdão de 7 de maio de 2020. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 DF, sendo Relatora Min. Rosa Weber. BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 6.387 DF. Relatora Ministra Rosa Weber. **Processos**. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em: 24 jun. 2021.

configuram como as responsáveis pelo tratamento dos dados armazenados; porém, nosso foco é o do repasse de tais dados à ANAC e, por esta, à Polícia Federal.

Nessa toada, é crescente a busca do modo que os dados disponibilizados são utilizados, aumentando a exigência pela transparência, proteção e privacidade destes. É sob essa perspectiva que o tratamento desses dados ganha contornos e amparo jurídico na tentativa de limitar as utilizações tendenciosas deles.

No caso da União Europeia, a Diretiva UE-PNR[6], aprovada e publicada, em simultâneo, com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), prevê que os Estados-Membros devem garantir o direito à proteção de dados, respeitando a confidencialidade, segurança e tratamento dos dados de todos os passageiros, devendo evitar a discriminação dos indivíduos (OLIVEIRA, 2018, p. 159). Se por um lado, há a intenção de efetivar a segurança pública e combater a criminalidade, com base na utilização de dados PNR, por outro lado, “a possibilidade de que inocentes sejam identificados erroneamente como eventuais criminosos ou terroristas é um facto já reconhecido pela Diretiva UE-PNR” (OLIVEIRA, 2018, p. 167).

No Brasil, com a advinda da Lei Geral de Proteção de Dados Pessoais – Lei nº 13.853, de 2019 – também denominada pela sigla LGPD, o tratamento de dados pessoais recebeu uma proteção mais adequada, considerando a importância e o valor destes. De acordo com o artigo 1º, se aplica a mencionada lei ao “tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado”, objetivando “proteger os direitos fundamentais

[6] A Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, sobre a mesma e por todos, *vide* OLIVEIRA, 2018, p. 155.

de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"[7].

Quanto à delimitação territorial da aplicação da LGPD, a redação do artigo 3º (*caput*) determina que "[...] aplica-se 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". Ainda, deve ser observada que tal aplicação está subordinada aos seguintes preceitos: o tratamento de dados deve ser realizado no Brasil (inc. I, art. 3º); recaindo sobre os dados dos residentes no país, bem como das ofertas ou fornecimentos de bens ou serviços (inc. II, art. 3º); desde que coletados em território nacional (inc. III, art. 3º).

Nesse sentido, "como resultado, a LGPD protege todos os indivíduos no Brasil, não apenas os cidadãos brasileiros" (HOEREN; PINELLI, 2020, p. 28). Muito embora haja uma delimitação territorial, os destinatários da LGPD são todos os que estão em território nacional, independentemente, de sua nacionalidade. Ainda, calha clarear a distinção entre os dados pessoais e dados pessoais sensíveis. Seguindo as lições de Hoeren e Pinelli (2020, p. 29):

> No LGPD, dados pessoais são definidos como informações que podem ser atribuídas a uma pessoa física identificada ou identificável. Exemplos não estão incluídos nesta definição, mas você pode pensar em tudo, desde nomes, números de identificação, dados de navegação, nomes de usuários até fatos físicos, mentais, genéticos, econômicos, culturais ou sociais. [...] Dados pessoais sensíveis são definidos como dados pessoais que revelam a origem racial ou étnica, religião, opiniões políticas, filiação sindical, partido político ou crenças filosóficas ou religiosas, ou dados relativos à saúde ou sexualidade do sujeito dos dados.

A importância dessa definição reside no tratamento destinado a cada um, sendo que os dados pessoais estão previstos no artigo 7º da LGPD[8], e os dados

[7] BRASIL. Lei Geral da Proteção de Dados Pessoais. **Lei nº 13.709**, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Brasília, 2018. Acesso em: 17 jan. 2021.

[8] "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou

pessoais sensíveis devem observar o artigo 11 do mesmo Diploma[9]. Os dados pessoais sensíveis comportam informações mais íntimas, tendentes a gerar discriminações.

Observa-se, então, que o tratamento entre os dados pessoais e dados sensíveis possui métodos de processamento diferenciados, considerando a natureza de cada um. No caso dos dados PNR, pode-se considerar dados sensíveis, por exemplo, as informações sobre a saúde e alimentos dos viajantes.

PROTEÇÃO DOS DADOS PNR ENTRE FRONTEIRAS

A criação do sistema de dados PNR – *Passenger Name Record* – ocorreu após os atentados de 11 de setembro de 2000, nos Estados Unidos da América, como um mecanismo de segurança e de prevenção à criminalidade. Desde então,

---

respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou; X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente". BRASIL. Lei Geral da Proteção de Dados Pessoais. **Lei nº 13.709**, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Brasília, 2018. Acesso em: 22 jan. 2021.

[9] "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou; g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais". BRASIL. Lei Geral da Proteção de Dados Pessoais. **Lei nº 13.709**, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Brasília, 2018. Acesso em: 22 jan. 2021.

as empresas aéreas ficaram responsáveis pelo recolhimento dos dados PNR, bem como pelo repasse destes às autoridades públicas competentes.

No Brasil, tem-se a Resolução nº 255, de 13 de novembro de 2012, alterada pela Resolução nº 595, de 11 de novembro de 2020 – que entrou em vigor no dia 03 de maio de 2021 –, a qual estabelece regras sobre a disponibilização de Informações Antecipadas sobre Passageiro (API)[10] e do Registro de Identificação de Passageiros (PNR)[11].

O parágrafo 1º, do artigo 1º, da Resolução nº 255/2012, antes da alteração, previa que "a disponibilização de API e do PNR tem como finalidade a prevenção e a repressão a atos de interferência ilícita e a facilitação do desembaraço junto às autoridades de controle migratório, aduaneiro, sanitário e agropecuário"; no entanto, alterou-se o texto, disciplinando a matéria em voos internacionais (§ 1º, art. 1º) e voos domésticos (§ 2º, art. 2º), sendo aquele mais abrangente do que este. *In verbis*:

> § 1º A disponibilização de API e do PNR relativos a voos internacionais tem como finalidade a prevenção e a repressão a atos de interferência ilícita na aviação civil, a investigação de interesse à saúde pública e a facilitação do processamento de passageiros e bagagens de voos internacionais junto às autoridades de controle migratório, aduaneiro, sanitário e agropecuário.
> § 1º-A A disponibilização de API e do PNR, relativos a voos domésticos, tem como finalidade a prevenção e a repressão a atos de interferência ilícita na aviação civil e a investigação de interesse à saúde pública, junto às autoridades competentes.

Para cumprir o previsto nos parágrafos supramencionados, as empresas aéreas devem transmitir tais dados, de forma segura, por meio de mensagem eletrônica, seguindo os parâmetros indicados pela Polícia Federal e pela Resolução nº 255/2012 (§2º, art. 1º).

---

[10] "Sistema de Informações Antecipadas sobre Passageiros (*Advance Passenger Information* - API): sistema de comunicação eletrônica mediante o qual os dados requisitados sobre passageiros e tripulantes são coletados e transmitidos às autoridades competentes pela segurança e controle das fronteiras, antes da partida ou da chegada do voo, e colocados à disposição dos agentes de fiscalização no aeroporto". ANAC. **Resolução nº 255,** de 13 de novembro de 2012. Brasília, 2012. Disponível em: https://www.anac.gov.br/participacao-social/consultas-publicas/audiencias/2012/22/3-resolucao-api-e-pnr-versao-final.pdf.

[11] "Registro de Identificação de Passageiros (Passenger Name Record - PNR): registro dos dados de cada viagem reservada, por um passageiro ou em nome deste, criado pelas empresas aéreas ou seus agentes autorizados para uso próprio". ANAC. **Resolução nº 255,** de 13 de novembro de 2012. Brasília, 2012. Disponível em: https://www.anac.gov.br/participacao-social/consultas-publicas/audiencias/2012/22/3-resolucao-api-e-pnr-versao-final.pdf.

Repassar essa segurança, o correto cumprimento no tratamento dos dados PNR, é essencial, haja vista que envolve questões de segurança e privacidade dos titulares. Não obstante, em 2017, conforme noticiado pela *BBC News*, por meio do código PNR, foi possível levantar os dados de viajantes com certa facilidade. De acordo com a matéria[12]:

> Este código alfanumérico de cinco ou seis dígitos é fundamental. Os especialistas o chamam de PNR - o acrônimo em inglês de Passenger Name Record (registro de nome de passageiro, na tradução em português) -, mas ele armazena muito mais do que apenas os dados do voo. "Qualquer pessoa que tirar uma foto do seu código PNR, ou o encontrar na internet, pode saber quem você é, de onde viaja e com quem, seu número de celular, endereço, e-mail, itinerário de viagem, assento e até os números de cartões de crédito", conta à BBC Mundo Karsten Nohl, especialista em engenharia de informática e criptografia, que trabalha na companhia de segurança alemã *Security Research Labs.*

Como já referimos, os dados PNR são oriundos de passageiros nacionais e estrangeiros. Nesse sentido, há a necessidade de uma maior cautela no tratamento desses dados, de forma a evitar sua utilização, com intuitos maliciosos, e, até mesmo, para proteger a privacidade de seu titular. Tal preocupação ultrapassa as fronteiras, haja vista que esses dados percorrem para além do território nacional, bem como podem ser disseminados para toda parte do planeta pelos mais variados motivos e intenções. Ademais, “a sociedade digital constrói um novo território (mundo virtual), dificilmente demarcável como as fronteiras geográficas” (CAVALCANTI, 2020, p. 52).

Ao tratar de fronteiras, é pertinente ressaltar que a globalização e a tecnologia romperam a compreensão de fronteiras, apenas como delimitação geográfica[13], as quais ganharam novos sentidos e percepções. Muito embora as fronteiras sejam,

[12] BLASCO, Lucía. A brecha de segurança no Código de reserva aérea que expõe dados pessoais de passageiros. **BBC News Brasil**. 08 de fevereiro de 2017.

[13] “As fronteiras geográficas, cada vez mais ligadas a aspectos meramente simbólicos, não representam grande obstáculo à livre circulação pessoas, de serviços, de bens, de capitais, de informação e, principalmente, dos dados. Em verdade, a sociedade informacional permite que os dados sejam transmitidos instantaneamente, dando origem às redes sociais virtuais em níveis locais, regionais e globais”. CAVALCANTI, Natália Peppi. **Acesso a dados além das fronteiras**: a cooperação jurídica internacional como solução para o (aparente) conflito de jurisdições. Coordenadores: Luiz Rodrigues Wambier, Fábio L. Quintas, Georges Abboud. Salvador: Editora JusPodivm, 2020, p. 40.

também, uma delimitação territorial – e cada Estado possui sua soberania – já não há de se cogitar que um país possa coexistir sem os demais. O que separava, agora, une, em prol do bem comum global.

Sendo assim, “no momento atual da sociedade internacional, em que se vive a interdependência dos Estados e dos povos, nos mais diversos campos, a soberania deve ser compreendida de forma a ajustá-la à atual realidade” (CAVALCANTI, 2020, p. 44).

Destarte, como observado, os dados PNR de estrangeiros podem ser colhidos em território nacional, pelos motivos já expostos, refletindo uma nuance do rompimento da fronteira por vias tecnológicas. É possível obter informações sobre viajantes oriundos de outros países, ou seja, pessoas cujos dados pessoais não advêm do Brasil, mas estes podem ser colhidos e tratados, com base nas leis brasileiras, nos casos supramencionados. Caso o tratamento desses dados não esteja de acordo com a LGPD, e cause algum dano ao seu titular, esse dano ultrapassará as fronteiras, prejudicando-o como cidadão global.

Dessa forma, a coleta e a transferência indiscriminada dos dados PNR podem ocasionar lesões aos preceitos fundamentais, estabelecidos na Carta Magna. Nesse sentido, é importante salientar que foram abordados pelo Parlamento Europeu e pelo Tribunal de Justiça da União Europeia, quanto às questões de compatibilidade do acordo entre a União Europeia e o Canadá, sobre a transferência e o tratamento de dados PNR com os tratados e a Carta; pelo qual tal projeto de acordo permite e regula a transferência de grandes quantidades de dados, com a finalidade de combater a criminalidade transnacional grave, inclusive o terrorismo, podendo esses dados ser conservados por 5 anos, mas com possibilidade de transferência destes, com outras finalidades gerais, para outras autoridades do Canadá e outros Estados, acarretando uma grave e ampla violação aos direitos fundamentais (GUERRA, 2016, p. 63).

Por sua vez, alguns Estados-Membros da União Europeia aprovaram “legislação PNR para outros meios de transporte e alguns países já notificaram a Comissão quanto a quererem incluir os voos intra-UE nas suas legislações internas”

(OLIVEIRA, 2019, p. 187). A questão, no entanto, é que se aplicar tal legislação a todos os meios de transporte pode comprometer a eficiência e a eficácia do sistema, fora a impossibilidade de gerir todos os dados em tempo hábil (OLIVEIRA, 2019, p. 188). Apesar disso, é interessante refletir que “as razões por detrás deste meio de obtenção de dados estão truncadas pelo *fumus* de que há uma vontade de monitorização dos cidadãos por detrás de tudo isto” (OLIVEIRA, 2019, p. 188). O objeto utilizado em nome da segurança (dados PNR), também, pode ser objeto de vigilância.

Por mais que os transportes aéreos, na Europa, têm sido alvos preferenciais de ataques terroristas (OLIVEIRA, 2019, p. 174), não há de se atropelar os direitos e garantias fundamentais em nome da segurança pública. O que deve haver é um equilíbrio entre ambos. Aliás, cumpre esclarecer que o dado PNR não é um mecanismo de controle de identidade, mas de retenção de informações de passageiros, quanto à agenda europeia de política criminal (OLIVEIRA, 2019, p.182).

Por isso mesmo, não há de se coletar, indiscriminadamente, os dados PNR, com base na alegação de combate aos crimes transnacionais, colocando sob suspeita todos os passageiros de transportes aéreos, bem como a transferência desses dados devem observar os ditames constitucionais, considerando que a proteção de dados possui raízes fincadas nos direitos fundamentais, designadamente, na privacidade e na dignidade da pessoa humana.

OS IMPACTOS DA LGPD SOBRE A REGULAÇÃO DO TRATAMENTO DE DADOS PELA ANAC

Preliminarmente, cabe compreender o repasse dos dados PNR das transportadoras aéreas para a Polícia Federal e para a ANAC, sob a análise da decisão liminar da Ministra Rosa Weber – ADIs nº 6387, 6388, 6393 e 6390, relativas à Medida Provisória nº 954, de 17 de abril de 2020.

As transportadoras aéreas repassam os dados PNR para a Polícia Federal e ANAC, com base no Decreto nº 10.046, de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados, no âmbito da administração pública

federal, e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

A criação do Cadastro Base do Cidadão – CBC e do Comitê Central de Governança de Dados – CCGD é posterior à criação da LGPD. Feita essa observação, é, comumente, imaginar que o decreto supramencionado foi instituído, para efetivar os ditames da LGPD, no tocante à proteção de dados pessoais. Desse modo, a premissa inaugural pautou-se na justificativa de facilitar aos brasileiros o acesso aos serviços governamentais (G1, 2019).

Ainda, contam entre os objetivos do cadastro "aprimorar a gestão de políticas públicas"; "aumentar a confiabilidade dos cadastros de cidadãos existentes na administração pública" e "facilitar o compartilhamento de dados cadastrais do cidadão entre os órgãos da administração pública", pretendendo o governo "viabilizar a criação de meio unificado de identificação do cidadão para prestação de serviços públicos" (G1, 2019).

Está previsto, no Decreto nº 10.046/2019, que as informações biográficas constantes no CPF – nome, sexo e filiação – devem compor a base de dados do cadastro; todavia, há a previsão de os dados "provenientes de bases temáticas, por meio do número de inscrição do CPF", bem como o registro de digitais e íris, que são características biológicas, também, comporem a base de dados do cadastro (BRASIL, 2019).

Apesar da justificativa pautar-se na simplificação do acesso aos serviços públicos, o cerne da problemática, dessa centralização de acesso, se encontra na facilitação de repasse e cruzamento do banco de dados entre os órgãos da Administração Pública Federal[14]. A tentativa de desburocratizar tais acessos e de

[14] "Art. 1º Este Decreto estabelece as normas e as diretrizes para o compartilhamento de dados entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União, com a finalidade de: I - simplificar a oferta de serviços públicos; II - orientar e otimizar a formulação, a implementação, a avaliação e o monitoramento de políticas públicas; III - possibilitar a análise das condições de acesso e manutenção de benefícios sociais e fiscais; IV - promover a melhoria da qualidade e da fidedignidade dos dados custodiados pela administração pública federal; e V - aumentar a qualidade e a eficiência das operações internas da administração pública federal. § 1º O disposto neste Decreto não se aplica ao compartilhamento de dados com os conselhos de fiscalização de profissões regulamentadas e com o setor privado. § 2º Ficam excluídos

identificar eventuais problemáticas e incongruências, relacionadas aos dados pessoais, podem culminar em afronta aos preceitos da LGPD e aos direitos fundamentais, garantidos na Carta Magna, como a privacidade e dignidade da pessoa humana.

Admitiu-se a criação do *Big Data*[15] entre a Administração Pública Federal, sem a devida previsão no tocante à limitação desse uso. Esse compartilhamento de banco de dados, sem a observância dos preceitos da LGPD – como a proteção, privacidade e segurança dos dados pessoais – pode ocorrer, de forma prejudicial, ao titular dos dados, seja por meio de vazamento seja por repasse indevido.

As criações do CBC e do CCGD, no entanto, conflitam com a Autoridade Nacional de Proteção de Dados – ANPD, haja vista que aquelas possuem as atribuições que, até então, deveriam ser desta. Explica-se: o próprio CCGD será o órgão responsável pela fiscalização do uso dos dados, previstos pelo Decreto nº 10.046/2019, ou seja, o órgão fiscalizador fica encarregado de fiscalizar a si próprio, em tese. Tal encargo deveria, no mínimo, ser da ANPD, uma vez que a criação desta foi concebida como autoridade independente, com fins fiscalizatórios perpetrados em bases fincadas na proteção de dados pessoais e na privacidade.

Nesse sentido, o Conselho Federal da Ordem dos Advogados do Brasil ajuizou a Ação Direta de Inconstitucionalidade nº 6649, no Supremo Tribunal Federal, contra o Decreto nº 10.046/2019. Dessa forma, “a ação foi distribuída, por prevenção, ao ministro Gilmar Mendes, relator da Arguição de Descumprimento de

---

do disposto no **caput** os dados protegidos por sigilo fiscal sob gestão da Secretaria Especial da Receita Federal do Brasil do Ministério da Economia”. BRASIL. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados**. Decreto nº 10.046**, de 9 de outubro de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato20192022/2019/Decreto/D10046.htm#:~:text=DECRETO%20N%C2%BA%2010.046%2C%20DE%209,Central%20de%20Governan%C3%A7a%20de%20Dados. Brasília, 2019. Acesso em: 25 fev. 2021.

[15] “Big data é o termo utilizado para nomear o conjunto de dados. Representa uma enorme quantidade de dados contida em bancos interligados entre si distribuídos em diversos servidores pelo mundo em rede na internet”. CAVALCANTI, Natália Peppi. A ordem internacional contemporânea. **Acesso a dados além das fronteiras**: a cooperação jurídica internacional como solução para o (aparente) conflito de jurisdições. Coordenadores: Luiz Rodrigues Wambier, Fábio L. Quintas, Georges Abboud. Salvador: Editora JusPodivm, 2020, p. 151.

Preceito Fundamental (ADPF) 695, que questiona o mesmo decreto" (STF, ADI 6649, 2021).

Conforme explana a OAB, as medidas expressas na norma compõem a construção de um poderoso mecanismo de vigilância estatal, com bases nas informações atinentes à pessoa, ao trabalho e à família do titular dos dados (STF, ADI 6649, 2021). Para além dos dados pessoais, tem-se incluso a coleta de dados sensíveis, compostos pelos dados biométricos, com a finalidade de reconhecimento automatizado (STF, ADI 6649, 2021).

No relato acima, a OAB faz menção aos dados sensíveis, inseridos no inc. II, do artigo 2º, do Decreto nº 10.046/2019, que trata os atributos biométricos como "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar". Ademais, cabe salientar que, segundo a OAB, a referida norma se desalinha com a decisão do STF – conforme as ADIs 6387, 6388, 6389, 6390 e 6393 – de suspender a eficácia da Medida Provisória 954/2020, a qual abarcava o "compartilhamento de dados de usuários de telefonia fixa e móvel com o Instituto Brasileiro de Geografia e Estatística (IBGE)" (STF, ADI 6649, 2021).

Posto isso, é perceptível a ruptura com os direitos fundamentais instituídos pela Carta Magna, quais sejam: dignidade da pessoa humana (art. 1º, III); inviolabilidade à intimidade, privacidade, imagem e honra; autodeterminação informativa e proteção e sigilo dos dados pessoais (art. 5º, *caput*, incs. X e XII), consubstanciados como cláusulas pétreas.

No mesmo sentido, foi ajuizada a Arguição de Descumprimento de Preceito Fundamental 695 pelo Partido Socialista Brasileiro (PSB), no Supremo Tribunal Federal. No pedido estava contida a suspensão de compartilhamento de dados entre o Serviço Federal de Processamento de Dados (Serpro) e a Agência Brasileira de Inteligência (ABIN), que envolviam mais de 76 milhões de brasileiros detentores de Carteira Nacional de Habilitação (STF, 2020). O acordo entre esses órgãos da administração pública federal foi firmado, com base no Decreto nº 10.046/2019, e

tinha por intuito o compartilhamento de nomes, filiação, telefone, endereço, dados dos veículos e fotos dos portadores da CNH (STF, 2020).

O PSB sustentou "que a medida viola o direito à privacidade, à proteção de dados pessoais e à autodeterminação informativa, além de afrontar a dignidade da pessoa humana", ademais, "o compartilhamento não se enquadra nas hipóteses previstas no Decreto 10.046/2019 nem encontra respaldo na legislação que rege a atuação da agência de inteligência" (STF, 2020). Ainda:

> A transferência "massiva e indiscriminada" de dados estaria sendo operacionalizada sem transparência e à revelia dos titulares, que não receberam qualquer informação sobre o compartilhamento nem qualquer esclarecimento sobre o tratamento a ser realizado pela Abin. Para o partido, a medida subverte a finalidade para a qual os dados pessoais foram inicialmente coletados, destinando-os a um órgão e a um propósito inteiramente incompatíveis com a motivação original (STF, 2020).

Há de se rememorar, *in casu*, a obra "*1984"*, de George Orwell. Trata-se de um clássico que – embora escrito em tempos em que a tecnologia de comunicação e *internet* ainda não compunham à realidade da época – Orwell demonstra, com riqueza de detalhes, a realidade presenciada pela atual Sociedade da Informação e, quiçá, pela Sociedade da Dominação. Compreende-se esta última como àquela que "vende/doa/repassa" suas informações pessoais para as empresas e Estado em troca de serviços e segurança. Aqui, os dados pessoais ganham valor e passam a ser moeda de troca, em que ganha muito quem recolhe, e perde quem repassa[16].

[16] Atualmente, os dados pessoais possuem relevado valor econômico no mercado, dado o poder de direcionamento ao comportamento das empresas em relação aos seus clientes, como forma de fidelizar clientela e conquistar vantagens sobre a concorrência. Levando a análise para o lado estatal, o Estado passa a ter maior controle e, consequentemente, domínio sobre os cidadãos, uma vez que possui relevantes informações sobre as pessoas, sejam essas documentais (dados pessoais) ou inerentes à natureza e essência da formação individual de cada pessoa (dados sensíveis). Os dados pessoais e sensíveis podem ser requeridos de forma obrigatória pelo Estado, com base nas premissas estatais de se almejar políticas públicas, serviços essenciais e até por motivos de segurança nacional. Entretanto, também há o repasse de dados pessoais de forma espontânea pelo titular, ao adquirir acesso às tecnologias e aplicativos, compras online, ou até mesmo por visitar sites e blogs. Daí surge a noção de dados pessoais como moeda de troca no mercado. A impressão de que um determinado serviço de aplicativo é gratuito cai nas graças do "mero engano". O preço é muito bem pago com os dados pessoais e demais permissões que são concedidas pelo usuário, o qual muitas vezes nem lê os termos antes de aceitá-lo. Um click e o negócio já está feito. Ou seja, o antigo aperto de mãos na hora de fechar um negócio foi substituído pelo atual click. Todavia, o repasse de dados pode custar um preço alto para o titular quando ocorre sem a observância da lei ou até mesmo pelo vazamento de dados deixando-os expostos para as práticas de condutas criminosas.

Logo, no tocante ao Estado, este pode usar os dados pessoais e sensíveis como ferramenta/estratégia de dominação e controle sobre aqueles que estão sob sua tutela. Figura-se, então, o Estado de Vigilância, predito na obra 1984.

Não obstante, o filósofo e epistemologista francês Michel Focault, na década de 1970, trabalhou a sociedade da vigilância apresentada em sua obra “Vigiar e Punir”. Foucault valeu-se da Sociedade Moderna para fazer as análises sobre vigilância e poder. Em sua obra “Vigiar e Punir,” o autor faz menção “[...] dos olhares que devem ver sem ser vistos[...]” que agem com base em “[...] técnicas das vigilâncias múltiplas e entrecruzadas [...]” (FOUCAULT, 1987, p. 195).

Trata-se de uma estratégia que implica a invisibilidade de quem vigia, como forma de aumentar e perpetuar a capacidade de vigilância, não deixando azo para qualquer evasão ou tentativa de se esquivar desse sistema. Isso é transportado para os dias atuais, em que as pessoas são, constantemente, vigiadas, mesmo que de forma imperceptível; mas para quem vigia, nenhum movimento passa despercebido. É quase impossível escapar de todas as formas de vigilâncias.

Nesse sentido, a legislação e as jurisprudências pátrias caminham no sentido de controlar esse sistema de vigilância, que, atualmente, ocorre, em especial, pelo recolhimento e repasse de dados pessoais e sensíveis.

Ao tratar sobre dados, é pertinente ressaltar a hodierna Sociedade Dataísta, a qual “oferece tecnologias inovadoras, além de poderes inéditos e imensos, tanto para políticos, como para grandes corporações e cidadãos comuns” (CAVALCANTI, 2020, p. 34). Nesse sentido, cabe aduzir que:

> A sociedade dataísta, pós-capitalista e hiperglobalizda, é calcada na geração e monetização dos dados, além de dependente destes. Tal constatação é reforçada ao observar a quantidade de dados gerados em apenas um dia por um indivíduo que legitima o Big Data, conjunto gigantesco de dados computacionais complexos existentes no mundo (CAVALCANTI, 2020, p. 35).

Destarte, o fluxo de dados ganha roupagem de direito fundamental que deve ser amparado pelo Estado, carecendo de tutela jurisdicional, mas, por outro vértice,

alimentar a noção de uma terra sem lei, se torna uma tentação (CAVALCANTI, 2020, p. 36).

O Decreto nº 10.046/2019, pelos motivos já aduzidos, anda em caminho oposto ao perseguido pelo ordenamento jurídico pátrio. Dada premissa embasa-se no retrocesso, quanto à proteção aos dados pessoais, considerando sua previsão implícita na Carta Magna. As instituições do CBC e do CCGD, pelo decreto em comento, criam bases para um mega sistema de vigilância, em que o Estado detém dados pessoais e sensíveis da população, e a administração pública federal pode compartilhá-los entre si.

Destarte, os dados PNR, repassados das transportadoras aéreas para a Polícia Federal e ANAC, devem observar a LGPD e estar em consonância com os ditames constitucionais. A transparência e publicidade das informações devem, necessariamente, estarem presentes a todo o momento, sejam na coleta, tratamento, repasse seja no descarte dos dados pessoais. Os titulares dos dados têm o direito de saber o destino de seus dados pessoais e a finalidade de sua coleta de forma transparente. Ademais, deve-se atentar para as questões que envolvem coleta, repasse e transferência de dados PNR, de forma indiscriminada, sob o manto de controlar a criminalidade. A segurança pública não pode ser construída, sob a desconstrução da proteção dos dados pessoais.

Feitas as considerações supramencionadas, a ANAC, como órgão da administração federal, deve atentar aos enunciados da LGPD e verificar o conflito entre esta e o Decreto nº 10.046/2019, principalmente, quando envolver os atributos biométricos, ou seja, os dados sensíveis. A LGPD reveste-se de força normativa, surtindo como efeito a prerrogativa do titular dos dados de saber como será o tratamento de seus dados, e, caso ocorra algum equívoco ou vazamento, o controlador e operador deverão ser responsabilizados, solidariamente, pelo ocorrido.

CONSIDERAÇÕES FINAIS

Atualmente, os dados pessoais ganham devida notoriedade pela relevância que se revestem, ao configurarem como o motor que move a economia atual e como valor que lhes são conferidos, em tempos de Sociedade da Informação. Com efeito,

estes passam a ser tutelados pela ordem jurídica pátria, de forma a estender, aos titulares dos dados pessoais, o direito de autodeterminação informativa, bem como os concedem maior controle e transparência sobre os seus dados pessoais, conforme os ditames da LGPD.

Foi verificada a Diretiva (UE-PNR) 2016/681, pela qual foi constatado que, se por um lado, a coleta dos dados PNR tem por objetivo auxiliar no combate ao terrorismo e à criminalidade transnacional grave, por outro lado, a coleta indiscriminada pode acarretar sérias lesões aos direitos fundamentais, inclusive identificar, equivocadamente, eventuais criminosos. Tal exemplo está contido neste estudo, com o escopo de visualizar o tratamento dos dados PNR na União Europeia, considerando que esta está, consideravelmente, adiantada no assunto, podendo servir como parâmetro para o tratamento de dados PNR no Brasil.

Nesse diapasão, foi verificado o tratamento de dados PNR pela ANAC, com breve enfoque no tratamento de dados PNR feito pela Polícia Federal à luz da LGPD.

Constatou-se que o Decreto nº 10.046/2019, que dispõe sobre a governança no compartilhamento de dados, no âmbito da administração pública federal, e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados, violará os direitos fundamentais elencados na Constituição Federal de 1988, como a dignidade da pessoa humana, a inviolabilidade à intimidade, privacidade, imagem e honra e a autodeterminação informativa e proteção e sigilo dos dados pessoais. O fato é que os órgãos da administração pública federal ficam submetidos a tal decreto, englobando a ANAC e a PF, que compõem a administração pública federal.

A criação do referido decreto deu-se, posteriormente, à LGPD, e, mesmo assim, há um nítido conflito entre o Cadastro Base do Cidadão – CBC, o Comitê Central de Governança de Dados – CCGD, e a Autoridade Nacional de Proteção de Dados – ANPD. Tal incompatibilidade decorre do fato de que o Decreto nº 10.046/2019 delega ao CCGD à responsabilidade fiscalizatória, que deveria ser da ANPD, ou seja, o órgão fiscalizador fica encarregado de fiscalizar a si próprio.

Ademais, o Decreto nº 10.046/2019 confronta o entendimento do STF – conforme as ADIs 6387, 6388, 6389, 6390 e 6393, com a decisão de suspender a eficácia da Medida Provisória 954/2020, que tratava sobre compartilhamento de dados de usuários de telefonia fixa e móvel com o IBGE. Com base nisso, o Conselho Federal da Ordem dos Advogados do Brasil ajuizou a Ação Direta de Inconstitucionalidade nº 6649, no Supremo Tribunal Federal, contra o Decreto em comento.

Também, foi verificada, por meio da Arguição de Descumprimento de Preceito Fundamental 695, ajuizada pelo PSB, que a troca de informações de mais de 76 milhões de brasileiros, que detêm a CNH, entre o SERPRO e ABIN, afronta os direitos fundamentais à privacidade, à proteção de dados pessoais, à autodeterminação informativa e à dignidade da pessoa humana. Houve uma ruptura da transparência e informação do tratamento dos dados com seus titulares, inclusive, a finalidade da coleta restou violada, diante da incompatibilidade da transferência dos dados. O acordo entre esses órgãos da Administração Pública Federal foi firmado com base no Decreto nº 10.046/2019.

Dessa maneira, o repasse dos dados PNR, pelas empresas aéreas às autoridades nacionais, deve observar a LGPD, sob pena de insurgir ações constitucionais, como foi observado por este estudo. Do mesmo modo, o repasse de dados PNR entre a PF e ANAC não pode exceder os limites impostos por lei e devem observar os direitos e garantias fundamentais, estabelecidos pela Constituição Federal de 1988.

A observância aos preceitos do Decreto nº 10.046/2019, com o intuito de facilitar a utilização dos sistemas relacionados aos dados pessoais pela Administração Pública Federal, pode acarretar sérias lesões aos direitos fundamentais e contrariar as previsões contidas na LGPD. A criação do *Big Data* na Administração Pública Federal não pode ser ilimitada, mas, ao remeter-se aos assuntos atinentes aos dados PNR, estes devem estar em plena consonância com a Lei Geral de Proteção de Dados.

REFERÊNCIAS

ANAC. **Resolução nº 255,** de 13 de novembro de 2012. Brasília, 2012. Disponível em: Acesso em: 18 de jan. de 2020.

ANAC. **Resolução nº 595,** de 11 de novembro de 2020. Brasília, 2020. Disponível em: https://www.anac.gov.br/assuntos/legislacao/legislacao-1/resolucoes/2020/resolucao-no-595-11-11-2020/@@display-file/arquivo_norma/RA2020-0595.pdf. Acesso em: 25 jan. 2021.

BLASCO, Lucía. A brecha de segurança no Código de reserva aérea que expõe dados pessoais de passageiros. **BBC News Brasil**. 08 de fevereiro de 2017. Disponível em: https://www.bbc.com/portuguese/curiosidades-38882141. Acesso em: 21 jan. 2021.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral da Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Brasília, 2018.

BRASIL. **Decreto nº 10.046**, de 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm#:~:text=DECRETO%20N%C2%BA%2010.046%2C%20DE%209,Central%20de%20Governan%C3%A7a%20de%20Dados. Brasília, 2019.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6649. Relator Ministro Gilmar Mendes. **Notícias e textos.** Publicado em 25 de janeiro de 2021. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=459125&ori=1.

BRASIL. Supremo Tribunal Federal. PSB pede suspensão de compartilhamento de dados da CNH entre Serpro e Abin. **Notícias e textos**. Publicado em 18 de junho de 2020. Disponível em: http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=445873&ori=1.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 6.387 DF. Relatora Ministra Rosa Weber. **Processos**. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em: 24 jun. 2021.

CAVALCANTI, Natália Peppi. **Acesso a dados além das fronteiras**: a cooperação jurídica internacional como solução para o (aparente) conflito de jurisdições. Coordenadores: Luiz Rodrigues Wambier, Fábio L. Quintas, Georges Abboud. Salvador: Editora JusPodivm, 2020.

FALK, Matheus. Os princípios jurídicos da LGPD e do RGPD: uma leitura a partir da Teoria dos Princípios de Humberto Ávila. **Proteção de dados pessoais em perspectiva**: LGPD e RGPD na ótica do direito comparado. Org. Marcos Wachowicz. Curitiba: Gedai, UFPR, 2020.

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. 27. ed. Tradução Raquel Ramalhete. Petrópolis: Vozes, 1987.

G1. Bolsonaro publica decreto que cria cadastro para reunir informações sobre cidadãos. **G1**, 10 de outubro de 2019. Disponível em: https://g1.globo.com/politica/noticia/2019/10/10/bolsonaro-publica-decreto-que-cria-cadastro-para-reunir-informacoes-sobre-cidadaos.ghtml. Acesso em: 24 fev. 2021.

GUERRA, Clara. Dados dos Passageiros Aéreos – *Quo Vadis*. **Forum de Proteção de Dados**: em foco 40 anos da Constituição e do Direito à Proteção de Dados. nº 2. janeiro, semestral. Comissão Nacional de Proteção de Dados, 2016.

HOEREN, Thomas; PINELLI, Stefan. A nova lei brasileira de proteção de dados: uma visão crítica. **Proteção de dados pessoais em perspectiva**: LGPD e RGPD na ótica do direito comparado. Org. Marcos Wachowicz. Curitiba: Gedai, UFPR, 2020.

MASSENO, Manuel David. A segurança dos dados na LGPD, brasileira: uma perspectiva europeia, desde Portugal. **Revista do Direito UNISC**. Santa Cruz do Sul, RS. n. 59. Vol. 3. p. 80-103. Jan./abr. 2020. ISSN: 1982-9957. Disponível em: https://online.unisc.br/seer/index.php/direito/article/view/14819/8937.

OLIVEIRA, Emellin. O Passanger Name Record e a Proteção de Dados Pessoais: uma análise sobre a transferência da informação dos passageiros aos Estados. **Anuário da Proteção de Dados 2018**. Coordenação: Francisco Pereira Coutinho, Graça Canto Moniz. Lisboa: CEDIS, 2018.

OLIVEIRA, Ricardo Rodrigues de. *Birds flying hight*: a Diretiva (UE) 2016/681e a proposta da Lei 137/XIII da Presidência do Conselho de Ministros. **Anuário de Proteção de Dados 2019**. Coordenação Francisco Pereira Coutinho; Graça Canto Moniz. Lisboa: CEDIS, 2019.

PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica**: teoria e prática. 13 ed. Florianópolis: Conceito Editorial, 2015.

ROCHFELD, Judith. Como qualificar os dados pessoais? Uma perspectiva teórica e normativa da União Europeia em face dos gigantes da Internet. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 10, n. 1, p. 61-84, maio 2018.