REVISTA BRASILEIRA DE DESENVOLVIMENTO E INOVAÇÃO

PROTEÇÃO DE DADOS PESSOAIS EM ATIVIDADES DE INTELIGÊNCIA, SEGURANÇA E PERSECUÇÃO CRIMINAL: DESAFIOS E PERSPECTIVAS

Vladimir Aras[1]

Resumo: O artigo analisa o impacto da Lei Geral de Proteção de Dados Pessoais (LGPD) nas atividades de inteligência e de segurança pública e no processo penal brasileiro. A partir da perspectiva constitucional, internacional e jurisprudencial, o texto examina os desafios jurídicos, os limites normativos e as lacunas existentes na regulamentação do tratamento de dados pessoais por órgãos estatais. Com base em precedentes da Suprema Corte dos EUA, da Corte Interamericana de Direitos Humanos (casos *Escher vs. Brasil* e *CAJAR vs. Colômbia*) e em normas internacionais como a Convenção 108 e o RGPD europeu, o autor propõe a elaboração de uma LGPD Penal e, desde já, a adoção da principiologia adequada para regular tais atividades. A proposta visa assegurar os princípios da proporcionalidade, necessidade e autodeterminação informativa, conciliando a eficácia da persecução penal com a proteção dos direitos fundamentais.

Palavras-chave: proteção de dados pessoais; processo penal; tecnologias digitais; LGPD; autodeterminação informativa.

DATA PROTECTION IN INTELLIGENCE, SECURITY, AND CRIMINAL PROSECUTION ACTIVITIES: CHALLENGES AND PERSPECTIVES

Abstract: This article examines the impact of Brazil's General Data Protection Act (LGPD) on intelligence gathering, public security operations and criminal proceedings. From a constitutional, international, and jurisprudential perspective, it explores the legal challenges, normative gaps, and regulatory limits concerning the processing of personal data by state authorities. Drawing on case law from the U.S. Supreme Court and the Inter-American Court of Human Rights (notably *Escher v. Brazil* and *CAJAR v. Colombia*), as well as international instruments like Convention 108 and the EU GDPR, the author advocates for the enactment of a Criminal Data Protection Law and, from now on, the adoption of appropriate principles to regulate such activities. Such a statute would uphold proportionality, necessity, and informational self-determination, balancing effective criminal prosecution with fundamental rights protection.

Keywords: Personal data protection; criminal procedure; digital technologies; LGPD; informational self-determination.

[1] Doutor em Direito (Ceub), Mestre em Direito Público (UFPE), Especialista MBA em Gestão Pública (FGV), Membro do MP desde 1993, atualmente no cargo de Procurador Regional da República em Brasília (MPF), Professor Adjunto de Processo Penal da UnB, Professor do PPGD/MPD do IDP, Secretário de Cooperação Internacional da PGR (2013-2017), Fundador do Instituto de Direito e Inovação (ID-i), editor do site www.vladimiraras.blog (Blog do Vlad), integrou a Comissão de Juristas que redigiu o anteprojeto da LGPD Penal.

REVISTA BRASILEIRA DE DESENVOLVIMENTO E INOVAÇÃO

PROTEZIONE DEI DATI PERSONALI NELLE ATTIVITÀ DI INTELLIGENCE, SICUREZZA E GIUDIZIO PENALE: SFIDE E PROSPETTIVE

Riassunto: L'articolo analizza l'impatto della Legge Generale sulla Protezione dei Dati Personali (LGPD) sulle attività di intelligence e di pubblica sicurezza e sul processo penale brasiliano. Attraverso una prospettiva costituzionale, internazionale e giurisprudenziale, si esplorano le sfide legali e le lacune normative relative al trattamento dei dati personali da parte dello Stato. Basandosi sulla giurisprudenza della Corte Suprema degli Stati Uniti e della Corte Interamericana dei Diritti Umani (casi *Escher vs. Brasile* e *CAJAR vs. Colombia*), nonché su strumenti internazionali come la Convenzione 108 e il GDPR dell'UE, l'autore propone l'adozione di una LGPD penale e, fin da ora, l'adozione dei principi adeguati per regolamentare tali attività. Tale normativa dovrà garantire i principi di proporzionalità, necessità e autodeterminazione informativa, conciliando l'efficacia della repressione penale con la tutela dei diritti fondamentali.

Parole chiave: protezione dei dati personali; processo penale; tecnologie digitali; LGPD; autodeterminazione informativa.

Sumário: 1 Introdução – 2 Marco jurídico internacional sobre proteção de dados pessoais – 3 A jurisprudência da Suprema Corte dos EUA e a proteção de dados pessoais – 4 Marco jurídico doméstico sobre PDP – 4.1 A Constituição e a LGPD – 4.2 Proteção esparsa em leis especiais e o conteúdo da futura LGPD Penal – 4.3 A proteção de dados em atividades de inteligência – 5 A jurisprudência da Corte Interamericana em matéria de PDP – 5.1 O caso *Escher vs. Brasil*: o direito à privacidade – 5.2 O caso *CAJAR vs. Colômbia*: o direito à PDP – 6 Princípios de PDP aplicáveis ao processo penal e às atividades de inteligência – 7 Cooperação internacional e transferência internacional de dados – 7.1 Convenção de Budapeste – 7.2 Interpol – 7.3 Europol – 7.4 Eurojust – 7.5 Equipes conjuntas de investigação – 7.6 Intercâmbio internacional de informações tributárias – 8 A aplicabilidade da LGPD brasileira a atividades de inteligência e de segurança pública e ao processo penal – 9 O compartilhamento de dados entre órgãos de inteligência e instituições de persecução penal – 9.1 Os contextos do compartilhamento de dados entre agências estatais – 9.2 Um breve panorama do compartilhamento de dados na jurisprudência – 10 Conclusão – Referências.

1 INTRODUÇÃO

A ascensão da sociedade da informação provocou um rearranjo na atividade probatória no processo penal. Se, por um lado, o Estado necessita capturar e analisar quantidades inéditas de dados para enfrentar delitos locais e transnacionais, por outro, o *Bill of Rights* impõe barreiras à coleta indiscriminada de dados pessoais. O embate, já latente desde o caso *Olmstead vs. Estados Unidos*, de 1928,[2] ganhou contornos diversos com o avanço de tecnologias intrusivas, exigindo a aprovação de normas internacionais, como a Convenção 108, de 1981, do Conselho da Europa (COE); normas supranacionais, como o Regulamento Geral de Proteção de Dados da União Europeia (RGPD), de 2016; e normas domésticas, como a Lei 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), que serve como exemplo.

Este estudo pretende cartografar o campo normativo — internacional e doméstico — que conforma o tratamento de dados pessoais nas atividades de inteligência, de segurança e de persecução penal, oferecendo críticas e delineando uma proposta de atualização legislativa. O método adotado combina análise dogmática, exame de direito comparado e revisão da jurisprudência estrangeira e interamericana recentíssima, notadamente o caso *CAJAR vs. Colômbia*, julgado pela Corte Interamericana de Direitos Humanos (Corte IDH) em 2023, que delineia o direito à autodeterminação informativa nas Américas.

Não deixamos, contudo, de analisar o precedente *Escher e Outros vs. Brasil*, pela sua contribuição para o desenvolvimento deste campo de proteção, no contexto das novas tecnologias da informação e da comunicação. Em 2009, já dizia a Corte IDH:

> A fluidez informativa que existe atualmente coloca o direito à vida privada das pessoas em uma situação de maior risco, devido à maior quantidade de novas ferramentas tecnológicas e à sua utilização cada vez mais frequente. Esse progresso, especialmente quando se trata de interceptações e gravações telefônicas, não significa que as pessoas devam estar em uma situação de vulnerabilidade frente ao Estado ou aos particulares. Portanto, o Estado deve

[2] O caso *Olmstead v. United States*, decidido pela Suprema Corte dos Estados Unidos em 1928, é um marco histórico no debate sobre privacidade e escutas telefônicas no direito constitucional norte-americano. A decisão teve implicações profundas para o desenvolvimento do direito à privacidade e à proteção de dados nos Estados Unidos, mesmo antes da era digital. Os réus foram condenados por violarem a Lei Seca (*National Prohibition Act*) pelo contrabando de bebida alcoólica na região de Seattle. A prova fundamental foi uma série de escutas telefônicas, realizadas há um século. UNITED STATES. Supreme Court. **Olmstead v. United States,** 277 U.S. 438 (1928).

> assumir um compromisso com o fim adequar aos tempos atuais as fórmulas tradicionais de proteção do direito à vida privada.[3]

Para os fins deste artigo, adotamos o conceito interamericano de dados pessoais, como sendo a:

> [...] informação que, direta ou indiretamente, identifica ou pode ser usada para identificar uma pessoa natural, em relação a sua "identidade física, fisiológica, genética, mental, econômica, cultural ou social […] expressada em forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica, electrónica, visual o de qualquer outro tipo".[4]

Ao longo deste artigo, examinaremos os contornos normativos, jurisprudenciais e institucionais da proteção de dados pessoais no âmbito das atividades de inteligência, de segurança pública e de persecução penal. Partindo de um panorama internacional, exploraremos os tratados e padrões estrangeiros relevantes — como a Convenção 108 do Conselho da Europa, o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e a Diretiva LED no contexto do efeito Bruxelas —, bem como a evolução da jurisprudência da Suprema Corte dos Estados Unidos, desde os votos dissidentes de Brandeis até precedentes mais recentes como *Carpenter v. United States*. Esse percurso será complementado pelo exame do marco jurídico brasileiro, com destaque para a Emenda Constitucional nº 115/2022, a LGPD e a constatação da necessidade premente de uma legislação penal específica que discipline o tratamento de dados sensíveis no processo penal e em atividades de inteligência.

Trataremos também dos princípios de proteção de dados pessoais aplicáveis à inteligência e ao processo penal, como finalidade, minimização, segurança, responsabilização e proporcionalidade.

A análise se estenderá aos regimes jurídicos de transferência internacional de dados, com destaque para mecanismos de cooperação como a Convenção de Budapeste, a Interpol, a Europol, a Eurojust, as equipes conjuntas de investigação e o intercâmbio de dados fiscais. Finalmente, dedicaremos atenção à aplicabilidade da LGPD brasileira a atividades de segurança pública e ao compartilhamento de dados entre órgãos estatais,

[3] CORTE IDH. **Caso Escher e Outros vs. Brasil.** Sentença de 6 de julho de 2009, § 115. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf.

[4] OEA. **Principios Actualizados sobre la Privacidad y la Protección de Datos Personales**. Washington: Departamento de Derecho Internacional, 2022, §123. https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf.

concluindo pela urgência de uma LGPD Penal à altura dos desafios constitucionais e convencionais contemporâneos.

2 MARCO JURÍDICO INTERNACIONAL SOBRE PROTEÇÃO DE DADOS PESSOAIS

Primeiro tratado dedicado à proteção de dados pessoais, a Convenção do Conselho da Europa (COE) de 1981 para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados Pessoais (Convenção 108)[5] inaugurou a era da autodeterminação informativa e influenciou sucessivas normatizações – como a Diretiva EU 95/46/CE[6] – e diplomas legislativos latino-americanos.

Ainda no âmbito do Conselho da Europa, tem importância a Recomendação 15, de 1987, do Comitê de Ministros do COE, sobre o uso de dados pessoais na atividade policial, o que inclui a prevenção e a investigação de crimes e a manutenção da ordem pública.[7] Este documento de *soft law*[8] procurou estender, para o campo policial, as proteções criadas pela Convenção 108, de 1981, entre os Estados Partes do Conselho da Europa.

A Carta Europeia de Direitos Fundamentais, do ano 2000,[9] e o Regulamento Geral de Proteção de Dados, de 2016,[10] elevaram a proteção de dados à condição de *lex*

[5] A Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, do Conselho da Europa (Convenção 108) entrou em vigor em 1º de outubro de 1985. COUNCIL OF EUROPE. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**, done at Strasbourg, in 28 January 1981.

[6] UNIÃO EUROPEIA. **Diretiva 95/46/CE** do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

[7] COUNCIL OF EUROPE. **Recommendation No. R (87) 15** of the Committee of Ministers to member states regulating the use of personal data in the police sector, *adopted by the Committee of Ministers on 17 September 1987.* Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804e7a3c.

[8] As normas de soft law são normas de quase-direito ou direito em formação. Cf. ARAS, Vladimir. **Direito internacional público**. 2.ed. Rio de janeiro: Método, 2023.

[9] A CDFUE reconhece o direito à privacidade (art. 7º) e o direito à proteção de dados pessoais (art. 8º). UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**, Lisboa, 7 de dezembro de 2000. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=PT.

[10] UNIÃO EUROPEIA. **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).

fundamentalis regional na União Europeia. Além de valer na UE, o RGPD alcança três dos quatro países da Associação Europeia de Comércio Livre (EFTA),[11] com exceção da Suíça[12], consagrando nesse âmbito geográfico princípios de proteção de dados como minimização, finalidade e segurança.

Quanto à atividade estritamente penal e securitária, destacam-se a Diretiva Policial (*Law Enforcement Directive* - LED)[13] e a Diretiva *Passenger Name Record* (PNR),[14] ambas de 2016, que disciplinam o tratamento de dados para fins de prevenção, investigação e repressão criminal no âmbito dos 27 Estados da União Europeia.

Essas normas espraiam-se para além das fronteiras europeias mediante acordos de cooperação e cláusulas espelhadas em convênios bilaterais e em virtude do chamado "efeito Bruxelas", expressão que define a influência que o ordenamento da União Europeia produz nos processos legislativos de Estados terceiros.[15]

No contexto brasileiro, não se pode ignorar a incidência das normas de proteção da intimidade e da vida privada que estão positivadas no Pacto Internacional de Direitos Civis e Políticos (PIDCP), de 1966,[16] e na Convenção Americana de Direitos Humanos (CADH), de 1969.[17] Embora tais tratados não contenham previsão expressa sobre o direito à proteção de dados pessoais (direitos dataprotetivos), seu reconhecimento, como veremos, é uma consequência lógica da proteção da autonomia privada e da privacidade e do direito à informação.

No campo da *soft law*, tenhamos em conta ainda os Princípios da OEA sobre Privacidade e Proteção de Dados Pessoais. São estes 13 os princípios interamericanos:

---

[11] A *European Free Trade Association* (EFTA) abrange Islândia, Liechtenstein, Noruega e Suíça.
[12] Este mercado ampliado (26 UE + 3 EFTA) configura o Espaço Econômico Europeu (EEE).
[13] UNIÃO EUROPEIA. **Diretiva (UE) 2016/680**, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados.
[14] UNIÃO EUROPEIA. **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.
[15] "The Brussels Effect refers to the EU's unilateral power to regulate global markets". BRADFORD, Anu. **The Brussels Effect:** How the European Union Rules the World. Oxford: Oxford University Press, 2020, p. xiv.
[16] BRASIL. **Decreto 592, de 6 de julho de 1992**. Promulga o Pacto Internacional de Direitos Civis e Políticos, adotado em 16 de dezembro de 1966.
[17] BRASIL. **Decreto 678, de 6 de novembro de 1992.** Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969.

finalidade legítima e lealdade; transparência e consentimento; pertinência e necessidade; tratamento e conservação; confidencialidade; segurança dos dados; exatidão dos dados; direitos de acesso, retificação, cancelamento, oposição e portabilidade; dados pessoais sensíveis; responsabilidade; fluxo transfronteiriço de dados e responsabilidade; exceções e autoridade de proteção de dados.[18] O Princípio Interamericano 12 parece legitimar a opção do legislador brasileiro em 2018, na LGPD, de não tratar de matéria processual penal, ao estabelecer que:

> Quaisquer exceções a esses Princípios devem ser expressa e especificamente previstas na legislação nacional, tornadas públicas e limitadas apenas a motivos relacionados à soberania nacional, à segurança nacional, à segurança pública, à proteção da saúde pública, à luta contra o crime, à aplicação de regulamentos ou outras prerrogativas de política pública ou ao interesse público.[19]

3 A JURISPRUDÊNCIA DA SUPREMA CORTE DOS EUA E A PROTEÇÃO DE DADOS PESSOAIS

A jurisprudência da Suprema Corte dos Estados Unidos em matéria de proteção de dados pessoais é fragmentada, mas reveladora de um lento amadurecimento do entendimento sobre o direito à privacidade no contexto digital. Seu marco zero está na contribuição doutrinária de Brandeis e Warren, em 1890, com o texto seminal *The Right to Privacy*.

Muito antes do reconhecimento internacional de um direito à proteção de dados pessoais, este artigo teve profunda influência na formação do entendimento jurídico norte-americano acerca da privacidade, ao trazer uma nova concepção jurídica: o direito do indivíduo de "ser deixado em paz" (*the right to be let alone*), em reação ao avanço da imprensa sensacionalista e das tecnologias fotográficas que, no final do século 19, começavam a invadir a vida privada.[20]

A contribuição de Brandeis e Warren foi marcante, pois deslocou o foco da proteção da honra e da propriedade para a tutela da personalidade e da vida íntima como

[18] OEA. **Principios Actualizados sobre la Privacidad y la Protección de Datos Personales**. Washington: Departamento de Derecho Internacional, 2022. https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf.
[19] OEA. **Principios Actualizados sobre la Privacidad y la Protección de Datos Personales**, p. 83.
[20] WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193–220, 1890.

bens jurídicos autônomos. Seu argumento lançou as bases para o reconhecimento judicial da privacidade como um direito implícito no ordenamento constitucional norte-americano, mesmo sem previsão literal no texto da Constituição daquele país. Anos depois, já como juiz (*justice*) da Suprema Corte dos EUA, Brandeis reiteraria essas ideias em seu voto dissidente no caso *Olmstead vs. Estados Unidos* (1928), quando defendeu que escutas telefônicas realizadas sem mandado judicial violavam o espírito da Quarta Emenda, mesmo que não houvesse invasão física de propriedade.[21] Ratificada em 1791, a Quarta Emenda à Constituição norte-americana protege os cidadãos de buscas e apreensões não razoáveis e exige que os mandados judiciais expedidos para sua execução se baseiem em uma justa causa (*probable cause*).[22]

Décadas mais tarde, a concepção de Brandeis influenciaria fortemente decisões da Corte como a proferida no caso *Griswold v. Connecticut* (1965), no qual se reconheceu um "direito à privacidade" implícito nas chamadas *penumbras* das liberdades garantidas pela Constituição norte-americana, notadamente entre os direitos da Primeira, Terceira, Quarta, Quinta e Nona Emendas.[23] O texto de Brandeis e Warren não apenas inaugurou o debate jurídico moderno sobre privacidade nos EUA, como se tornou uma pedra angular na construção teórica e jurisprudencial que culminaria na proteção da vida privada digital. Os autores forneceram a linguagem e os fundamentos filosóficos que, ao longo do século XX, permitiram à Suprema Corte moldar uma jurisprudência protetiva da intimidade.

Tradicionalmente, no campo criminal, o fundamento constitucional para a proteção da privacidade nos EUA deriva da Quarta Emenda, que garante o direito à proteção contra buscas e apreensões não razoáveis. Contudo, esse direito foi

[21] SCOTUS: "The information which led to the discovery of the conspiracy and its nature and extent was largely obtained by intercepting messages on the telephones of the conspirators by four federal prohibition officers. Small wires were inserted along the ordinary telephone wires from the residences of four of the petitioners and those leading from the chief office. The insertions were made without trespass upon any property of the defendants. They were made in the basement of the large office building. The taps from house lines were made in the streets near the houses. The gathering of evidence continued for many months. Conversations of the conspirators, of which refreshing stenographic notes were currently made, were testified to by the government witnesses". UNITED STATES. Supreme Court. **Olmstead v. United States**, 277 U.S. 438 (1928).

[22] NEWTON, Brent E. The Real-World Fourth Amendment**. Hastings Constitutional Law Quarterly**, vol. 43, issue 4, 2016. DOI: 10.2139/SSRN.2769106.

[23] SCOTUS: "The Connecticut statute forbidding use of contraceptives violates the right of marital privacy which is within the penumbra of specific guarantees of the Bill of Rights". UNITED STATES. Supreme Court. **Griswold v. Connecticut,** 381 U.S. 479 (1965).

originalmente concebido para proteger bens físicos e domicílios. Adoção de uma abordagem baseada na propriedade ("*property-based approach to Fourth Amendment*" ou teoria do *trespass*)[24] exigiu adaptação pretoriana para também cobrir a coleta e o tratamento de dados no ambiente digital.

Além do muito conhecido precedente *Katz*, de 1967, que fixou a doutrina da razoável expectativa de privacidade,[25] outro marco importante nessa evolução é o caso *Carpenter v. United States* (2018), no qual a Suprema Corte decidiu que o Estado deve obter um mandado judicial para acessar registros históricos de localização de celulares, mantidos por empresas de telecomunicações. Este julgado revela uma evolução significativa do pensamento da Corte, tendo em conta a utilização crescente de tecnologias de vigilância digital e de coleta de dados, que desafiam as noções tradicionais de privacidade contra busca e apreensão relacionadas ao conceito de propriedade.[26] A Corte reconheceu que, mesmo que os dados do suspeito estejam sob custódia de terceiros, como operadoras de telefonia, sua obtenção sem autorização judicial viola uma razoável expectativa do réu quanto à sua privacidade,[27] que aqui chamamos de privacidade locacional.[28]

Em 2024, este tema apareceu na jurisprudência do STF, na ADI 5642, que questionava a constitucionalidade dos arts. 13-A e 13-B do CPP. Na ocasião, a ministra Rosa Weber asseverou que os usuários de telefonia celular têm expectativa de privacidade ao conectar seus aparelhos às estações rádio-base (ERB), de modo que, embora seus movimentos físicos sejam sabidamente documentados, tais dados só podem ser acessados mediante prévia autorização judicial.

> Na realidade, de modo geral, pessoas comuns esperam que sua rotina de deslocamentos esteja a salvo de monitoramentos e invasões indevidas. Há, portanto, uma inequívoca expectativa de privacidade sobre os dados que permitem a análise em tempo real de sua locomoção, bem

[24] UNITED STATES. Supreme Court. **Florida v. Jardines**, 569 U.S. 1 (2013).
[25] UNITED STATES. Supreme Court. **Katz v. United States**, 389 U.S. 347 (1967).
[26] CAMINKER, Evan H. Location Tracking and Digital Data: Can Carpenter Build a Stable Privacy Doctrine? **Supreme Court Review,** 2018, p. 411-481.
[27] UNITED STATES. Supreme Court. **Carpenter v. United States**, 585 U.S.___(2018).
[28] Quando a privacidade locacional é afetada, os usuários de *location-based services* (LBS) "[…] may have less control over what is known of their whereabouts (past, present, and future) and thus their activities and behavior. Locational disclosure—the ability to identify or infer sensitive characteristics of people from locations they occupy in space—may result from the analysis of LBS-derived tracking data and used for unethical practices such as 'Spatial Spam'." BRIDWELL, Scott A. The dimensions of locational privacy. *In*: MILLER, Harvey J. (Org.). **Societies and Cities in the Age of Instant Access**. Dordrecht: Springer Netherlands, 2007, p. 209–225.

> assim daqueles que propiciam a elaboração de um verdadeiro mapa de sua movimentação. Não constitui demasia assinalar que, hoje em dia, a partir de técnicas sofisticadas de cruzamento de dados, é possível, com base na localização – mais ou menos precisa – de indivíduos, extrair as mais diversas informações públicas e privadas, a exemplo, domicílio residencial e profissional, a frequência em academias, os locais de lazer, os restaurantes de predileção e, até mesmo, dados mais sensíveis como a periodicidade de consultas médicas e as respectivas especialidades, a regularidade de idas a farmácias, bem assim aspectos mais íntimos relativos ao comportamento sexual.[29]

Outros precedentes relevantes nos EUA, como *Riley vs. Califórnia* (2014), também mostram a sensibilidade crescente da Suprema Corte norte-americana frente às peculiaridades dos dados digitais. Em *Riley*, o tribunal decidiu unanimemente que a Polícia, em regra, precisa de um mandado judicial para revistar o conteúdo de celulares apreendidos durante prisões, reconhecendo que tais dispositivos contêm vastas quantidades de informações pessoais que não podem ser equiparadas a itens físicos tradicionais. Esta decisão aumentou o *standard* necessário para o acesso a dados de celulares apreendidos para busca sobre provas digitais.[30]

O precedente *Estados Unidos vs. Jones* (2012) também abordou as tecnologias de vigilância. A Suprema Corte considerou inconstitucional, por violação à Quarta Emenda, a instalação de um dispositivo de rastreamento GPS no veículo de Antoine Jones sem mandado judicial. Embora a decisão tenha se baseado na doutrina da invasão física à propriedade – evocando uma leitura originalista, capitaneada por Antonin Scalia –, diversos ministros (especialmente Samuel Alito e Sonia Sotomayor) destacaram preocupações com os riscos à privacidade em um contexto de vigilância persistente e tecnologicamente sofisticada, sinalizando a necessidade de reinterpretar os limites do "expectativa de privacidade" diante da era digital. Assim, o caso *Jones* promove uma inflexão doutrinária que pode contribuir para atualizar a jurisprudência da SCOTUS diante dos novos desafios da vigilância eletrônica estatal, parecendo reforçar a centralidade da autodeterminação informativa como bem jurídico tutelado.[31]

---

[29] STF, Pleno, **ADI 5642/DF**, Rel. Min. Edson Fachin, j. em 18/04/2024, voto da Min. Rosa Weber, p. 30.
[30] UNITED STATES. Supreme Court. **Riley v. California**, 573 U.S. 373 (2014).
[31] SCOTUS: "*Held:* The Government's attachment of the GPS device to the vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search under the Fourth Amendment. Pp. 3–12. (a) The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Here, the Government's physical intrusion on an "effect" for the purpose of obtaining information constitutes a "search." This type of encroachment on an area enumerated in the Amendment would have been considered a search within the meaning of the Amendment at the time it was adopted. Pp. 3–4. (b) This conclusion is consistent with this Court's Fourth Amendment jurisprudence, which until the latter half of the 20th century was tied to common-law trespass.

Apesar desses avanços, a jurisprudência americana ainda carece de uma teoria sólida sobre autodeterminação informativa, tal como desenvolvida no direito europeu e posteriormente na América Latina. A ausência de uma lei federal sobre proteção de dados – semelhante ao RGPD europeu ou à LGPD brasileira – faz com que a proteção dependa de interpretações constitucionais casuísticas, de leis estaduais e de normas setoriais esparsas.

De todo modo, a doutrina americana tem mostrado como tecnologias emergentes – como a localização de pessoas por GPS e torres de telefonia celular e novas medidas investigativas, como o cerco digital[32] (*geofence)*[33] – desafiam os limites tradicionais da Quarta Emenda, levando a Suprema Corte a adaptar sua posição às novas realidades digitais.[34]

Kerr resume bem o quadro. Baseando-se nas decisões em *Riley* (2014) e *Carpenter* (2018), o autor sustenta que as novas tecnologias de hoje, como as tecnologias de ontem, levaram a Suprema Corte americana a se reposicionar, na interpretação da Quarta Emenda, em busca de uma zona de equilíbrio, que continue a proteger os direitos

---

Later cases, which have deviated from that exclusively property-based approach, have applied the analysis of Justice Harlan's concurrence in *Katz* v. *United States*, 389 U. S. 347, which said that the Fourth Amendment protects a person's "reasonable expectation of privacy," *id.*, at 360. Here, the Court need not address the Government's contention that Jones had no "reasonable expectation of privacy," because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, the Court must "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo* v. *United States*, 533 U. S. 27, 34. *Katz* did not repudiate the understanding that the Fourth Amendment embodies a particular concern for government trespass upon the areas it enumerates. The *Katz* reasonable-expectation-of-privacy test has been added to, but not substituted for, the common-law trespassory test. See *Alderman* v. *United States*, 394 U. S. 165, 176; *Soldal* v. *Cook County*, 506 U. S. 56, 64. *United States* v. *Knotts*, 460 U. S. 276, and *United States* v. *Karo*, 468 U. S. 705—post-*Katz* cases rejecting Fourth Amendment challenges to "beepers," electronic tracking devices representing another form of electronic monitoring—do not foreclose the conclusion that a search occurred here. *New York* v. *Class*, 475 U. S. 106, and *Oliver* v. *United States*, 466 U. S. 170, also do not support the Government's position." UNITED STATES. Supreme Court. **United States v. Jones**. 565 US 400 (2012).

[32] ARAS, Vladimir. Cerco digital (*geofence*) e varredura terminológica: balizas constitucionais e legais. *In*: SALGADO, Daniel de Resende; GRANDIS, Rodrigo de; BECHARA, Fábio Ramazzini (Orgs.). **10 anos da Lei das Organizações Criminosas: aspectos criminológicos, penais e processuais penais**. São Paulo: Almedina Brasil, 2023, p. 597–662.

[33] BRODNER, Emily. Navigating the Terrain of Geofence Warrants. **Arizona Law Journal of Emerging Technologies**, vol. 7, issue 2, 2024, p. 1-23. https://doi.org/10.2458/azlawjet.6395.

[34] CAMINKER, Evan H. Location Tracking and Digital Data: Can Carpenter Build a Stable Privacy Doctrine? **Supreme Court Review,** 2018, p. 411-481.

fundamentais nela previstos,[35] mesmo quando estiverem em jogo os seus equivalentes digitais.

4 MARCO JURÍDICO DOMÉSTICO SOBRE PDP

O direito à proteção de dados pessoais (PDP) nasceu na Alemanha, nos anos 1970, e se afirmou internacionalmente na década seguinte. Foi também nos anos 1980 que adveio o seu reconhecimento no plano constitucional, no famoso caso do censo alemão.[36]

> A primeira lei no mundo sobre o assunto foi editada em 1970 pelo estado alemão de Hessen. No ano de 1977, o Parlamento alemão aprovou lei federal de proteção de dados (*Bundesdatenschutzgesetz*). Todavia, o ápice do reconhecimento da proteção de dados ocorreu com a decisão do Tribunal Constitucional Federal sobre a questão do censo demográfico que se realizava na Alemanha no ano de 1983 (*Volkszählungsurteil*). Esta decisão estabeleceu o direito fundamental à autodeterminação informativa (*Grundrecht auf informationelle Selbstbestimmung*).[37]

Atualmente, inúmeros países têm suas leis de proteção de dados. Entre eles, estão todos os Estados europeus, várias nações latino-americanas, como a Argentina, o Brasil, o México e o Uruguai, assim como países africanos e asiáticos. A China pôs em vigor sua legislação em 2017 e 2021, formando um subsistema com a Lei de Proteção a Informações Pessoais (conhecida pela sigla PIPL em inglês), a Lei de Cibersegurança e a Lei de Segurança de Dados.[38]

4.1 A Constituição e a LGPD

A Emenda Constitucional 115/2022 positivou, no art. 5º, LXXIX, o direito fundamental à proteção de dados pessoais no Brasil. A norma criou um direito fundamental que, mesmo antes de sua promulgação, já vinha sendo reconhecido pelo Supremo Tribunal Federal (STF).[39] A disciplina do novo direito foi encomendada ao legislador ordinário.

---

[35] KERR, Orin S. **The digital Fourth Amendment:** privacy and policing in our online world. New York: Oxford University Press, 2025, p. 201-202.
[36] ALEMANHA. Tribunal Constitucional Federal. Sentença de 15 de dezembro de 1983. **1 BvR 209, 269, 362, 420, 440, 484/83.** Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html.
[37] MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **Revista Jurídica Luso-Brasileira**, n. 5, p. 781–809, 2019, p. 782.
[38] ZAYAT, Rami; LUCENTE, Kate; LURQUIM, Lea. Data protection laws of the World, **DLA Piper**, 20 January 2025. Disponível em: https://www.dlapiperdataprotection.com/index.html?c=CN.
[39] STF, **ADI 6387 MC-Ref**, Pleno, Relatora Ministra Rosa Weber, j. em 7/05/2020.

A LGPD, de 2018, lei geral de alcance transversal, aplica-se *ratione materiae* ao setor público e ao setor privado, mas traz exceção aberta no art. 4º, III, para atividades de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) investigação e repressão de infrações penais. Esses campos de competência estatal deverão ser objeto de uma legislação específica futura.

Conforme os padrões internacionais, as atividades de inteligência são as que visam a obter, analisar e difundir informação para apoiar a tomada de decisão por parte dos órgãos responsáveis pela implementação de políticas de segurança pública e de Estado.[40]

Já a investigação criminal diz respeito aos procedimentos adotados pela Polícia ou pelo Ministério Público para coligir informações e provas sobre a autoria e a materialidade de uma possível infração penal. Segundo a Corte IDH:

> [...] embora ambos os conceitos tenham como objetivo buscar e processar informações e possam usar métodos semelhantes, como a vigilância de comunicações e a captura de dados, suas finalidades são essencialmente diferentes, pois os serviços de inteligência operam com uma função preventiva e não de supressão direta do crime.[41]

4.2 Proteção esparsa em leis especiais e o conteúdo da futura LGPD Penal

Atualmente, vigora no Brasil um mosaico de normas que tratam direta ou indiretamente de proteção de dados pessoais (PDP). Tais diplomas costumam regular os chamados meios especiais de obtenção de prova e o fazem sem unidade principiológica. Essa deficiência normativa gera insegurança jurídica, incentiva interpretações extensivas e compromete a confiança pública na persecução penal.

Apesar da equivocada opção do Congresso Nacional de postergar a regulamentação dos temas de inteligência e de persecução penal, o ordenamento brasileiro está repleto de normas esparsas, embora limitadas, de proteção de dados pessoais.

Tomemos como exemplos a Lei 9.296/1996 (Lei das Interceptações), a Lei 12.965/2014 (Marco Civil da Internet), a Lei 12.850/2013 (Lei das Organizações

[40] UNITED NATIONS. Human Rights Council. Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, **A/HRC/14/46**, 17 May 2010, Boa Prática 1. Disponível em: https://documents.un.org/doc/undoc/gen/g10/134/10/pdf/g1013410.pdf. Vide também: COLOMBIA. Corte Constitucional. **Sentencia C-540/12, de 1 de julio de 2012**. Disponível em: https://www.corteconstitucional.gov.co/relatoria/2012/c-540-12.htm.

[41] CORTE IDH. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia**. Sentencia de 18 de octubre de 2023, § 550. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.

Criminosas), a Lei 12.037/2009 (Lei de Identificação Criminal), a Lei 7.210/1984 (Lei de Execução Penal) e o Código de Processo Penal (CPP). Também podemos inserir neste campo a Convenção sobre Cibercriminalidade, concluída em Budapeste em 2001, no âmbito do Conselho da Europa, e internalizada no Brasil pelo Decreto 11.491/2023. Há, aqui e ali nesses textos normativos, regras de PDP.

O hiato normativo em termos de PDP, posto em confronto com a norma constitucional de 2022, exige a imediata aprovação de uma LGPD penal que consolide princípios de necessidade, finalidade, proporcionalidade e minimização de dados nas atividades em questão; que estabeleça procedimentos padronizados de coleta, preservação e compartilhamento internacional de dados pessoais; e que preveja um regime sancionatório próprio para violações cometidas por agentes estatais.

Uma futura norma também deve prever quais direitos do titular se aplicam às atividades atualmente excluídas e em que medida a pessoa pode exercer sua autodeterminação informacional. Segundo a Corte IDH, a lei pode prever limitações aos direitos do titular no que tange às atividades de inteligência, para atender a suas peculiaridades, numa sociedade democrática.[42] Esta compreensão também se aplica a atividades de persecução criminal. Vemos a aplicação destas restrições, quanto ao objeto e prazo de sigilo, na Lei de Acesso à Informação (Lei 12.527/2011). Segundo Calabrich:

> A autodeterminação informativa, que é o poder de dispor, de ter ciência e de eventualmente controlar o uso que se faz de seus próprios dados, obstando ou promovendo a correção de ilegalidades ou abusos, é um direito fundamental positivado no art. 5º da CF/88 e, como em qualquer outra seara, deve balizar o tratamento de dados no processo penal. A autodeterminação informativa é, para o processo penal, um direito instrumental, ou uma garantia, que limita a atividade do Estado, no sentido de que este só pode realizar um tratamento se atender a determinados requisitos legais – obediência à cadeia de custódia, ao procedimento previsto em lei e, quando excepcionalmente exigida, prévia autorização judicial –, além dos decorrentes dos princípios gerais que regem o tratamento de dados pessoais no Brasil e que, como vetores axiológicos, hão de ser sopesados conforme a situação concreta verificada: finalidade, adequação, necessidade, minimização, qualidade dos dados, segurança, prevenção, não discriminação, responsabilização, prestação de contas, livre acesso e transparência (estes últimos, temperados pelas peculiaridades de uma investigação criminal).[43]

[42] CORTE IDH. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia**. Sentencia de 18 de octubre de 2023, § 601-602. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.

[43] CALABRICH, Bruno. **Proteção de Dados Pessoais na Investigação Criminal e no Processo Penal**: garantismo, eficiência e *standards* de validade. São Paulo: Editora JusPodivm, 2024, p. 293-294.

Além de reconhecer o direito à PDP, o STF também afirmou o direito à autodeterminação informacional. Em 2020, no julgamento da medida cautelar na ADI 6.387, o Tribunal asseverou a existência de um direito fundamental autônomo à proteção de dados pessoais e à autodeterminação informacional.[44] Professando entendimento similar, em 1987, no caso *Leander vs. Suécia*, o Tribunal Europeu de Direitos Humanos afirmou que a lei deve prever especificamente as atribuições e competências dos órgãos de inteligência (e, agregamos, dos órgãos de persecução criminal), para o tratamento de dados pessoais, assim como os fins desse tratamento.[45] A Corte IDH seguiu a mesma concepção no que diz respeito ao conteúdo da legislação sobre PDP:

> Tal lei deve regular, da forma mais precisa possível, o seguinte: (a) os fundamentos pelos quais os órgãos de inteligência podem manter arquivos contendo dados pessoais; tais fundamentos, compatíveis com os objetivos das atividades de inteligência, devem limitar as ações das autoridades a esse respeito; (b) os tipos e espécies de dados pessoais que as autoridades estão autorizadas a manter em seus arquivos; e (c) os parâmetros aplicáveis ao uso, retenção, verificação, retificação, apagamento ou divulgação de tais dados.[46]

Um elemento essencial do modelo é também a previsão de instrumentos adequados de proteção de dados pessoais. Neste campo, desponta o *habeas data*, previsto no art. 5º, inciso LXXII, da Constituição[47] e regulado pela Lei 9.507/1997, sem prejuízo de outros

---

[44] STF, **ADI 6387 MC-Ref**, Pleno, Relatora Ministra Rosa Weber, j. em 07/05/2020.

[45] TEDH: "However, the requirement of foreseeability in the special context of secret controls of staff in sectors affecting national security cannot be the same as in many other fields. Thus, it cannot mean that an individual should be enabled to foresee precisely what checks will be made in his regard by the Swedish special police service in its efforts to protect national security. Nevertheless, in a system applicable to citizens generally, as under the Personnel Control Ordinance, the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life (ibid., p. 32, § 67). In assessing whether the criterion of foreseeability is satisfied, account may be taken also of instructions or administrative practices which do not have the status of substantive law, in so far as those concerned are made sufficiently aware of their contents (see the Silver and Others judgment of 25 March 1983, Series A no. 61, pp. 33-34, §§ 88-89). In addition, where the implementation of the law consists of secret measures, not open to scrutiny by the individuals concerned or by the public at large, the law itself, as opposed to the accompanying administrative practice, must indicate the scope of any discretion conferred on the competent authority with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference (see the above-mentioned Malone judgment, Series A no. 82, pp. 32-33, § 68)". EUROPEAN COURT OF HUMAN RIGHTS**. Case of Leander v. Sweden**. Judgment 26 March 1987, § 51. Disponível em: https://hudoc.echr.coe.int/eng?i=001-57519.

[46] CORTE IDH. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia.** Sentencia de 18 de octubre de 2023, § 577. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.

[47] Constituição: "Art. 5º. (...): LXXII - conceder-se-á *"habeas-data":* a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo".

remédios legais e constitucionais para sua tutela. Noutros Estados das Américas, esse direito pode ser tutelado por meio de *habeas data* (como no Equador, Honduras, Panamá, Paraguai e Peru), ações de *amparo* (como na Argentina, no México e na Nicarágua) ou ações civis de proteção à privacidade (como na Bolívia).[48]

4.3 A proteção de dados em atividades de inteligência

No Brasil, a atividade de inteligência é regida pela Lei 9.883/1999 (Lei do SISBIN),[49] pelo Decreto 11.693/2023, que a regulamenta;[50] pelo Decreto 8.793/2016,[51]que institui a Política Nacional e Inteligência (PNI), assim como pela Resolução nº 2/2013 do Congresso Nacional.[52] Apesar de duas breves referências ao respeito a direitos humanos, uma para o SISBIN[53] e outra para a Agência Brasileira de Inteligência (ABIN),[54] um direito humano em particular tem débil proteção nas atividades de inteligência: o direito à PDP.

Segundo a Política Nacional de Inteligência (PNI), a atividade de inteligência, que se compõe da inteligência em sentido estrito e da contrainteligência, é o:

> [...] exercício permanente de ações especializadas, voltadas para a produção e difusão de conhecimentos, com vistas ao assessoramento das autoridades governamentais nos respectivos níveis e áreas de atribuição, para o planejamento, a execução, o acompanhamento e a avaliação das políticas de Estado.[55]

Como atividade estatal, a inteligência tem por fim a produção e a difusão às autoridades competentes de informações sobre "fatos e situações que ocorram dentro e

---

[48] CORTE IDH. **Caso CAJAR,** nota 759, p. 183.
[49] BRASIL. **Lei 9.883, de 7 de dezembro de 1999.** Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências
[50] BRASIL. **Decreto 11.693, de 6 de setembro de 2023**. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência.
[51] BRASIL. **Decreto 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência.
[52] BRASIL**. Resolução nº 2, de 2013-CN**. Dispõe sobre a Comissão Mista de Controle das Atividades de Inteligência (CCAI), comissão permanente do Congresso Nacional, órgão de controle e fiscalização externos da atividade de inteligência, previsto no art. 6º da Lei nº 9.883, de 7 de dezembro de 1999.
[53] Lei do SISBIN: "Art. 1º. [...]. § 1º. O Sistema Brasileiro de Inteligência tem como fundamentos a preservação da soberania nacional, a defesa do Estado Democrático de Direito e a dignidade da pessoa humana, devendo ainda cumprir e preservar os direitos e garantias individuais e demais dispositivos da Constituição Federal, os tratados, convenções, acordos e ajustes internacionais em que a República Federativa do Brasil seja parte ou signatário, e a legislação ordinária".
[54] Lei do SISBIN: "Art. 3º. [...]. Parágrafo único. As atividades de inteligência serão desenvolvidas, no que se refere aos limites de sua extensão e ao uso de técnicas e meios sigilosos, com irrestrita observância dos direitos e garantias individuais, fidelidade às instituições e aos princípios éticos que regem os interesses e a segurança do Estado".
[55] BRASIL. **Decreto 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência.

fora do território nacional, de imediata ou potencial influência sobre o processo decisório, a ação governamental e a salvaguarda da sociedade e do Estado".[56] Conforme o Conselho de Direitos Humanos das Nações Unidas:

> Prática 1. Os serviços de inteligência desempenham um papel importante na proteção da segurança nacional e na defesa do Estado de direito. Seu principal objetivo é coletar, analisar e disseminar informações que auxiliem os formuladores de políticas e outras entidades públicas a tomar medidas para proteger a segurança nacional. Isso inclui a proteção da população e de seus direitos humanos.[57]

A LGPD não se aplica às atividades de inteligência. No entanto, a previsão do inciso LXXIX do art. 5º da Constituição não pode cair no vazio, especialmente numa área tão suscetível a abusos sobre direitos fundamentais.

À luz da Boa Prática 21, impõe-se que o direito interno descreva, de forma clara e acessível, o catálogo de medidas de coleta de dados à disposição dos serviços de inteligência, as finalidades legítimas que podem justificá-las, as pessoas e atividades passíveis de sujeição a tais técnicas, o grau mínimo de suspeita exigido para seu emprego, os prazos de duração da ingerência e os procedimentos formais de autorização, fiscalização e revisão. Em termos jurídico-constitucionais, isso reclama tipicidade das medidas, vinculação a objetivos determinados, delimitação subjetiva e objetiva do alvo, exigência de lastro indiciário suficiente, marcos temporais estritos e um ciclo completo de controle — autorização prévia, supervisão continuada e auditoria *ex post* — para prevenir arbitrariedades.[58]

Consoante a Boa Prática 23, a legislação doméstica deve especificar quais dados pessoais podem ser armazenados pelos órgãos de inteligência e quais critérios regem seu uso, conservação, eliminação e eventual divulgação. A retenção somente se legitima quando estritamente necessária ao cumprimento das atribuições do órgão público, sob os princípios da necessidade, adequação e proporcionalidade, com regras de minimização,

[56] BRASIL. **Decreto 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência.
[57] UNITED NATIONS. Human Rights Council. Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, **A/HRC/14/46**, 17 May 2010, Practice 1. Disponível em: https://documents.un.org/doc/undoc/gen/g10/134/10/pdf/g1013410.pdf.
[58] UNITED NATIONS. Human Rights Council. Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, **A/HRC/14/46**, 17 May 2010, Practice 21. Disponível em: https://documents.un.org/doc/undoc/gen/g10/134/10/pdf/g1013410.pdf.

prazos definidos, mecanismos de anonimização quando cabíveis e deveres de registro e *accountability* que permitam a verificação independente do ciclo de vida dos dados.

A PNI, estabelece, no seu item 5.V, como instrumento essencial às atividades de inteligência, o "intercâmbio de dados e conhecimentos no âmbito do SISBIN, nos termos da legislação em vigor". A importância do compartilhamento de dados é reiterada no item, segundo o qual a atuação estatal exitosa exige "compartilhamento oportuno de dados [...], observadas as características específicas da atividade de Inteligência, em especial quanto aos usuários que a eles devem ter acesso". Esta interação entre inteligência e persecução criminal mostra-se crucial no enfrentamento à criminalidade organizada.[59]

> A atuação cada vez mais integrada nas vertentes preventiva (Inteligência) e reativa (Policial) mostra ser a forma mais efetiva de enfrentar esse fenômeno, inclusive no que diz respeito a subsidiar os procedimentos de identificação e interrupção dos fluxos financeiros que lhe dão sustentação. Atualmente, a grande maioria dos países desenvolve e aprofunda o intercâmbio de dados e conhecimentos entre os órgãos de Inteligência e de repressão em âmbito nacional e internacional.[60]

É de se notar que o art. 3º, inciso XI, da Resolução nº 2, de 2013 do Congresso Nacional, atribui à Comissão Mista de Controle de Atividades de Inteligência (CCAI) apurar denúncias sobre violações a direitos fundamentais praticadas por órgãos públicos, em atividades de inteligência e contrainteligência, "apresentadas por qualquer cidadão, partido político, associação ou sociedade".[61]

Em se apurando qualquer ilícito civil ou penal – inclusive sobre violações ao direito à PDP – a CCAI deve, nos termos do art. 21 da Resolução, encaminhar suas conclusões "ao Ministério Público competente, conforme o caso, para que este promova a ação de responsabilidade civil ou criminal dos infratores."[62] Pode-se dizer que este é um dos remédios efetivos, no sentido do art. 25 da CADH, para lidar com ofensas ao direito à autodeterminação informacional na ordem jurídica brasileira.

[59] BRASIL. **Decreto 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência.
[60] BRASIL. **Decreto 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência.
[61] BRASIL**. Resolução nº 2, de 2013-CN**. Dispõe sobre a Comissão Mista de Controle das Atividades de Inteligência (CCAI), comissão permanente do Congresso Nacional, órgão de controle e fiscalização externos da atividade de inteligência, previsto no art. 6º da Lei nº 9.883, de 7 de dezembro de 1999.
[62] BRASIL**. Resolução nº 2, de 2013-CN**. Dispõe sobre a Comissão Mista de Controle das Atividades de Inteligência (CCAI), comissão permanente do Congresso Nacional, órgão de controle e fiscalização externos da atividade de inteligência, previsto no art. 6º da Lei nº 9.883, de 7 de dezembro de 1999.

Como veremos no próximo tópico, as atividades de inteligência também estão sujeitas à PDP.

5 A JURISPRUDÊNCIA DA CORTE INTERAMERICANA EM MATÉRIA DE PDP

Na jurisprudência da Corte Interamericana, o direito à vida privada (art. 11 da CADH) foi o tronco a partir do qual, anos depois, brotaram os ramos dos direitos à proteção de dados e autodeterminação informativa, que exigem do Estado bases legais claras, finalidade legítima e controles estritos de necessidade e proporcionalidade para o tratamento de dados.

Em *Escher e outros vs. Brasil*, a Corte censurou interceptações e uso indevido de registros de comunicação sem salvaguardas suficientes, articulando requisitos de autorização judicial, fundamentação, delimitação temporal e proteção contra difusão arbitrária.[63]

Em *Tristán Donoso vs. Panamá*, consolidou-se a vedação à divulgação estatal de comunicações privadas obtidas em investigação, sem justificativa robusta e controle judicial efetivo, pois tal revelação a público ofende o direito à privacidade.[64]

E, diante de vigilâncias ilegais e formação de bancos de dados de inteligência, a sentença *CAJAR vs. Colômbia* reafirmou que a coleta, conservação e circulação de informações pessoais devem obedecer aos princípios de minimização, finalidade e segurança, com acesso a recursos efetivos e responsabilização estatal.[65]

O resultado é um padrão interamericano que desautoriza devassas, impede "pescarias probatórias" digitais e impõe ao poder público um dever ativo de instituir salvaguardas técnicas e jurídicas contra abusos, inclusive no ciberespaço.

5.1 O caso *Escher vs. Brasil*: o direito à privacidade

[63] CORTE IDH. **Caso Escher e Outros vs. Brasil.** Sentença de 6 de julho de 2009. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf.
[64] CORTE IDH. **Caso Tristán Donoso vs. Panamá**. Sentencia de 27 de enero de 2009, § 75-83. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_193_por.pdf
[65] CORTE IDH. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia**. Sentencia de 18 de octubre de 2023, nota 759, p. 183. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.

Partindo da perspectiva brasileira, é inevitável mencionar o caso *Escher e Outros vs. Brasil*, julgado pela Corte IDH em 2009,[66] que discutiu a violação à vida privada de trabalhadores rurais do Estado do Paraná, vítimas de escutas telefônicas feitas à margem de Lei 9.296/1996. Citando o caso dos *Massacres de Ituango vs. Colômbia*,[67] naquela ocasião a Corte IDH lembrou que:

> O artigo 11 da Convenção proíbe toda ingerência arbitrária ou abusiva na vida privada das pessoas, enunciando diversos âmbitos dela, como a vida privada de suas famílias, seus domicílios e suas correspondências. Nesse sentido, a Corte sustentou que "o âmbito da privacidade se caracteriza por estar isento e imune a invasões ou agressões abusivas ou arbitrárias por parte de terceiros ou da autoridade pública". [68]

O caso *Escher* teve origem em fatos ocorridos em 1999, quando a Polícia Militar paranaense interceptou ilegalmente linhas telefônicas vinculadas a membros de organizações da sociedade civil, especialmente trabalhadores rurais ligados à Cooperativa Agrícola de Conciliação Avante Ltda (COANA) e à Associação Comunitária de Trabalhadores Rurais (ADECON).

A Corte IDH ressaltou a gravidade das interceptações telefônicas sem ordem judicial fundamentada,[69] sem adequada supervisão judicial, realizadas por tempo excessivo e de forma indiscriminada, em evidente violação à privacidade e ao direito à intimidade dos indivíduos monitorados. Destacou-se especialmente o descumprimento ao devido processo legal (quebra de legalidade)[70] e a falta de motivação legítima para o monitoramento dos membros das associações afetadas, já que as vítimas não estavam envolvidas em práticas criminosas, mas em atividades legítimas e protegidas pela Convenção Americana, como o direito à associação e à livre expressão política.

O Tribunal enfatizou que a divulgação posterior das gravações para a imprensa constituiu também uma violação da Convenção, uma vez que o material estava sob

---

[66] CORTE IDH. **Caso Escher e Outros vs. Brasil.** Sentença de 6 de julho de 2009. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf.

[67] CORTE IDH. **Caso de Las Masacres de Ituango vs. Colombia**. Sentencia de 1 de julio de 2006, § 193-196. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_148_esp.pdf.

[68] CORTE IDH. **Caso Escher e Outros vs. Brasil**. Sentença de 6 de julho de 2009, § 113. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf.

[69] "No dia 5 de maio de 1999, a juíza Elisabeth Khater (doravante "a juíza Khater"), titular da Vara de Loanda, autorizou o pedido de interceptação telefônica através de uma simples anotação na margem da petição, na qual escreveu 'R[ecebido] e A[nalisado]. Defiro. Oficie-se. Em 05.05.99'. A juíza não notificou o Ministério Público da decisão adotada". CORTE IDH. **Caso Escher e Outros vs. Brasil**. Sentença de 6 de julho de 2009, § 91 Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf.

[70] CORTE IDH, **Caso Escher e Outros vs. Brasil**, § 146.

custódia do Estado e protegido por segredo de justiça. Mesmo assim, foi revelado a uma emissora de televisão, com entrega de transcrições a jornalistas de outros veículos.

> Em termos gerais, a Corte considera que manter sigilo quanto às conversas telefônicas interceptadas durante uma investigação penal é um dever estatal: a) necessário para proteger a vida privada das pessoas sujeitas a uma medida de tal natureza; b) pertinente para os efeitos da própria investigação; e c) fundamental para a adequada administração da justiça. No presente caso, tratava-se de informação que deveria permanecer apenas em conhecimento de um reduzido número de funcionários policiais e judiciais e o Estado falhou em sua obrigação de mantê-la sob o devido resguardo.[71]

Este caso tornou-se referência obrigatória para o debate sobre os limites estatais na vigilância da privacidade no Brasil e na América Latina, servindo de alerta contra abusos estatais no tratamento de dados na persecução criminal.

5.2 O caso *CAJAR vs. Colômbia*: o direito à PDP

Quase 15 anos depois dos precedentes *Escher*, em 2023, a Corte IDH avançou no tema da PDP, reconhecendo pela primeira vez o direito à autodeterminação informacional. No caso *CAJAR vs. Colômbia* (2023), a Corte decidiu que atividades de inteligência estatal se sujeitam aos mesmos limites de privacidade impostos a qualquer forma de tratamento de dados, afirmando a autodeterminação informativa como um direito autônomo, mediante desdobramento do art. 11 da Convenção Americana.[72]

A partir de 1990, agentes do Estado colombiano (Forças Armadas, Polícia Nacional e Departamento Administrativo de Segurança - DAS) implementaram vigilância sistemática, interceptações de comunicações, perfilação e formação de dossiês de membros da Corporação Coletivo de Advogados José Alvear Restrepo[73] (CAJAR), seus familiares e colaboradores, sem base legal ou controle judicial apropriado. Essas atividades de inteligência, que perduraram por mais uma década e meia, eram ilegais, correspondendo a assédios, coações e ameaças a tais pessoas, e a intromissões em suas

[71] CORTE IDH. **Caso Escher e Outros vs. Brasil**, § 162.
[72] ISERTE, Jonathan Mendoza; ANGARITA, Nelson Remolina. In a Landmark Judgment, The IACHR recognized an autonomous right to informational self-determination. **FPF**, December 16, 2024. Disponível em: https://fpf.org/blog/in-a-landmark-judgment-the-inter-american-court-of-human-rights-recognized-an-autonomous-right-to-informational-self-determination/?utm_source=chatgpt.com.
[73] José Alvear Restrepo (1913-1953) foi um político, advogado e guerrilheiro colombiano. A ONG que leva seu nome foi fundada como associação civil em 1980. Tem sede em Bogotá.

vidas privadas, em prejuízo de seus papeis sociais como defensores de direitos humanos.[74]

Houve participação ativa de agentes estatais e de organizações paramilitares, que receberam informações pessoais das vítimas. Os abusos foram favorecidos por discursos de deslegitimação provenientes do Poder Executivo. Comunicados oficiais do governo colombiano referiam-se aos defensores como "inimigos do Estado", "terroristas", "integrantes das guerrilhas", "traidores da pátria". As práticas de violência, intimidação e ameaças geraram deslocamentos de integrantes do coletivo e seus familiares e outros dissabores pessoais.[75]

Sobre a inteligência estatal, a Corte IDH acentuou que tal atividade deve proteger todas as pessoas que vivem no território do Estado, sendo certo que seu impacto na PDP "torna essencial delimitar as exigências, os requisitos e os controles que são impostos para tornar essas atividades compatíveis com as condições e os propósitos de um Estado de Direito e, portanto, com o conteúdo da Convenção Americana."[76]

Disse ainda o Tribunal que qualquer compressão de direitos fundamentais, inclusive do direito à privacidade, "deve estar prevista em lei, buscar um fim legítimo e atender aos requisitos de idoneidade, necessidade e proporcionalidade, isto é, devem ser necessárias em uma sociedade democrática".[77]

Assim, embora veladas, as atividades de inteligência não são executadas num vácuo. Devem observar critérios de legalidade e respeitar direitos humanos, como se vê

---

[74] CORTE IDH: "Esta Corte ha tenido oportunidad de referirse, en distintas oportunidades, a las personas defensoras de derechos humanos y a su trascendental papel en el marco de un sistema democrático. Así, el Tribunal en forma reiterada ha puesto de relieve la importancia de la labor de las defensoras y los defensores de derechos humanos, al considerarla fundamental para el fortalecimiento de la democracia y el Estado de Derecho, lo que justifica un deber especial de protección por parte de los Estados". CORTE IDH. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia.** Sentencia de 18 de octubre de 2023, § 471. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.

[75] **CORTE IDH. Caso CAJAR,** § 706.

[76] **CORTE IDH. Caso CAJAR,** § 520.

[77] CORTE IDH. **Caso CAJAR**, § 521. No mesmo sentido, vide: CORTE IDH. **Caso Tristán Donoso vs. Panamá**. Sentencia de 27 de enero de 2009, § 55-56 e 83, relativo à divulgação ilegal de comunicações telefônicas do advogado panamenho Santander Tristán Donoso.

na jurisprudência europeia[78] e na *soft law* universal, adotadas pelo Conselho de Direitos Humanos das Nações Unidas.[79]

Desde 1978, o TEDH vem acentuando a necessidade de lei para legitimar as ingerências nos direitos fundamentais, como o fez no famoso precedente *Klass vs. Alemanha*: "Os poderes de vigilância secreta dos cidadãos, característicos do estado policial, são toleráveis ao abrigo da Convenção apenas na medida em que sejam estritamente necessários para salvaguardar as instituições democráticas."[80]

Noutro julgamento, proferido no ano 2000, no caso *Rotaru vs. Romênia*, o TEDH voltou ao tema, tendo afirmado que as normas que preveem interferências na vida privada devem ser interpretadas restritivamente, devendo sempre observar a lei e seus requisitos. Para o TEDH, embora "os serviços de inteligência possam existir legitimamente em uma sociedade democrática", sua capacidade de vigilância velada somente é compatível com a Convenção Europeia se forem necessários para a proteção do Estado democrático de Direito.[81]

Desde cedo, a Corte IDH acompanhou essa concepção. No caso *Myrna Mack Chang*, de 2006, o Tribunal em San José pontuou que as atividades de inteligência devem respeitar os direitos individuais e submeter-se ao rigoroso controle de autoridades civis, "uma vez que, dadas as condições de sigilo sob as quais essas atividades são realizadas, elas podem levar ao cometimento de violações de direitos humanos e infrações penais [...]".[82] Obviamente, tal manifestação se estende ao direito à PDP e à autodeterminação informativa. Porém, como adverte Calabrich:

> [...] uma proteção excessiva a direitos individuais pode conduzir ao estrangulamento de direitos transindividuais, assim como uma proteção excessiva a direitos transindividuais pode conduzir ao estrangulamento de direitos individuais. Uma visão garantista da intersecção do

[78] No TEDH, ver o *Caso Klass e Outros vs. Alemanha*, Sentença de 6 de setembro de 1978, § 42; o *Caso Rotaru vs. Romênia* [GC], Sentença de 4 de maio de 2000, § 47, e o *Caso Segerstedt-Wiberg e Outros vs. Suécia*, Sentença de 6 de setembro de 2006, § 88.

[79] UNITED NATIONS. Human Rights Council. Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, **A/HRC/14/46**, 17 May 2010. Disponível em: https://documents.un.org/doc/undoc/gen/g10/134/10/pdf/g1013410.pdf.

[80] EUROPEAN COURT OF HUMAN RIGHTS. **Case of Klass and Others vs. Germany**. Judgment 6 September 1978, § 42. Disponível em: https://hudoc.echr.coe.int/eng?i=001-57510.

[81] EUROPEAN COURT OF HUMAN RIGHTS. **Case of Rotaru v. Rumania [GC].** Judgment 4 May 2000, § 47-48. Disponível em: https://hudoc.echr.coe.int/eng?i=001-58586.

[82] CORTE IDH. **Caso Myrna Mack Chang vs. Guatemala**. Sentencia de 25 de noviembre de 2003, § 284. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_101_esp.pdf.

> processo penal com a proteção de dados pessoais, por exemplo, impõe admitir que criar restrições desproporcionais, porquanto sem justificativa racional plausível, para o tratamento de dados pessoais na persecução penal resultará em investigações e processos nos quais as partes não disporão de ferramentas úteis para certificar os fatos. Não criar restrições, ou fixá-las em grau demasiadamente reduzido, resultará em investigações e processos nos quais os titulares de dados pessoais serão vulnerabilizados. Uma persecução penal só será eficiente quando puder proporcionar equilíbrio na proteção do interesse de réus e investigados, do interesse público e do interesse de titulares dos dados pessoais. A proteção simultânea e harmoniosa de todos esses interesses é, em si, um interesse público."[83]

Em 2023, ao revisitar o tema das atividades de inteligência, a Corte IDH avançou na afirmação de sua sujeição às normas de PDP, reconhecendo um direito humano autônomo, que se acha abrangido pelo art. 11 (direito à vida privada) e pelo art. 13 (direito de acesso à informação) da Convenção Americana de Direitos Humanos, e que serve à proteção de outros direitos como a privacidade, a honra, a reputação e a dignidade da pessoa humana [84]

No caso colombiano, as várias ações de inteligência empreendidas pela DAS, com a interceptação de comunicações, a entrada em domicílio, o monitoramento, a tomada de fotografias de residências, escritórios de trabalho e círculos familiares das vítimas, e a requisição de dados pessoais a entidades privadas foram desenvolvidas sem autorização ou controle de uma autoridade judicial. Para a Corte, tal autoridade, "além de analisar a proporcionalidade da medida", deve decidir sobre a forma, o tempo, o alcance e os limites impostos para salvaguardar os direitos das pessoas afetadas.[85] Quanto a estas, é preciso também levar em conta sua condição pessoal, pois jornalistas e advogados merecem proteção especial, em função da atividade que desempenham, o que faz limitar as atividades de inteligência (e de persecução, acrescemos), para assegurar a confidencialidade de suas fontes e o segredo de suas comunicações no interesse de seus clientes.[86]

Como advertiu a Corte IDH, a efetiva proteção à vida privada e às liberdades de pensamento e de expressão – diante do "extremo risco de arbitrariedade que implica o uso de técnicas de vigilância, seletiva ou em grande escala, das comunicações,

---

[83] CALABRICH, Bruno. **Proteção de Dados Pessoais na Investigação Criminal e no Processo Penal**: garantismo, eficiência e *standards* de validade. São Paulo: Editora JusPodivm, 2024, p. 117.
[84] CORTE IDH. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia**. Sentencia de 18 de octubre de 2023, § 586-588. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.
[85] CORTE IDH. **Caso CAJAR**, § 624.
[86] CORTE IDH. **Caso CAJAR**, § 555-561.

especialmente em vista das novas tecnologias existentes" – exige que qualquer medida de interceptação, vigilância ou monitoramento de comunicações seja precedida de autorização de uma autoridade competente, cabendo, em princípio, a um juiz decidir sobre sua adequação, "definindo os limites impostos, incluindo o modo, o tempo e o alcance da medida autorizada". [87] Esta também é a posição do TEDH, como se nota no caso *Big Brother Watch e Outros vs. Reino Unidos* (2021):

> A revisão e a supervisão das medidas de vigilância secreta podem ocorrer em três estágios: quando a vigilância é solicitada pela primeira vez, enquanto está sendo executada ou depois de ter sido encerrada. Com relação aos dois primeiros estágios, a própria natureza e lógica do monitoramento sigiloso ditam que não apenas a vigilância em si, mas também a revisão que a acompanha, deve ser realizada sem o conhecimento do indivíduo. Consequentemente, uma vez que o indivíduo será necessariamente impedido de buscar um recurso efetivo por conta própria ou de participar diretamente de qualquer processo de revisão, é essencial que os procedimentos estabelecidos forneçam garantias adequadas e equivalentes que salvaguardem seus direitos. Em um campo no qual o abuso em casos individuais é potencialmente tão fácil e pode ter consequências tão prejudiciais para a sociedade democrática como um todo, a Corte decidiu que, em princípio, é desejável confiar o controle de supervisão a um juiz, pois o controle judicial oferece as melhores garantias de independência, imparcialidade e um procedimento adequado.[88]

Esses julgados continentais mostram que é desejável um procedimento legal que exija prévia autorização judicial, mas este requisito não é imprescindível, pois o controle *ex ante* pode ser exercido por outra autoridade que seja independente do Poder Executivo.[89] Contudo, para a entrada em domicílio e busca e apreensão domiciliar, como regra, a Corte IDH exige a autorização de um juiz, com observância dos requisitos de idoneidade, necessidade e proporcionalidade da ingerência.[90] Quanto às técnicas ou métodos que permitem "o acesso a metadados e dados telemáticos sensíveis como correio eletrônico e metadados de aplicações OTT,[91] dados de localização, endereços IP, estações

[87] CORTE IDH. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia.** Sentencia de 18 de octubre de 2023, § 547. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.

[88] EUROPEAN COURT OF HUMAN RIGHTS. **Case of Big Brother Watch and Others vs. The United Kingdom [GC]**. Judgment 25 May 2021, § 336. Disponível em: https://hudoc.echr.coe.int/fre?i=001-210077.

[89] TEDH: "Turning first to authorisation, the Grand Chamber agrees with the Chamber that while judicial authorisation is an 'important safeguard against arbitrariness' it is not a 'necessary requirement' (see paragraphs 318-320 of the Chamber judgment). Nevertheless, bulk interception should be authorised by an independent body; that is, a body which is independent of the executive. EUROPEAN COURT OF HUMAN RIGHTS. **Case of Big Brother Watch and Others vs. The United Kingdom [GC**]. Judgment 25 May 2021, § 351. Disponível em: https://hudoc.echr.coe.int/fre?i=001-210077.

[90] CORTE IDH. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia.** Sentencia de 18 de octubre de 2023, § 548. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.

[91] Aplicações *Over the Top* (OTT) são serviços de mídia que fazem distribuição de conteúdos pela internet.

de torres celulares, nuvens de dados, GPS e Wi-Fi, exigem também prévia autorização judicial".[92]

Nenhum direito deve estar despido de mecanismos de proteção. No caso *Schrems I,* de 2015, o TEDH previu que "uma regulamentação que permita às autoridades públicas aceder de modo generalizado ao conteúdo das comunicações eletrônicas deve ser considerada lesiva do conteúdo essencial do direito fundamental ao respeito da vida privada". No mesmo julgado, a Corte em Luxemburgo determinou que a legislação dos Estados deve prever alguma via judicial para garantir o acesso aos dados pessoais ou para obter sua retificação ou supressão ou depuração. Só assim haverá o respeito "ao conteúdo essencial do direito fundamental a uma proteção jurisdicional efetiva".[93] Não escapará a um observador atento que, salvo pelo §1º do art. 1º e pelo parágrafo único do art. 3º da Lei 9.883/1999, a lei que instituiu o Sistema Brasileiro de Inteligência (SISBIN) carece de dispositivos desta natureza, sendo necessário recorrer à Lei de Acesso à Informação (LAI), de 2011, em conjunto com a Resolução nº 2/2013-CN.

Neste tópico dos remédios efetivos, a Corte IDH acentuou que:

> [...] a efetividade do direito à autodeterminação informativa exige que os Estados prevejam mecanismos ou procedimentos adequados, ágeis, livres e eficazes para processar e responder, pela mesma autoridade que administra os dados ou por outra instituição competente na área de proteção ou supervisão de dados pessoais (par. 582 supra), às solicitações de acesso e controle desses dados, com prazos razoáveis definidos para sua resolução e sob a responsabilidade de funcionários devidamente capacitados. Esse requisito, derivado do dever estabelecido pelo artigo 2º da Convenção Americana, na medida em que abrange a emissão de regras e o desenvolvimento de práticas conducentes à observância dos direitos humanos, incluindo procedimentos administrativos apropriados, constitui uma garantia essencial para a aplicação e o exercício do direito.[94]

É inegável a importância do caso CAJAR também na jurisdição brasileira. Esse precedente produz efeito *erga omnes* interpretativo, como *res interpretata* interamericana, e merece adoção por todos os órgãos de inteligência e de persecução penal como parâmetro de controle de convencionalidade.

---

[92] CORTE IDH. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia**. Sentencia de 18 de octubre de 2023, nota 690, parte final, p. 167. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.

[93] UNIÃO EUROPEIA. Tribunal de Justiça. **Processo C-362/14,** Maximillian Schrems contra Data Protection Commissioner [GS]. Acórdão de 6 de outubro de 2015, § 94-95. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62014CJ0362.

[94] CORTE IDH. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia.** Sentencia de 18 de octubre de 2023, § 599. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.

Tal exercício é fundamental para o Ministério Público, em função da Recomendação 96/2023 do Conselho Nacional do Ministério Público (CNMP),[95] e da Recomendação 122/2023, do Conselho Nacional de Justiça (CNJ),[96] que exortam juízes, promotores e procuradores a observarem a jurisprudência interamericana. Não foi por outro motivo que, ao decidir o caso *CAJAR*, a Corte IDH reiterou sua jurisprudência constante, segundo a qual:

> [...] quando um Estado ratificou um tratado internacional como a Convenção Americana, todos os seus órgãos, incluindo seus juízes, estão sujeitos a ela, o que os obriga a garantir que os efeitos das disposições da Convenção não sejam diminuídos pela aplicação de normas contrárias a seu objeto e propósito. Consequentemente, os juízes e os órgãos envolvidos na administração da justiça em todos os níveis estão obrigados a exercer ex *officio* um controle de convencionalidade entre as normas internas e a Convenção Americana, obviamente no âmbito de suas respectivas competências e dos regulamentos processuais correspondentes, e nessa tarefa devem levar em conta não apenas o tratado, mas também a interpretação do mesmo pela Corte Interamericana, intérprete final da Convenção Americana. Por sua vez, o controle de convencionalidade requer uma interpretação conjunta do direito interno e do direito internacional, a fim de dar prioridade ao que é mais favorável à proteção dos direitos.[97]

Deste modo, quando juízes, membros do Ministério Público, autoridades policiais e autoridades supervisoras de órgãos de inteligência estiverem diante de um choque entre suas atividades e o direito à autodeterminação informacional, devem "prover a máxima proteção àquele direito", em consonância com a CADH, com a jurisprudência interamericana e com o princípio *pro persona.*[98]

6 PRINCÍPIOS DE PDP APLICÁVEIS AO PROCESSO PENAL E ÀS ATIVIDADES DE INTELIGÊNCIA

Diversos são os princípios que regem a proteção de dados pessoais. Tais preceitos ligam-se a outros direitos, como a inviolabilidade da vida privada (arts. 5º, incisos X, XI e XII, CF) e a autodeterminação informativa (inciso LXXIX), e têm conformação própria.

---

[95] BRASIL. Conselho Nacional do Ministério Público. **Recomendação nº 96, de 28 de fevereiro de 2023.** Recomenda aos ramos e às unidades do Ministério Público a observância dos tratados, convenções e protocolos internacionais de direitos humanos, das recomendações da Comissão Interamericana de Direitos Humanos e da jurisprudência da Corte Interamericana de Direitos Humanos; e dá outras providências.

[96] BRASIL. Conselho Nacional de Justiça. **Recomendação nº 123, de 7 de janeiro de 2022**. Recomenda aos órgãos do Poder Judiciário brasileiro a observância dos tratados e convenções internacionais de direitos humanos e o uso da jurisprudência da Corte Interamericana de Direitos Humanos.

[97] CORTE IDH. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia.** Sentencia de 18 de octubre de 2023, § 649. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.

[98] CORTE IDH. **Caso CAJAR**, § 650.

É o que acontece com o princípio da finalidade, que submete o tratamento de dados pessoais a um propósito limitado e específico, desde que previsto em lei; ou com o princípio da necessidade, que só permite o tratamento de dados para atendimento de uma necessidade legítima, mesmo assim com a adoção dos meios e modos menos intrusivos, qualitativa e quantitativamente (minimização).

Conforme Calabrich, "O processo penal é o campo em que diversos direitos fundamentais precisam ser afirmados e equacionados. A autodeterminação informativa é um destes direitos, mas não é o único nem é aprioristicamente superior aos demais."[99] A Recomendação 15, de 1987, do Comitê de Ministros do Conselho da Europa, lista diversos princípios de PDP – na verdade diretrizes – aplicáveis à atividade policial, a saber: controle e notificação; coleta de dados; armazenamento de dados; uso pela Polícia; compartilhamento de dados; publicidade, direito de acesso e retificação e direito a recurso; tempo de guarda e atualização dos dados; segurança dos dados.[100]

Os princípios da proteção de dados pessoais têm relevância no âmbito das atividades de inteligência e segurança e no processo penal brasileiro, moldando o modo como informações pessoais devem ser tratadas e garantindo a compatibilidade dessas práticas estatais com direitos fundamentais constitucional e convencionalmente consagrados. O §1º do art. 1º da Lei 9.883/1999 deixa claro que o SISBIN opera mediante o respeito à "dignidade da pessoa humana, devendo ainda cumprir e preservar os direitos e garantias individuais e demais dispositivos da Constituição Federal, os tratados, convenções, acordos e ajustes internacionais" de que o Brasil seja parte".[101]

A privacidade constitui o ponto de partida, protegida pela Constituição Federal em seu art. 5º, incisos X, XI e XII, assegurando a inviolabilidade da vida privada. Tal princípio determina que qualquer medida investigativa ou probatória, que envolva a coleta, processamento ou armazenamento de dados pessoais, deve respeitar rigorosamente os limites impostos pela proteção da intimidade e da vida privada do

[99] CALABRICH, Bruno. **Proteção de Dados Pessoais na Investigação Criminal e no Processo Penal**: garantismo, eficiência e *standards* de validade. São Paulo: Editora JusPodivm, 2024, p. 150.
[100] COUNCIL OF EUROPE. **Explanatory Memorandum to Recommendation No. R (87) 15** of the Committee of Ministers to member states regulating the use of personal data in the police sector. Disponível em: https://rm.coe.int/168062dfd4.
[101] BRASIL. **Lei 9.883, de 7 de dezembro de 1999.** Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências

indivíduo, exigindo, assim, uma rigorosa ponderação entre o interesse público na persecução criminal e a esfera de proteção da pessoa humana, sobretudo quanto aos dados sensíveis que podem ser capturados. Esses limites aplicam-se, *mutatis mutandi*, a atividades de segurança pública, para a prevenção do crime e captura de criminosos, como se torna óbvio em programas de reconhecimento facial de pessoas e em projetos como as "muralhas digitais" para cidades seguras.

O direito à PDP não é absoluto, devendo imperar quando haja uma razoável expectativa de privacidade, conforme o entendimento solidificado no ordenamento jurídico norte-americano a partir de *Katz vs. Estados Unidos*, de 1967.[102] No Brasil, esta concepção também vem sendo adotada, como se nota na jurisprudência do Superior Tribunal de Justiça (STJ) sobre o acesso pela Polícia a dados colhidos por câmeras de vigilância em via pública. A Corte Superior decidiu que "a requisição de imagens de logradouros localizados em via pública não está sujeita a cláusula de reserva jurisdicional, pois não se relaciona com a intimidade ou vida privada dos cidadãos".[103] Noutro julgado de 2025, o STJ entendeu que um monitoramento realizado pela Polícia gaúcha não violou o direito à intimidade,

> [...] pois a câmera foi instalada em um poste de energia elétrica, captando imagens da via pública (espaço de acesso coletivo, e não privado), em conformidade com o princípio constitucional da segurança pública. Então, descaracteriza-se ação controlada, prevista no art. 53, II, da Lei 11.343/2006, a exigir autorização judicial. A câmera exclusivamente registrou a movimentação do investigado em espaço público, sem invasão à privacidade protegida constitucionalmente, algo que poderia ser feito por qualquer agente policial de forma presencial, com a natural posterior admissão em juízo a título de prova testemunhal, e a captação por meio de filmagem resguarda a ampla defesa e o contraditório, na medida em que é fidedigna aos fatos.[104]

De igual modo, o STF também fez essa ponderação ao decidir a ADI 5642 em 2024, permitindo o acesso da Polícia ou do Ministério Público a dados de localização de suspeitos, sem prévia autorização judicial, em casos de crimes em curso cometidos contra a liberdade pessoal, indicados no art. 13-A do CPP. São situações de potencial flagrante

[102] Para a ministra Rosa Weber, do STF: "Conforme a doutrina hoje acolhida de forma sólida pela Suprema Corte norte-americana (*Katz test*), é preciso analisar (i) se o indivíduo possui uma real expectativa de privacidade e (ii) se a sociedade, de maneira geral, reconhece como razoável tal expectativa. Balizados por esses critérios, torna-se possível identificar a imprescindibilidade de autorização judicial pelo fato de a medida confundir-se com a busca e apreensão descrita na Quarta Emenda à Constituição daquele país". STF, Pleno, **ADI 5642/DF**, Rel. Min. Edson Fachin, j. em 18/04/2024, voto vista Min. Rosa Weber, p. 29.
[103] STJ, **HC 969.801/SP**, Rel. Min. Sebastião Reis Júnior, Sexta Turma, j. em 20/5/2025.
[104] STJ, **AgRg no RHC 203.030/SC**, Rel. Ministro Carlos Cini Marchionatti (Desembargador Convocado TJRS), Quinta Turma, j. em 01/04/2025.

de crimes graves, com risco atual à vida, liberdade ou integridade física e sexual de vítimas, que levaram à fixação da seguinte tese:

> São passíveis de requisição sem controle judicial prévio, mas sempre sujeito ao controle judicial posterior, a localização de terminal ou IMEI de cidadão em tempo real por meio de ERB por um período determinado e desde que necessário para os fins de reprimir os crimes contra a liberdade pessoal descritos no art. 13-A do Código de Processo Penal; o extrato de ERB; os dados cadastrais dos terminais fixos não figurantes em lista telefônica divulgável e de terminais móveis; o extrato de chamadas telefônicas; o extrato de mensagens de texto (SMS ou MMS); e os sinais para localização de vítimas ou suspeitos, após o decurso do prazo de 12 horas constante do § 4º do art. 13-B do Código de Processo Penal.[105]

A autodeterminação informativa complementa e expande a proteção conferida pela privacidade, estabelecendo que cada indivíduo deve ter controle efetivo sobre seus dados pessoais, podendo decidir livremente sobre o tratamento a que são submetidos, nos limites da lei. No contexto penal, embora existam limitações legítimas decorrentes do interesse estatal em investigar delitos, a autodeterminação informativa exige que o titular seja informado sobre o uso de seus dados sempre que possível, além de estabelecer limites claros e proporcionais à interferência estatal, com a possibilidade de provocação *ex post* do controle judicial.

Já o princípio da finalidade é particularmente crítico nas atividades de inteligência, segurança e no processo penal. Neste último campo, nota-se sua presença no inciso XII do art. 5º da Constituição, que determina que os dados pessoais obtidos durante investigações e procedimentos judiciais sejam utilizados exclusivamente para propósitos específicos, legítimos e transparentes.[106] Isso significa que qualquer desvio ou uso secundário de informações deve ser coibido, preservando-se assim a confiança pública e prevenindo abusos institucionais.

A necessidade ou minimização exige que autoridades policiais, ministeriais e judiciais empreguem sempre os métodos menos intrusivos no tratamento de dados pessoais. A adoção deste princípio orienta-se pela busca constante da proporcionalidade, limitando o impacto das medidas penais sobre os direitos fundamentais. Desta forma, as diligências e técnicas investigativas devem ser cuidadosamente avaliadas quanto à sua

[105] STF, Pleno, **ADI 5642/DF**, Rel. Min. Edson Fachin, j. em 18/04/2024.
[106] Cuidando do arts. 13-A e 13-B do CPP, o STF decidiu: "A requisição apresentada pela autoridade policial, exclusivamente para os crimes previstos no art. 13-A do Código de Processo Penal, conquanto possível, deve se restringir apenas à finalidade a que foi fixada, qual seja, a de reprimir e impedir a ocorrência dos delitos descritos no caput, do citado dispositivo". STF, Pleno, **ADI 5642/DF**, Rel. Min. Edson Fachin, j. em 18/04/2024.

indispensabilidade e eficácia, evitando-se a coleta excessiva e desnecessária de informações pessoais.

A separação informacional também deve ter algum relevo na persecução criminal, especialmente na interseção entre atividades de inteligência e de investigação criminal, de modo que a execução de medidas que recaem diretamente sobre pessoas, como prisões, não sejam permitidas a agências de inteligência. Para a Corte IDH, em consonância com padrões internacionais,[107] é preciso "diferenciar as faculdades específicas a cargo dos organismos de inteligência das tarefas próprias de segurança pública, pois atribuí-las indistintamente àqueles poderia causar um risco maior de arbitrariedade e, depois, de vulneração dos direitos humanos".[108] Sobre isso, Calabrich leciona que o princípio da separação informacional:

> [...] tem como corolário a compartimentação dos bancos de dados administrados por órgãos públicos. Isso significa que cada órgão será responsável pela custódia e o tratamento dos dados que coleta e administra, não podendo simplesmente transferir essa responsabilidade mediante a cessão da integralidade desse banco de dados a outros entes. O princípio da separação informacional não implica que dados pessoais armazenados em seus bancos de dados não possam ser entregues a outros órgãos públicos. Ao revés: havendo razões de fato e direito, que hão de ser declaradas em ato devidamente registrado e auditável, o acesso a dados armazenados em bancos controlados por outros entes públicos deve ser facilitado.[109]

Por fim, os princípios de segurança e responsabilização demandam uma atuação diligente das autoridades em relação à integridade dos dados pessoais coletados, armazenados e processados no contexto das atividades de inteligência, segurança pública e de persecução penal. A obrigação do Estado é dupla: prevenir ameaças e violações, por meio de políticas robustas de segurança da informação, e responsabilizar claramente aqueles que praticarem abusos ou permitirem negligentemente o vazamento ou uso indevido de dados pessoais. Somente com essa rigorosa observância dos princípios citados se pode garantir um processo penal democrático, justo e respeitoso aos direitos fundamentais e atividades de inteligência e segurança pública aderentes à Constituição e

[107] UNITED NATIONS. Human Rights Council. Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, **A/HRC/14/46**, 17 May 2010, Boa Prática 27. Disponível em: https://documents.un.org/doc/undoc/gen/g10/134/10/pdf/g1013410.pdf.

[108] CORTE IDH. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia**. Sentencia de 18 de octubre de 2023, § 549. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.

[109] CALABRICH, Bruno. **Proteção de Dados Pessoais na Investigação Criminal e no Processo Penal**: garantismo, eficiência e *standards* de validade. São Paulo: Editora JusPodivm, 2024, p. 277.

aos tratados de direitos humanos. Neste aspecto, vale lembrar do conjunto de dispositivos, no Código Penal, na Lei 9.296/1996, na Lei 13.869/2019 e na Lei Complementar 105/2001 que se ocupam da tutela penal dos segredos.

Leis que autorizam interceptações ou quebras de sigilo ou busca e apreensão de dados ou acesso a dados devem ser lidas à luz desses princípios. Devem também conciliar-se com alguma forma de controle judicial, que pode ser *ex ante* (como no caso das buscas e apreensões e interceptações) ou *ex post* (como se dá na prisão em flagrante e no intercâmbio de informações com a unidade de inteligência financeira).[110]

7 COOPERAÇÃO INTERNACIONAL E TRANSFERÊNCIA INTERNACIONAL DE DADOS

A atividade de cooperação internacional, especialmente a de natureza probatória – por meio de acordos de assistência jurídica mútua – e a cooperação para fins de captura de foragidos – mediante tratados de extradição e de acordos de detenção e entrega – levam ao trânsito transnacional de uma grande quantidade de dados pessoais. Este cenário se repete nos casos de rastreamento, bloqueio e confisco de bens no exterior.

A transferência internacional de dados de pessoais é uma das formas de tratamento. Deve, portanto, reger-se pelos princípios próprios de PDP e observar o direito à autodeterminação informativa, na medida do possível, tendo em vista a confidencialidade, em regra, dos pedidos de cooperação jurídica internacional em matéria penal. Apesar de uma forte tendência à adoção de normas sobre soberania digital, sobretudo com determinações de *data localisation*,[111] a União Europeia adotou e projeta

[110] STF: "É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil - em que se define o lançamento do tributo - com os órgãos de persecução penal para fins criminais sem prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional". STF. Pleno, **RE 1.055.941/SP**, Tema 990 da Repercussão Geral, Rel. Min. Dias Toffoli, j. em 04/12/2019. No mesmo sentido: STF, **Recl 81.531/DF**, Rel. Min. Cármen Lúcia, d. em 15 jul. 2025.

[111] Para a OCDE, a expressão *data localisation* refere-se à exigência expressa de que os dados sejam armazenados ou processados dentro do território de um Estado. DEL GIOVANE, Chiara; FERENCZ, Janos; LÓPEZ-GONZÁLEZ, Javier. The Nature, Evolution and Potential Implications of Data Localisation Measures. **OECD Trade Policy Papers,** No. 278, OECD Publishing, Paris, 2023. Disponível em: https://doi.org/10.1787/179f718a-en.

um modelo de livro fluxo de dados, dentro do seu esquema das "cinco liberdades".[112] O livre fluxo de dados pessoais na esfera internacional é salutar para o comércio exterior e para inúmeras atividades econômicas, notadamente no ciberespaço e na criptoeconomia.

Como se nota na jurisprudência da União Europeia, sobretudo nos casos *Schrems I* (2015) [113] e *Schrems II* (2020),[114] a transferência internacional de dados pessoais exige que o Estado de destino das informações ofereça um nível de proteção adequada, para assegurar os direitos do titular contra eventuais ingerências noutro Estado, especialmente por seus órgãos de inteligência e de persecução criminal.

7.1 Convenção de Budapeste

A adesão do Brasil à Convenção de Budapeste,[115] de 2001, viabilizou a introdução no ordenamento jurídico brasileiro de mecanismos probatórios essenciais ao enfrentamento da cibercriminalidade e à obtenção de provas digitais de *cybercrimes* e de crimes não digitais ("analógicos").[116]

Diligências de interceptação de comunicações, busca e apreensão de dados e preservação rápida de dados informáticos, acesso a tais dados e seu fornecimento transfronteiriço também se orientam pelas regras de PDP e estão sujeitas em alguma medida à autodeterminação informativa, desde que respeitados a confidencialidade

---

[112] AKKERMANS, Bram. The influence of the four (or five) freedoms on property law. *In*: ERP, Sjef van; ZIMMERMANN, Katja (Orgs.). **Research Handbook on European Property Law**. Cheltenham, UK ; Northampton, MA: Edward Elgar Publishing, 2024, p. 18–27.

[113] UNIÃO EUROPEIA. Tribunal de Justiça. **Processo C-362/14**, Maximillian Schrems contra Data Protection Commissioner [GS]. Acórdão de 6 de outubro de 2015, § 94-95. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62014CJ0362.

[114] UNIÃO EUROPEIA. Tribunal de Justiça. **Processo C-311/18**, Data Protection Commissioner contra Facebook Ireland Ltd, Maximilian Schrems et al. Acórdão de 16 de julho de 2020, § 188. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=10257253.

[115] BRASIL. **Decreto 11.491, de 12 de abril de 2024**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001.

[116] Existe controvérsia se os procedimentos probatórios previstos na Convenção de Budapeste podem ser aplicados diretamente (como parece ser o caso em virtude da aplicação do art. 1º, inciso I, do CPP), ou se há necessidade de regulamentação de tais medidas por lei interna, em função do art. 14 do tratado, que diz: "Cada Parte adotará medidas legislativas e outras providências necessárias para estabelecer os poderes e procedimentos previstos nesta seção para o fim específico de promover investigações ou processos criminais." Ademais, a expressão "Cada Parte adotará medidas legislativas..." aparece nos artigos 16 a 21 da Convenção.

exógena do procedimento cooperacional e o interesse público na utilidade dessas vias investigativas.

Já no seu preâmbulo, a Convenção do Conselho da Europa sobre cibercrimes – que leva o número 185 na série de tratados europeus – anuncia a preocupação dos Estados Partes "com o direito à proteção de dados pessoais, como previsto, por exemplo, na Convenção Europeia para a Proteção de Dados Pessoais sujeitos a Processamento Eletrônico, de 1981". Como vimos, cuida-se da Convenção 108, do COE, o que torna evidente a necessidade de o Brasil também aderir a ela, para ampliar o status do País como um Estado com nível de proteção adequada para o tratamento de dados pessoais. Esse patamar assegura o livre fluxo de dados pessoais para o Brasil na persecução criminal.

O art. 15, §1º, da Convenção de Budapeste não deixa dúvidas da importância da conciliação das atividades de persecução criminal cibernética com os direitos fundamentais no processo penal, uma vez que exige que cada Parte observe o princípio da proporcionalidade e assegure que sua atividade probatória se sujeite a requisitos e garantias do direito interno e "proteção adequada aos direitos humanos e às liberdades públicas", o que inclui o Pacto Internacional de Direitos Civis e Políticos (PIDCP) e "outros instrumentos internacionais de direitos humanos".[117]

7.2 Interpol

Criada em 1923 e renovada em 1956, a Interpol é a Organização Internacional de Polícia Criminal. É a mais antiga instituição de cooperação internacional no campo penal.

A cooperação internacional promovida pelo Brasil através da Interpol tem implicações significativas em termos de proteção de dados pessoais, sobretudo quando as autoridades competentes solicitam a inserção das chamadas "difusões" (*diffusions*) e "alertas" (*notices*)[118] que contêm informações sensíveis como dados biográficos e

[117] BRASIL. **Decreto 11.491, de 12 de abril de 2024**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001.

[118] Segundo o art. 82 das Regras sobre Processamento de Dados (RDP) da Interpol, "Red notices are published at the request of a National Central Bureau or an international entity with powers of investigation and prosecution in criminal matters in order to seek the location of a wanted person and his/her detention, arrest or restriction of movement for the purpose of extradition, surrender, or similar lawful action". INTERPOL. **INTERPOL's Rules on the Processing of Data**. III/IRPD/GA/2011 (2024). Disponível em: https://www.interpol.int/content/download/5694/file/27%20E%20RulesProcessingData_RPD_2024.pdf.

biométricos de pessoas procuradas, sejam foragidos (difusão vermelha), menores abduzidos ou pessoas desaparecidas (difusão amarela).[119]

A conformidade com as normas internacionais de proteção de dados pessoais impõe à Interpol o dever de assegurar mecanismos eficazes, rápidos e transparentes de revisão e exclusão dessas informações, sempre que houver necessidade. A ausência de tais mecanismos pode levar a discriminações indevidas, violações de direitos fundamentais e responsabilizações internacionais.[120]

A Comissão de Controle dos Arquivos da Interpol (CCF) é o órgão responsável pela execução da política de PDP da Organização. A C*ommission for the Control of Interpol's Files* (CCF) é um órgão independente responsável por garantir que todos os dados pessoais processados pelos canais da Interpol observem as regras da Organização, especialmente as *Rules on the Processing of Data* (RPD), de 2011,[121] e o Estatuto do CCF, de 2016.[122] Sua função principal é garantir a conformidade com as regras aplicáveis relativas ao processamento de dados pessoais, incluindo nomes, fotos, características de identificação e impressões digitais, que são processados em grandes volumes por meio de difusões e avisos da Interpol.[123]

As Regras da Interpol sobre PDP, consolidadas nas RPD, seguem os princípios fundamentais de proteção de dados, em harmonia com instrumentos internacionais e regionais, "tais como legalidade, limitação da finalidade, qualidade dos dados,

---

[119] Diz o art. 90 das RPD: "Yellow notices are published to locate a missing person or to identify a person unable to identify himself/herself." INTERPOL. **INTERPOL's Rules on the Processing of Data**. III/IRPD/GA/2011 (2024). Disponível em: https://www.interpol.int/content/download/5694/file/27%20E%20RulesProcessingData_RPD_2024.pdf.

[120] INTERPOL**. Background Note on Interpol's Information System Safeguards for the Processing of Personal Data**. Lyon, 2019.

[121] INTERPOL: "The aim of the present Rules is to ensure the efficiency and quality of international cooperation between criminal police authorities through INTERPOL channels, with due respect for the basic rights of the persons who are the subject of this cooperation, in conformity with Article 2 of the Organization's Constitution and the Universal Declaration of Human Rights to which the said Article refers". INTERPOL. **INTERPOL's Rules on the Processing of Data**. III/IRPD/GA/2011 (2024). Disponível em: https://www.interpol.int/content/download/5694/file/27%20E%20RulesProcessingData_RPD_2024.pdf.

[122] INTERPOL. **Statute of the Commission for the Control of INTERPOL's Files**. II.E/RCIA/GA/2016. Disponível em: https://www.interpol.int/content/download/5695/file/Statute%20of%20the%20CCF-EN.pdf.

[123] INTERPOL. **Commission for the Control of INTERPOL's Files (CCF).** Disponível em: https://www.interpol.int/en/Who-we-are/Commission-for-the-Control-of-INTERPOL-s-Files-CCF.

transparência, confidencialidade e segurança".[124] Além disso, a Regra 18 prevê expressamente o "direito de acesso, correção e exclusão de dados por meio da apresentação de uma solicitação ao CCF".[125] Qualquer pessoa tem o direito de solicitar acesso aos dados sobre si mesma mantidos nos arquivos da Interpol, em Lyon, na França. Cabe à CCF processar as solicitações de acesso, retificação ou exclusão de dados pessoais.[126]

Nas relações com a Interpol, as autoridades brasileiras – sobretudo a Polícia Federal que a representa no Brasil – devem observar as normas de proteção de dados pessoais vigentes na organização, inclusive quando solicitam a inclusão de pessoas nas difusões e alertas. Os impropriamente chamados mandados internacionais de captura, que se convertem em *red notices* no sistema de informações da Interpol, podem ter sua inclusão rechaçada ou retificada mediante a aplicação dessas regras. Essas inclusões também podem ser suprimidas a pedido das pessoas atingidas, se os requisitos das RPD não forem observados.

7.3. Europol

A Europol é o serviço europeu de polícia judiciária. Essa entidade supranacional submete-se ao ordenamento da União Europeia, sendo regida por uma série de atos legislativos que evoluíram ao longo do tempo para se adaptar às necessidades políticas e operacionais em constante mudança no campo da PDP.

Inicialmente estabelecida pela Convenção Europol em 1995, a agência tem sua atual estrutura normativa definida pelo Regulamento da Europol, que descreve as funções, as responsabilidades e os mecanismos de cooperação da agência com outras instituições da União Europeia.[127] Esse regulamento enfatiza as atribuições de coleta de

[124] INTERPOL**. Background Note on Interpol's Information System Safeguards for the Processing of Personal Data**. Lyon, 2019.
[125] INTERPOL. **INTERPOL's Rules on the Processing of Data**. III/IRPD/GA/2011 (2024). Disponível em: https://www.interpol.int/content/download/5694/file/27%20E%20RulesProcessingData_RPD_2024.pdf.
[126] CHEAH, W. L. Policing Interpol: The Commission for the Control of Interpol's Files and the Right to a Remedy. **International Organizations Law Review**, v. 7, n. 2, p. 375–404, Jan. 2010.
[127] UNIÃO EUROPEIA. **Regulamento (UE) 2016/794** do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol). Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:32016R0794.

informações e de participação em equipes conjuntas de investigação para lidar com o crime organizado.[128]

Suas atividades têm implicações sobre a privacidade e a PDP, razão pela qual o art. 28 do Regulamento UE 2016/794 estabelece que os dados pessoais sujeitos a tratamento pela Europol são colhidos para fins específicos, explícitos e legítimos, "e não são tratados ulteriormente de forma incompatível com essas finalidades".

Ademais, os dados pessoais colhidos são apenas os "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para que são tratados". Devem ser exatos e atualizados, cabendo à Europol apagar os dados inexatos ou retificá-los sem demora. O regulamento também exige que os dados sejam "conservados de forma a permitir a identificação dos titulares dos dados apenas durante o período necessário para a prossecução das finalidades para que são tratados" e que haja segurança cibernética ou digital, para evitar vazamentos ou divulgações indevidas.[129]

A Europol não opera diretamente no Brasil, mas tem uma intensa cooperação com a Polícia Federal. O acordo firmado entre nosso País e a União Europeia em 2017, estabelecendo cooperação policial entre a Polícia Federal brasileira e a Europol, tornou-se um marco importante na expansão das capacidades nacionais no combate ao crime organizado transnacional. Tal acordo, contudo, não permite o intercâmbio de dados pessoais, por vedação expressa do seu art. 1º. Isso se deve ao momento de sua celebração, 2017, quando ainda não tínhamos nem sequer a LGPD comum.[130] Para contornar essa limitação, em 2025, foi celebrado em Brasília um novo acordo entre as Partes, com maior abrangência e regras mais robustas de PDP,[131] que deverão ser observadas pela Polícia Federal no tratamento de dados pessoais no Brasil.

---

[128] ORLANDI, E. Corporate Governance in EU Agencies: The Europol Case. **Journal of entrepreneurship and business development**, [*s. l.*], v. 1, n. 1, p. 20–32, 2021. Disponível em: https://doi.org/10.18775/jebd.11.5003.

[129] UNIÃO EUROPEIA. **Regulamento (UE) 2016/794** do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol). Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:32016R0794.

[130] BRASIL. **Decreto 10.364, de 21 de maio de 2020**. Promulga o Acordo de Cooperação Estratégica entre a República Federativa do Brasil e o Serviço Europeu de Polícia, firmado em Haia, em 11 de abril de 2017

[131] BRASIL. **Ministério da Justiça**. Ministério da Justiça e da Segurança Pública. Brasil e União Europeia assinam acordo para cooperação entre a Polícia Federal e a Europol, Brasília, 5 de março de 2025. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/brasil-e-uniao-europeia-assinam-acordo-para-cooperacao-entre-a-policia-federal-e-a-europol.

A novo acordo contém regras que asseguram o respeito a princípios e obrigações em matéria de PDP, especialmente as dos arts. 3º, 4º, 5º, 7º, 10º, 11, 12, 13, 18 e 19. Há também dispositivos sobre direitos individuais nos arts. 6º, 8º e 9º, previsão de um controle independente (art. 14) e vias de recurso administrativo e judicial eficazes em caso de violação dos direitos e garantias reconhecidos no acordo (art. 15).[132] Quando estiver em vigor, as informações pessoais recebidas da Europol no Brasil deverão receber um nível de proteção adequada, inclusive nas chamadas transferências subsequentes (*onward transfers*).

Conforme o art. 7º do futuro tratado, o Estado brasileiro deverá assegurar que os dados pessoais só podem ser retransmitidos dentro do Brasil mediante prévia autorização expressa da Europol, para os mesmos fins de sua transferência inicial, mantendo-se as condições e garantias aplicáveis à transmissão original. Apesar da limitada lista de "autoridades brasileiras" legitimadas no anexo II,[133] a regra não deve causar problemas para o compartilhamento de dados com o Ministério Público e o Judiciário, mas pode resultar em limitações para difusão dessas informações no âmbito do SISBIN.

7.4 Eurojust

A Agência da União Europeia para a Cooperação Judiciária Penal (Eurojust) foi criada para reforçar a cooperação judiciária entre os Estados-Membros da UE na luta contra a criminalidade transfronteiriça grave. Inicialmente concebida no Conselho Europeu de Tampere, em 1999, a Eurojust foi formalmente constituída em 2002, evoluindo de uma unidade provisória de cooperação judiciária para uma agência da UE de pleno direito com personalidade jurídica.[134]

---

[132] EUROPEAN UNION. **European Commission. Proposal for a Council Decision on the signing, on behalf of the European Union, of the Agreement between the European Union and the Federative Republic of Brazil on cooperation with and through the European Union Agency for Law Enforcement Cooperation (Europol) and the Federal Police of Brazi**l. Brussels, 18 December 2024. COM(2024) 581 final. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52024PC0581.

[133] A Polícia Federal, as Polícias Civis dos Estados e do Distrito Federal e unidades especializadas em prevenção e repressão ao crime do Ministério da Justiça.

[134] NILSSON, Hans G. Article 85 [Eurojust]. *In*: **Treaty on the Functioning of the European Union**: a commentary. [s.l.] Springer, Cham, 2021. p. 1603–1622.

A principal função da agência é facilitar e coordenar as investigações e ações penais em todos os países da UE, abordando as complexidades da criminalidade transnacional que muitas vezes exigem colaboração além das fronteiras da União. A estrutura e o mandato da Eurojust foram significativamente moldados pelo Tratado de Lisboa e pelo Regulamento (UE) 2018/1727.[135]

A posição única da Eurojust permite-lhe atuar como elo entre as autoridades judiciárias nacionais (*lato sensu*) e entre estas e Estados terceiros, promovendo a confiança mútua e reforçando o Estado de direito no Espaço de Liberdade, Segurança e Justiça da União.[136]

Desde o início do século 20, a Procuradoria-Geral da República funciona como *Contact Point* da Eurojust no Brasil, para as atividades de cooperação entre o Parquet brasileiro e os Ministérios Públicos e juízes de instrução da União Europeia. Desde 2014, a PGR vem buscando assegurar um acordo de cooperação entre o Brasil e a agência, para viabilizar também a criação de procuradores de ligação (*liaison prosecutors*) entre as Partes. Um dos óbices desde então foi a falta de uma legislação brasileira de PDP no âmbito processual penal, o que, entre outros fatores, impedia o reconhecimento do Brasil como um Estado com um nível de proteção adequado para o tratamento de dados pessoais.[137]

O Regulamento da Eurojust, de 2018, contém diversas regras de PDP, relativas ao tratamento de dados pela agência, o compartilhamento de dados intra-UE e a transferência internacional de dados para Estados terceiros, como se vê, neste último caso, nos arts. 56 a 59. Conforme o considerando 50 desse Regulamento, se a Agência identificar uma necessidade operacional de cooperação com um país terceiro, pode solicitar à Comissão Europeia em Bruxelas que emita uma decisão de adequação ou uma recomendação de

[135] UNIÃO EUROPEIA. **Regulamento (UE) 2018/1727** do Parlamento Europeu e do Conselho de 14 de novembro de 2018 que cria a Agência da União Europeia para a Cooperação Judiciária Penal (Eurojust). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32018R1727.

[136] ŠKRLEC, B. Eurojust and External Dimension of EU Judicial Cooperation. **Eucrim**, n. 3, p. 188–193, 2019. Disponível em: https://doi.org/10.30709/EUCRIM-2019-018.

[137] O autor participou pessoalmente dessa negociação, quando ocupava o cargo de Secretário de Cooperação Internacional da PGR (2013-2017).

abertura de negociações sobre um acordo internacional nos termos do artigo 218 do Tratado sobre o Funcionamento da União Europeia (TFUE).[138]

As transferências internacionais de dados que não sejam baseadas numa decisão de adequação da Comissão Europeia só podem ocorrer se houver garantias adequadas num instrumento juridicamente vinculante que assegure a proteção dos dados pessoais ou caso a Eurojust tenha avaliado todas as circunstâncias inerentes à transferência de dados e, com base nessa avaliação, considere que existem garantias adequadas no que diz respeito à proteção de dados pessoais no país de destino.

> Tais instrumentos [...] poderão ser, por exemplo, acordos bilaterais juridicamente vinculativos que os Estados-Membros tenham celebrado e integrado no seu ordenamento jurídico e que possam ser executados pelos titulares de dados desses Estados-Membros, assegurando a observância dos requisitos relativos à proteção de dados e dos direitos dos titulares dos dados, incluindo o direito de recurso administrativo ou judicial. Ao avaliar todas as circunstâncias relativas à transferência de dados, a Eurojust deverá ter em conta os acordos de cooperação que tenham sido celebrados entre a Eurojust e países terceiros e que permitam o intercâmbio de dados pessoais. A Eurojust deverá ainda ter em conta que a transferência de dados pessoais ficará sujeita a obrigações de confidencialidade e ao princípio da especificidade, assegurando que os dados não sejam tratados para efeitos que não sejam os da transferência. Além disso, a Eurojust deverá ter em conta que os dados pessoais não serão utilizados para requerer, aplicar ou executar uma pena de morte ou qualquer forma de tratamento cruel ou desumano. Embora essas condições possam ser consideradas garantias adequadas para a transferência de dados, a Eurojust deverá poder exigir garantias adicionais.[139]

Em 2021, a Comissão Europeia foi autorizada a iniciar a negociação de um acordo deste tipo com o Brasil, para estabelecer uma base jurídica para cooperação judicial em matéria penal com a Eurojust, incluindo a troca de dados pessoais operacionais. O tratado deverá ter foco na investigação e repressão de crimes graves – como terrorismo, crime organizado, tráfico de armas, drogas, tráfico de pessoas, contrabando migratório e cibercrimes –, garantindo a proteção de dados e direitos fundamentais conforme os regulamentos da União Europeia[140] e a legislação brasileira.

---

[138] UNIÃO EUROPEIA. **Regulamento (UE) 2018/1727** do Parlamento Europeu e do Conselho de 14 de novembro de 2018 que cria a Agência da União Europeia para a Cooperação Judiciária Penal (Eurojust). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32018R1727.

[139] UNIÃO EUROPEIA. **Regulamento (UE) 2018/1727** do Parlamento Europeu e do Conselho de 14 de novembro de 2018 que cria a Agência da União Europeia para a Cooperação Judiciária Penal (Eurojust), Considerando 51. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32018R1727.

[140] EUROPEAN UNION. Council Decision authorising the opening of negotiations for Agreements between the European Union and Algeria, Argentina, Armenia, Bosnia and Herzegovina, Brazil, Colombia, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey on cooperation between the European Union Agency for Criminal Justice Cooperation (Eurojust) and the competent authorities for judicial cooperation in criminal matters of those third States. Brussels, 23 February 2021, 6153/21 + ADD1. **Council Decision**

Entre os princípios de PDP que devem constar desse acordo estão os da limitação da finalidade (relacionada às competências da Eurojust), com vedação de uso subsequente ou com esse uso estritamente regulado. É exigida a qualidade dos dados, quanto à sua adequação, precisão e atualização, com previsão de retenção limitada ao tempo estritamente necessário e revisão periódica obrigatória, atendida a proporcionalidade.

Um futuro acordo deve considerar medidas de proteção especial a dados sensíveis (políticos, biométricos, sobre saúde, vida sexual, etc.); garantias individuais de acesso, retificação, supressão e restrição de dados, salvo exceções justificadas e proporcionais, com remédios administrativos e judiciais efetivos; segurança e confidencialidade dos dados, mediante a adoção de técnicas organizacionais para assegurar a integridade, confidencialidade e acesso restrito aos dados; obrigação de notificação imediata em caso de violação de dados; e regulamentação restritiva de transferências subsequentes (*onward transfers*), que só serão permitidas se houver alinhamento à finalidade original e com autorização prévia da Eurojust.

De igual modo, transferências a outros países só são permitidas se a Eurojust também tiver fundamento legal para elas, conforme art. 56(2) do Regulamento UE 2018/1727. Por fim, o acordo deve prever supervisão de sua execução por autoridades independentes de proteção de dados com poder de investigação, intervenção e mecanismos de resposta a reclamações à disposição das pessoas prejudicadas.[141]

7.5 Equipes conjuntas de investigação

As equipes conjuntas de investigação (ECI) são instrumentos cada vez mais importantes para a cooperação transnacional, permitindo que as autoridades judiciais, ministeriais e policiais de diferentes Estados coordenem ações e partilhem resultados probatórios de forma eficaz.[142] Estas forças-tarefas multinacionais são particularmente úteis na luta contra crimes graves, como o terrorismo e a delinquência organizada, embora

adopted by written procedure on 1 March 2021 (CM 1990/21). Disponível em: https://www.statewatch.org/media/1972/eu-council-eurojust-agreements-negotiating-directives-6153-21-add1.pdf.

[141] EUROPEAN UNION. **Council Decision adopted by written procedure on 1 March 2021 (CM 1990/21)**, op. cit.

[142] GERACI, R. Beyond mutual recognition: the rules of joint investigation teams. **Optime**, [*s. l.*], v. 13, n. 2, p. 29–40, 2022. Disponível em: https://doi.org/10.55312/op.v13i2.378.

persistam desafios relacionados a seus elevados custos operacionais e ao respeito aos direitos dos investigados.[143]

A eficácia das ECIs na efetivação do *rule of law* em matéria criminal transnacional é sublinhada pela sua capacidade de simplificar a assistência jurídica e melhorar a coleta e a análise de provas.[144] Uma de suas primeiras aparições se deu no art. 13 da Convenção relativa ao Auxílio Judiciário Mútuo em Matéria Penal entre os Estados da União Europeia, do ano 2000:

> As autoridades competentes de dois ou mais Estados-Membros podem criar, de comum acordo, uma equipa de investigação conjunta para um objetivo específico e por um período limitado, que poderá ser prolongado com o acordo de todas as partes, para efetuar investigações criminais num ou em vários dos Estados-Membros que criarem a equipa. A composição da equipa será indicada no acordo.[145]

Para o Brasil, as chamadas *joint investigative teams (JIT)* estão previstas no art. 9.1.c da Convenção de Viena de 1988, sobre o Tráfico Ilícito de Entorpecentes;[146] no art. 19 da Convenção das Nações Unidas contra o Crime Organizado Transnacional, concluída em Palermo no ano 2000 (UNTOC);[147] e no art. 49 da Convenção das Nações Unidas contra a Corrupção, concluída em Mérida, em 2003 (UNCAC)[148].

No âmbito regional, foi firmado o Acordo Marco de Cooperação entre os Estados Partes do Mercosul e Estados Associados para a Criação de Equipes Conjuntas de

---

[143] SOUZA, Isac Barcelos Pereira. **Equipes Conjuntas de Investigação na cooperação jurídica internacional em matéria penal**. Salvador: JusPodivm, 2019.

[144] EGAMBERDIYEV, D. Type of legal assistance in criminal cases creation of joint investigation teams – on the example of eu countries. **International Journal of Law and Criminology**, [*s. l.*], 2023. Disponível em: https://doi.org/10.37547/ijlc/volume03issue06-15.

[145] UNIÃO EUROPEIA. **Convenção da União Europeia, relativa ao Auxílio Judiciário Mútuo em Matéria Penal entre os Estados Membros da União Europeia**, assinada em Bruxelas em 29 de maio de 2000. Disponível em: https://dcjri.ministeriopublico.pt//sites/default/files/documentos/instrumentos/convencao_aux_judiciario_mutuo_mat_penal_entre_est_membros_ue.pdf.

[146] Convenção de Viena de 1988: "c) quando for oportuno, e sempre que não contravenha o disposto no direito interno, criar equipes conjuntas, levando em consideração a necessidade de proteger a segurança das pessoas e das operações, para dar cumprimento ao disposto neste parágrafo. Os funcionários de qualquer umas das Partes, que integrem as equipes, atuarão de acordo com a autorização das autoridades competentes da Parte em cujo território se realizará a operação. Em todos os casos, as Partes em questão velarão para que seja plenamente respeitada a soberania da parte em cujo território se realizará a operação". BRASIL. **Decreto 154, de 26 de junho de 1991.** Promulga a Convenção Contra o Tráfico Ilícito de Entorpecentes e Substâncias Psicotrópicas.

[147] BRASIL. **Decreto 5.015, de 12 de março de 2004**. Promulga a Convenção das Nações Unidas contra o Crime Organizado Transnacional, concluída em Palermo em 2000.

[148] BRASIL. **Decreto 5.687, de 31 de janeiro de 2006**. Promulga a Convenção das Nações Unidas contra a Corrupção, adotada pela Assembleia-Geral das Nações Unidas em 31 de outubro de 2003 e assinada pelo Brasil em 9 de dezembro de 2003.

Investigação (Acordo de San Juan, de 2010). Resultante da Decisão CMC 22/2010, este tratado entrou em vigor para o Brasil em 2020. As autoridades competentes de um Estado do Mercosul encarregadas de uma investigação criminal podem solicitar a criação de uma ECI às autoridades competentes de outra Parte, "quando essa investigação tiver por objeto condutas delituosas que por suas características exijam a atuação coordenada de mais de uma Parte".[149]

Fora do ambiente convencional, o art. 5º, inciso III, da Lei 13.344/2016 (Lei do Tráfico de Pessoas) incentiva a formação de equipes conjuntas ou mistas de investigação para apuração desse tipo de delinquência. Tais JITs podem ser constituídas com base em acordos específicos (*ad hoc*) ou sobre uma base convencional mais geral, quando dois ou mais Estados tenham jurisdição sobre um mesmo fato (jurisdição concorrente), com o objetivo de coordenar a persecução criminal transnacional.[150]

Os temas de PDP se apresentam intensamente nessa ferramenta cooperacional, uma vez que a transferência de dados pessoais se fará internacionalmente, entre as agências policiais e os Ministérios Públicos integrantes da ECI. Lidando com o tema da utilização da prova, o art. 11 do Acordo de San Juan determina que as provas e informações "obtidas em virtude da atuação da ECI somente poderão ser utilizadas nas investigações que motivaram sua criação, salvo acordo em contrário das Autoridades Competentes". Ademais, "as Autoridades Competentes poderão acordar que a informação e a prova obtidas, em virtude da atuação da ECI, tenham caráter confidencial."[151]

7.6 Intercâmbio internacional de informações tributárias

[149] BRASIL. **Decreto 10.452, de 10 de agosto de 2020**. Promulga o texto do Acordo Quadro de Cooperação entre os Estados Partes do Mercosul e Estados Associados para a Criação de Equipes Conjuntas de Investigação, firmado pela República Federativa do Brasil, em San Juan, em 2 de agosto de 2010.
[150] ARAS, Vladimir. Direito probatório e cooperação jurídica internacional. *In*: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Orgs.). **A prova no enfrentamento à macrocriminalidade**. 2.ed. Salvador: JusPodivm, 2016, p. 315–382.
[151] BRASIL. **Decreto 10.452, de 10 de agosto de 2020**. Promulga o texto do Acordo Quadro de Cooperação entre os Estados Partes do Mercosul e Estados Associados para a Criação de Equipes Conjuntas de Investigação, firmado pela República Federativa do Brasil, em San Juan, em 2 de agosto de 2010.

Acordos bilaterais e multilaterais de troca de informações tributárias também implicam a transferência internacional de dados e, por isso mesmo, costumam conter dispositivos de PDP.

É o caso da Convenção da OCDE e do COE, de 2011, cujo art. 22 estabelece que as informações pessoais obtidas pelos Estados Partes

> [...] serão consideradas sigilosas e protegidas do mesmo modo que as informações obtidas com base na legislação interna dessa Parte e, na medida necessária para garantir o nível necessário de proteção de dados de caráter pessoal, em conformidade com as salvaguardas exigidas por força da legislação interna da Parte que presta as informações e por ela especificadas.[152]

Dando eficácia ao princípio da finalidade, o §2º do art. 22 dessa Convenção proíbe que os dados pessoais obtidos por esse canal de cooperação administrativa tributária sejam utilizados para outro propósito, diverso da arrecadação e cobrança de tributos.

Contudo, esta limitação não é absoluta, pois o §4º do art. 22 autoriza que tais informações sejam utilizadas para outros fins, se a legislação da Parte que forneceu as informações permitir e se a autoridade competente desse Estado concordar com essa utilização. Esta regra viabiliza o uso dos dados para fins penais tributários e eventualmente para a persecução de lavagem de dinheiro. De igual modo, o Estado destinatário das informações pessoais poderá repassá-las a um terceiro Estado, se a Parte fornecedora dos dados autorizar. Com isso se observa tanto o princípio da finalidade (aderência a um fim específico), incidente na PDP, quanto o princípio da especialidade da cooperação jurídica internacional, inclusive para *onward transfers*.

Um acordo bilateral de mesmo propósito, o *Tax Information Exchange Agreement* (TIEA),[153] celebrado com os Estados Unidos para implementação da *Foreing Account Tax Compliance Act* (FATCA), tem forte impacto na proteção transnacional de dados pessoais. No entanto, não contém dispositivos expressos sobre PDP, talvez refletindo o momento de sua adoção, em 2007, quando não tínhamos uma LGPD. Em 2025, os Estados Unidos continuam a não ter uma lei federal deste tipo.

---

[152] BRASIL. **Decreto 8.842, de 29 de agosto de 2016.** Promulga o texto da Convenção sobre Assistência Mútua Administrativa em Matéria Tributária emendada pelo Protocolo de 1º de junho de 2010, firmada pela República Federativa do Brasil em Cannes, em 3 de novembro de 2011.

[153] BRASIL. **Decreto 8.506, de 24 de agosto de 2015**. Promulga o Acordo entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América para o Intercâmbio de Informações relativas a Tributos, assinado em Brasília, no dia 20 de março de 2007 ("TIEA").

8 A APLICABILIDADE DA LGPD BRASILEIRA A ATIVIDADES DE INTELIGÊNCIA E DE SEGURANÇA PÚBLICA E AO PROCESSO PENAL

Desde a tramitação do projeto que se converteu na Lei 13.709/2018– conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD) – pende o debate sobre sua aplicabilidade ou não a certas atividades estatais relacionadas às atividades de inteligência e segurança pública e à persecução criminal.

Na Nota Técnica nº 175/2023, a Autoridade Nacional de Proteção de Dados (ANPD) tomou posição. O objeto da manifestação da Agência foi o "Acordo de Cooperação entre o MJSP e a CBF para compartilhamento de dados pessoais visando ao aprimoramento do Projeto Estádio Seguro".[154]

Esta importante iniciativa da Confederação Brasileira de Futebol (CBF) e do Ministério da Justiça e da Segurança Pública (MJSP), para aumentar a segurança dos espectadores das competições futebolísticas, visa implementar "ações de combate ao racismo e à violência nos estádios brasileiros, com a aplicação do uso de tecnologias que permitam identificar torcedores que tenham se envolvido em ilícitos e possam, porventura, causar problemas nas praças esportivas." [155]

Segundo o § 3º do art. 4º da LGPD, compete à ANPD emitir "(…) opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais". Valendo-se desse dispositivo e do art. 55-J, inciso XX, da LGPD,[156] a ANPD considerou ter competência para se manifestar sobre o projeto *Estádio Seguro.*

Esta competência autárquica é limitada, uma vez que não cabe à ANPD regular as atividades de persecução criminal e de segurança pública. Estas devem estar sujeitas a um órgão próprio no âmbito do sistema de justiça, formado pelo Conselho Nacional de

[154] BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. **Nota Técnica nº 175/2023/CGF/ANPD, de 25 de outubro de 2023**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdf.

[155] BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. **Nota Técnica nº 175/2023/CGF/ANPD, de 25 de outubro de 2023**.

[156] Segundo este inciso, compete à ANPD "deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos".

Justiça (CNJ)[157] e pelo Conselho Nacional do Ministério Público (CNMP), a fim de preservar a autonomia e a independência do Poder Judiciário e do Ministério Público no desenho geral dos poderes estatais. Assim, sustentamos que, nas duas atividades em tela, a atribuição da ANPD é meramente consultiva, não podendo ser imposta ao Ministério Público nem ao Poder Judiciário. A utilização da palavra "recomendação" pelo legislador apoia este entendimento.

Como quer que seja, o Projeto Estádio Seguro tem uma inegável relação com atividades de segurança pública – devido à atuação de torcidas violentas nas arenas desportivas – e com atividades de persecução penal – devido ao interesse de localização e captura de foragidos da justiça criminal. Ademais, a inciativa governamental dialoga com o art. 148 da Lei Geral do Esporte (Lei 14.597/2023), que prevê que praças desportivas com mais de 20 mil lugares devem ter serviços de monitoramento por videovigilância e sistemas de identificação biométrica.

> Art. 148. O controle e a fiscalização do acesso do público a arena esportiva com capacidade para mais de 20.000 (vinte mil) pessoas deverão contar com meio de monitoramento por imagem das catracas e com identificação biométrica dos espectadores, assim como deverá haver central técnica de informações, com infraestrutura suficiente para viabilizar o monitoramento por imagem do público presente e o cadastramento biométrico dos espectadores.
> Parágrafo único. O disposto no **caput** deste artigo deverá ser implementado no prazo máximo de até 2 (dois) anos a contar da entrada em vigor desta Lei.[158]

A segunda questão controvertida – e que é a que mais importa – está nas exceções previstas no art. 4º, inciso III, da LGPD, que, como vimos, aparentemente excluiriam sua incidência sobre o tratamento de dados pessoais realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais.

A ANPD examinou o âmbito de aplicação do diploma legal à luz do referido inciso III do art. 4º da LGPD. Apesar do que ali está escrito, o §1º do mesmo dispositivo legal estabelece uma *proteção mínima* para os titulares dos dados sujeitos a tratamento no

[157] O art. 59 do anteprojeto da LGPD Penal propõe que "O Conselho Nacional de Justiça (CNJ), por meio da sua Unidade Especial de Proteção de Dados em Matéria Penal (UPDP), será responsável por zelar, implementar e fiscalizar a presente lei em todo o território nacional". BRASIL. Câmara dos Deputados. Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados, de 26 de novembro de 2019. **Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal**. Disponível em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf.

[158] BRASIL. **Lei 14.597, de 14 de junho de 2023**. Institui a Lei Geral do Esporte.

âmbito da segurança pública e do processo penal. Esse campo de força de proteção não pode ser ignorado pela Administração Pública nem pelo sistema de justiça criminal.

Ao examinar as finalidades do projeto *Estádio Seguro*, a ANPD entendeu, conforme a própria LGPD, que os princípios gerais e os direitos do titular dos dados nela previstos se aplicam ao tratamento de dados pessoais no contexto da segurança pública. Conforme o § 5.8 da NT 175:

> A partir da análise dos documentos encaminhados, foi possível identificar as finalidades principais da operação de compartilhamento de dados no âmbito do Projeto Estádio Seguro: (i) recapturar indivíduos com mandado de prisão ou medidas penais restritivas; (ii) auxiliar na recuperação de veículos roubados ou furtados; e (iii) evitar a venda de ingressos utilizando dados de pessoas falecidas, combatendo o cambismo.[159]

Tais atividades são inequivocamente de segurança pública e interessam ao Ministério da Justiça neste âmbito, tendo repercussões diretas em ações penais em andamento. Basta pensar na possibilidade de identificação e captura de pessoas foragidas a partir de dispositivos de reconhecimento facial, baseados ou não em sistemas de inteligência artificial. Os dados das câmeras instaladas nos estádios, nos pontos de venda e nos seus estacionamentos poderão ser compartilhados com o Ministério da Justiça.

O projeto CBF e pelo MJ visa à prevenção de crimes envolvendo torcedores e frequentadores de eventos. Por outro lado, o direito à proteção de dados pessoais (PDP) não pode ficar desguarnecido justamente naquelas atividades que mais podem lhe causar impacto, devido à intrusividade que lhes é inerente.

Desde a promulgação da Emenda 115, de 2022, que é posterior à Lei 13.709/2018, o direito à PDP passou a ter *status* constitucional no inciso LXXIX do art. 5º,[160] o que aciona obrigações estatais para sua proteção imediata sempre que estiver sujeito a interferências estatais ou de terceiros. Como escrevemos em 2020, tal exclusão:

> […] foi um erro de legística, uma vez que as sensíveis questões abordadas em segurança pública e persecução criminal mereceriam regulamentação simultânea às questões gerais, hoje abrangidas pela LGPD, num enfoque que garantisse a proteção

[159] BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. **Nota Técnica nº 175/2023/CGF/ANPD, de 25 de outubro de 2023**, item 5.8. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdf.

[160] Constituição Federal, art. 5º, inciso LXXIX: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

> de dados e, ao mesmo tempo, não criasse dificuldades insuperáveis para os órgãos de inteligência e de persecução criminal.[161]

Embora o § 1º do art. 4º da LGPD assevere que o tratamento de dados pessoais para fins exclusivos de segurança pública e de persecução criminal "será regido por legislação específica", é essencial notar que tal diploma futuro "deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular". Tais direitos e princípios já estão listados na LGPD, embora não apenas nela. Portanto, a futura "LGPD Penal", como tem sido chamado o diploma, "deverá observar os mesmos parâmetros, que, desde já, devem ser aplicados ao tratamento de dados pelo Poder Público, tendo em vista o princípio do efeito imediato, insculpido no §1º do art. 5º da Constituição".[162]

Mais ainda: conforme o inciso XXXV do art. 5º, a lei não pode excluir da apreciação do Poder Judiciário qualquer lesão ou ameaça de lesão a direito fundamental. Trata-se da garantia de acesso à justiça, que também tem dignidade convencional, à luz da Convenção Americana de Direitos Humanos e do Pacto Internacional de Direitos Civis e Políticos, de 1966. Tanto na instância penal quanto na tutela coletiva, deve haver instrumentos para a proteção do direito à PDP, inclusive nos segmentos excluídos pela LGDP. Foi o que vimos ao examinar a decisão da Corte IDH em *CAJAR vs. Colômbia*.[163] É também a consequência do conjunto normativo de cooperação internacional, que examinamos e que impõe a observância da PDP na transferência transnacional de dados pessoais.

Estamos diante de uma situação que reclama a aplicação do princípio da proporcionalidade, em função de potencial desproteção a direitos internacionalmente reconhecidos. Direitos fundamentais previstos em normas de eficácia plena ou de eficácia

[161] ARAS, Vladimir. A título de introdução*:* segurança pública e investigações criminais na era da proteção de dados. In: ARAS, Vladimir B.; MENDONÇA, Andrey Borges de; CAPANEMA, Walter A.; SILVA, Carlos Bruno F. da; COSTA, Marcos Antônio da S. (Org.). **Proteção de dados pessoais e investigação criminal.** Brasília: ANPR, 2020, p. 14-31.

[162] ARAS, Vladimir. Boate Kiss: a seleção dos jurados e o direito à proteção dos dados pessoais. **Jota**, 4 de janeiro de 2022. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/boate-kiss-selecao-jurados-direito-protecao-dados-04012022.

[163] CORTE IDH. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia.** Sentencia de 18 de octubre de 2023, § 740. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.

contida têm aplicação imediata[164] e, se não pode haver excessos ou abusos na ação estatal, tampouco pode haver deficiência nas suas salvaguardas. Ao interpretar tais direitos, devemos ter em conta o princípio *pro persona*, que, como regra interpretativa prevista em tratados internacionais, coloca a pessoa humana no centro da ordem jurídica,[165] seja ela o acusado ou a vítima de uma interferência, dado que a Constituição, assegurando a igualdade, não faz acepção de pessoa, isto é, não se inclina para este ou para aquele indivíduo.

A incapacidade do Estado brasileiro de plenamente proteger dados pessoais no campo das atividades de inteligência e de segurança pública e do processo penal pode resultar em portas fechadas inclusive nas interações internacionais para o enfrentamento ao crime organizado e outras graves formas de delinquência transnacional.[166] O já mencionado Acordo do Brasil com a União Europeia para cooperação policial entre a Europol e a Polícia Federal[167] confirma essa asserção, segundo se vê na parte final do seu art. 1º, que exclui expressamente o intercâmbio de dados pessoais de seu escopo.

A falta de um regime adequado de PDP no Brasil e a inexistência de um acordo sobre *Passenger Name Records* (PNR)[168] com a União Europeia dificulta o acesso aos dados de passageiros de voos com origem ou destino em países da Europa (*extra-EU flights*), causando óbices à identificação de pessoas autoras ou vítimas de crimes, sob investigação no Brasil. A Diretiva PNR da União Europeia é rigorosa quanto ao tratamento de dados pessoais de passageiros, cujo tratamento é autorizado apenas para

[164] Constituição Federal, art. 5º, § 1º: "As normas definidoras dos direitos e garantias fundamentais têm aplicação imediata".
[165] CAVALLO, G.; NOGUEIRA ALCALÁ, H. El principio favor persona en el derecho internacional y en el derecho interno como regla de interpretación y de preferencia normativa. **Revista de Derecho Público**, [*s. l.*], n. 84, p. 13–43, 2016. Disponível em: https://doi.org/10.5354/0719-5249.2016.43057.
[166] De se recordar que a Política Nacional de Inteligência prevê o emprego de instrumentos de inteligência para lidar com o terrorismo, o crime organizado, a cibercriminalidade, a corrupção e ações contrárias ao Estado Democrático de Direito. BRASIL. **Decreto 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência, § 6.
[167] BRASIL. **Decreto 10.364, de 21 de maio de 2020.** Promulga o Acordo de Cooperação Estratégica entre a República Federativa do Brasil e o Serviço Europeu de Polícia, firmado em Haia, em 11 de abril de 2017.
[168] Desde 2016, o Brasil tem com os EUA "o Acordo de Cooperação Técnica firmado entre a Polícia Federal (PF) e o Departamento de Segurança Interna dos Estados Unidos (DHS), por meio da Agência de Fiscalização de Alfândega e Proteção de Fronteiras (CBP), com o objetivo de avaliar e analisar Informações Antecipadas sobre Passageiros (API) e o Registro Identificação de Passageiros (PNR), visando combater o crime transnacional e outras ameaças à segurança fronteiriça, elevando a segurança na República Federativa do Brasil e nos Estados Unidos da América, além de facilitar o fluxo de viagens", assinado em 24 e 25 de junho de 2016, publicado no **DOU nº 144, de 28 de julho de 2016**, Seção 3, p. 79.

prevenção e repressão ao terrorismo e a outros crimes graves.[169] Países como o Canadá, a Austrália e Estados Unidos têm ou estão negociando acordos PNR com a Bruxelas.[170]

A Diretiva 681, de 2016, visa regulamentar a transferência desses dados de base das companhias aéreas para as autoridades nacionais, enquanto os regulamentos relativos às informações antecipadas sobre os passageiros estabelecem regras para a coleta e a transferência de mais dados pessoais para as autoridades nacionais.

> A partilha de dados relativos aos passageiros é útil para efeitos de prevenção, deteção e repressão das infrações terroristas e da criminalidade grave. A diretiva relativa aos registos de identificação dos passageiros visa regulamentar a transferência desses dados de base das companhias aéreas para as autoridades nacionais, enquanto os regulamentos relativos às informações antecipadas sobre os passageiros estabelecem regras para a recolha e transferência de mais dados pessoais para as autoridades nacionais.[171]

No campo processual, como antes visto, é somente com grande dificuldade que o Brasil vem desde 2014 buscando um acordo pleno de cooperação com a Eurojust. Este projeto, que é muito importante para as atividades transnacionais do Ministério Público, foi retardado em alguns anos por falta de equacionamento do déficit legislativo e institucional na proteção dos dados pessoais na persecução criminal no Brasil.

Embora o direito à proteção de dados tenha uma história de mais de meio século, desde que surgiu na Alemanha no pós-guerra, somente nos últimos vinte anos a PDP se tornou um tema corrente na doutrina brasileira. Ainda não somos partes da Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108), de 1981. Contudo, a Convenção de Budapeste sobre Cibercriminalidade, que entrou em vigor para o Brasil em 2023,[172] faz referência expressa a documentos internacionais sobre PDP e, como já ressaltamos, no seu art. 15, impõe aos Estados, como obrigação positiva, que garantam:

> [...] proteção adequada aos direitos humanos e às liberdades públicas, incluindo os direitos nascidos em conformidade com as obrigações que esse Estado tenha assumido

---

[169] MAESA, Costanza di Francesco. Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR). **Eurojusitalia**, 24/052016, p. 1-17.

[170] UNIÃO EUROPEIA. **Parecer 1/15 do Tribunal de Justiça (Grande Seção), de 26 de julho de 2017.** Projeto de acordo entre o Canadá e a União Europeia. Transferência dos dados dos registos de identificação dos passageiros aéreos da União para o Canadá. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62015CV0001%2801%29.

[171] UNIÃO EUROPEIA**.** Conselho Europeu. **Dados relativos aos passageiros**. Disponível em: https://www.consilium.europa.eu/pt/policies/passenger-name-record/.

[172] BRASIL. **Decreto 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm.

> na Convenção do Conselho da Europa para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, de 1950, na Convenção Internacional da ONU sobre Direitos Civis e Políticos, de 1966, e em outros instrumentos internacionais de direitos humanos, e que tais poderes e procedimentos incorporarão o princípio da proporcionalidade.

Na mesma medida, não se pode ignorar que a tendência jurisprudencial do STF e do STJ é, sem dúvida, de fortalecer o direito à PDP e o direito à autodeterminação informativa,[173] assim como de salvaguardar do direito à privacidade no ambiente digital.[174] Segundo a concepção adotada pelo Tribunal de Justiça da União Europeia (TJUE) no caso *Schrems II*, a conferência do *status* de país com nível de proteção adequado a Estados terceiros depende, não apenas da existência de leis e de órgãos de proteção de dados, mas também da disponibilidade de remédios efetivos para lidar com eventuais violações e de uma jurisprudência robusta dos órgãos judiciários nacionais.[175]

Conforme o art. 45, §2º, do Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, ao avaliar a adequação do nível de proteção, a Comissão Europeia deve levar em conta o primado do Estado de direito, o respeito aos direitos humanos, a legislação em vigor em matéria de segurança pública, defesa, segurança nacional e

---

[173] STF, **ADIn 6387 MC-Ref**, Relatora Ministra Rosa Weber, Tribunal Pleno, julgado em 07/05/2020.

[174] STF: "8. A concepção do direito à privacidade como uma garantia individual de abstenção do Estado na esfera privada individual passou por profundas transformações no decorrer do século XX. Devido ao próprio avanço das tecnologias da informação, assistiu-se a uma verdadeira mutação jurídica do sentido e do alcance do direito à privacidade. A releitura do direito à privacidade coincide com o desenvolvimento jurisprudencial do conceito de autodeterminação informacional (*die informationelle Selbsstbestimmung*) pelo Tribunal Constitucional Alemão. Essa nova abordagem revelou-se paradigmática por ter permitido que o direito à privacidade não mais ficasse estaticamente restrito à frágil dicotomia entre as esferas pública e privada, mas, sim, se desenvolvesse como uma proteção dinâmica e permanentemente aberta às referências sociais e aos múltiplos contextos de uso. 9. A maior abrangência da proteção atribuída ao direito de autodeterminação repercute no âmbito de proteção do direito à proteção de dados pessoais, que não recai sobre a dimensão privada ou não do dado, mas sim sobre os riscos atribuídos ao seu processamento por terceiros. A força normativa do direito fundamental à proteção de dados pessoais decorre da necessidade de proteção da dignidade da pessoa humana, vis-à-vis a contínua exposição dos indivíduos ao risco de comprometimento da autodeterminação informacional". [174] STF. **HC 222.141 AgR**, Relator Ministro Ricardo Lewandowski, Segunda Turma, julgado em 06/02/2024.

[175] TJUE: "188. Para este efeito, o artigo 45.º, n.º 2, alínea a), do RGPD exige que, no âmbito da sua avaliação da adequação do nível de proteção garantido por um país terceiro, a Comissão tenha em conta, nomeadamente, as 'vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência'. O considerando 104 do RGPD sublinha, a este respeito, que o país terceiro 'deverá garantir o controlo efetivo e independente da proteção dos dados e estabelecer regras de cooperação com as autoridades de proteção de dados dos Estados-Membros' e precisa que este deve 'ainda conferir aos titulares dos dados direitos efetivos e oponíveis e vias efetivas de recurso administrativo e judicial'". UNIÃO EUROPEIA. Tribunal de Justiça. **Processo C-311/18**, Data Protection Commissioner contra Facebook Ireland Ltd., Maximilian Schrems et al. Acórdão de 16 de julho de 2020, § 188. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=10257253.

processo penal "e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência".[176]

Como abordamos anteriormente, o direito à proteção de dados pessoais passou a integrar o *corpus juris* regional das Américas, quando a Corte IDH o reconheceu expressamente, no âmbito do art. 11 da Convenção Americana de 1969. No caso *Membros da Corporação Coletivo de Advogados José Alvear Restrepo ("CAJAR") vs. Colômbia*,[177] a Corte IDH afirmou categoricamente que o tratamento de dados pessoais para fins de inteligência de segurança pública e de Estado deve observar o direito à PDP e o direito à autodeterminação informativa, que também foi reconhecido regionalmente.

Visto esse cenário, a supressão ou a fragilização dos direitos do titular quando do tratamento de dados para fins de segurança pública e persecução criminal é incompatível com o art. 5º, incisos XXXV e LXXIX, da Constituição. Tal conjuntura é também inconvencional, por limitar a proteção judicial efetiva exigida pelo art. 25 da Convenção Americana de Direitos Humanos para a garantia do direito à PDP e à autodeterminação informativa.

Nesta linha de ideias, embora a ANPD não seja nem possa ser a autoridade de controle das atividades do Poder Judiciário e do Ministério Público no campo da segurança pública e do processo penal, a Nota Técnica 175/2023, como instrumento opinativo, diz exatamente o que deveria dizer sobre a necessária incidência dos direitos do titular previstos na LGPD em atividades de tratamento de dados para fins de segurança pública. Esta é a mesma conclusão a que chegamos no tocante à incidência das normas

[176] UNIÃO EUROPEIA. **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). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679.

[177] CORTE IDH: "En lo que atañe al objeto de este proceso, las Buenas prácticas para garantizar los derechos humanos por los servicios de inteligencia reconocen el derecho de los particulares de acceder a sus datos personales que obren en poder de los organismos con facultades para desarrollar acciones de inteligencia, así como el de reclamar su rectificación cuando no sean exactos. Cualquier excepción a esta regla, además de estar regulada legalmente, debe ser proporcional y necesaria para el desempeño del mandato que rige los servicios de inteligencia". CORTE INTERAMERICANA DE DIREITOS HUMANOS. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvar Restrepo" vs. Colombia**. Sentencia de 18 de octubre de 2023, § 584. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.

de PDP nas atividades de inteligência e de persecução criminal, inclusive nos incidentes de cooperação internacional que envolvam a transferência internacional de dados pessoais.

É passada a hora de o Congresso Nacional se debruçar sobre o tema para que vençamos esse eloquente déficit legislativo, e o Brasil tenha um marco normativo que concilie a defesa dos direitos dataprotetivos e as necessidades das atividades de inteligência e de segurança pública e da persecução criminal numa sociedade democrática.

9 O COMPARTILHAMENTO DE DADOS PESSOAIS ENTRE ÓRGÃOS DE INTELIGÊNCIA E INSTITUIÇÕES DE PERSECUÇÃO PENAL

Na era digital, é sem igual a capacidade estatal de coletar, armazenar e compartilhar dados. Este poder corporativo e estatal deve estar sujeito a estritos limites, que não comprometam a economia nem a segurança da sociedade em sentido amplo.

O avanço das tecnologias de investigação criminal para a obtenção de provas digitais de crimes de informática (*computer crimes*), de crimes facilitados pelas tecnologias (*computer-facilitated crimes*) e provas digitais de crimes não digitais ("analógicos") impulsiona cada vez mais o tratamento de dados pessoais pelas agências de persecução criminal, com impactos também nas atividades de inteligência e de segurança pública, inclusive nas vertentes transfronteiriça e transnacional.[178]

Uma coisa é o compartilhamento de dados para uma investigação certa e determinada, casuisticamente, sob demanda, no âmbito dos poderes de requisição de órgãos como a Polícia e o Ministério Público. Outra coisa é o compartilhamento generalizado de massas de informações pessoais com os órgãos de persecução criminal, para fins de inteligência. Há um risco de expansão do poder punitivo e de abusos a direitos fundamentais quando bancos de dados inteiros são repassados indiscriminadamente a

[178] Segundo a Doutrina da Atividade de Inteligência, a inteligência transnacional é a "área de atuação da inteligência voltada para temas transfronteiriços, parcialmente sob capacidade de intervenção do Estado, mas que exigem negociações e parcerias internacionais para adoção de políticas efetivas para concretização dos objetivos do Estado". BRASIL. **Doutrina da Atividade de Inteligência,** Brasília: ABIN, 2023, p. 22. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023.

órgãos estatais, sem previsão legal expressa. Nestes casos, a lei deve prever salvaguardas adicionais para o tratamento desses dados.

A Constituição Federal de 1988 estabelece, no art. 5º, incisos X, XI, XII e LXXIX, os direitos à intimidade, vida privada e sigilo e proteção de dados, oponíveis a pessoas físicas, jurídicas e ao Estado. Todavia, esses direitos não são absolutos: podem ceder frente à necessidade legítima e proporcional da segurança pública ou da persecução penal, desde que respeitados os princípios do devido processo legal (art. 5º, LIV), da legalidade (art. 5º, II), da razoabilidade e da finalidade, além de outros princípios gerais de PDP. Como alerta Calabrich:

> Caso fosse possível eleger como único objetivo no processo penal a máxima proteção aos direitos dos titulares dos dados pessoais, a solução seria simples: bastaria proibir qualquer forma de tratamento de dados pessoais no processo penal. Banidas todas as medidas relacionadas à persecução e que de algum modo caracterizem o tratamento de dados pessoais – como "quebras" de sigilo bancário, fiscal, de dados telemáticos, interceptação de comunicações ou a apreensão de documentos e arquivos de computador – não haveria tratamento nem afetação à autodeterminação informativa. Se não houver nenhum tratamento de dados pessoais, não haverá abuso contra o titular dos dados pessoais. Obviamente, trata-se uma solução obtusa, pois considera apenas o interesse do titular dos dados e ignora que o processo penal também deve servir para esclarecer fatos e, eventualmente, aplicar penas a quem tiver praticado um crime, na medida de sua culpabilidade.[179]

É admissível o compartilhamento de informações entre órgãos públicos, inclusive no âmbito da segurança pública e persecução criminal, desde que exista base legal clara, finalidade legítima, proporcionalidade e mecanismos adequados de controle. O tratamento de dados pessoais para fins penais e de segurança pública exige reserva legal reforçada (*quality of law*), controle jurisdicional *ex ante* ou *ex post* e aderência ao princípio da finalidade específica, de modo a impedir usos arbitrários ou desvios de finalidade, chamados de tredestinações.

> Impedir, aprioristicamente, o compartilhamento do acesso a bancos de dados entre entes públicos não atende os diversos interesses públicos em jogo por limitar extremamente as possibilidades de atuação inteligente e eficiente em políticas públicas, e não exclusivamente na persecução penal. Não se faz política pública eficiente sem dados pessoais, assim como não é possível, sem o tratamento de dados pessoais, promover uma persecução penal eficiente, especialmente em face da criminalidade organizada. Os limites ao Estado devem existir preponderantemente como regras claras e rígidas para a realização desse tratamento - como direitos procedimentais, portanto -, e não como vedações absolutas e apriorísticas a uma determinada forma de tratamento de dados pessoais. Tais limites também pressupõem sua sindicabilidade e a existência de vias formais de controle […].[180]

[179] CALABRICH, Bruno. **Proteção de Dados Pessoais na Investigação Criminal e no Processo Penal**: garantismo, eficiência e *standards* de validade. São Paulo: Editora JusPodivm, 2024, p. 150.
[180] CALABRICH, Bruno. **Proteção de Dados Pessoais na Investigação Criminal e no Processo Penal**: garantismo, eficiência e *standards* de validade. São Paulo: Editora JusPodivm, 2024, p. 287.

O conceito de "qualidade da norma" ou "qualidade da lei" (*quality of law*), na jurisprudência do TEDH, é particularmente relevante na PDP. Tal concepção dá ênfase a um entendimento substantivo do que constitui uma "lei", ultrapassando as preocupações tradicionais com a posição hierárquica ou a origem parlamentar das disposições legais.[181] Esta mudança é significativa para os países da Europa continental com tradição de direito civil (*civil law*), uma vez que influencia a redação de atos normativos de modo a cumprir as diretrizes do TEDH em matéria de precisão, clareza, acessibilidade e previsibilidade. A interpretação do TEDH quanto ao *rule of law* sublinha a necessidade de as leis nacionais serem previsíveis e acessíveis, assegurando garantias processuais e o acesso à justiça, o que está em consonância com as tradições jurídicas europeias mais amplas.[182]

9.1 Os contextos do compartilhamento de dados entre agências estatais

O compartilhamento de dados entre instituições como Polícia Civil, Polícia Federal, Ministério Público, Receita Federal e COAF pode ocorrer em dois grandes contextos: compartilhamento para fins de investigação criminal, com fundamento em dispositivos do CPP, a exemplo dos art. 3º-B, 13-A, 13-B, 47, 425, e 156, e de leis especiais, como o art. 15 da Lei 9.613/1998; e o compartilhamento administrativo ou preventivo no âmbito do SISBIN, para fins de inteligência, atividade regulada pela Lei 9.883/1999.

Segundo o parágrafo único do art. 4º da Lei do SISBIN, "os órgãos componentes do Sistema Brasileiro de Inteligência fornecerão à ABIN, nos termos e condições a serem aprovados mediante ato presidencial, para fins de integração, dados e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais".

Apesar de a LGPD excluir sua aplicação nos casos penais *stricto sensu* (art. 4º), impõe limites implícitos ao compartilhamento de dados, pois a persecução criminal continua sujeita ao controle de proporcionalidade e à vedação de provas ilícitas (art. 5º, LVI, da CF) e a certos princípios de proteção previstos noutras leis (art. 5º, LXXIX, da

[181] LUPO, Nicola; PICCIRILLI, Giovanni. European Court of Human Rights and the Quality of Legislation: Shifting to a Substantial Concept of 'Law'? **Legisprudence**, v. 6, n. 2, p. 229–242, 2012. Disponível em: https://doi.org/10.5235/175214612803596668

[182] LAUTENBACH, Geranne. **The Concept of Rule of Law and the European Court of Human Rights**. Oxford: Oxford University Press, 2014, *passim*.

CF). De igual modo, ao menos no plano da lei federal, as atividades de inteligência também devem observar as normas de proteção à pessoa humana.

Segundo a Corte IDH, se a legislação de um Estado permitir o compartilhamento de dados internamente ou internacionalmente, a lei "deve especificar as condições para esse intercâmbio, as finalidades permitidas, os órgãos autorizados e as proteções necessárias para a segurança das informações (especialmente dados pessoais)".[183] Não é de estranhar que a Doutrina da Atividade de Inteligência[184] declare que "Leis específicas, como a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI), reforçam os mecanismos de transparência e legitimidade da atividade de inteligência".[185]

Neste campo, também devem incidir as Boas Práticas das Nações Unidas sobre o respeito aos direitos humanos em atividades de inteligência contra o terrorismo, de 2010. Conforme a Boa Prática 31 (*Practice 31*), o compartilhamento de informações entre agências de inteligência de um Estado ou com as autoridades de um Estado estrangeiro deve obedecer a legislação nacional. Esta lei deve estabelecer:

> [...] parâmetros claros para o intercâmbio de informações, incluindo as condições que devem ser cumpridas para que as informações sejam compartilhadas, as entidades com as quais as informações podem ser compartilhadas e as salvaguardas que se aplicam ao intercâmbio de informações.[186]

---

[183] CORTE IDH. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia.** Sentencia de 18 de octubre de 2023, § 539. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.

[184] A Doutrina da Atividade de Inteligência foi aprovada pela Portaria GAB/DG/ABIN/CC/PR nº 1.205, de 27 de novembro de 2023.

[185] BRASIL. **Doutrina da Atividade de Inteligência,** Brasília: ABIN, 2023, p. 22. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023.

[186] HRC: "It is good practice for all forms of information-sharing between intelligence services and other domestic or foreign entities to have a clear basis in national law. National law includes criteria on the purposes for which intelligence may be shared, the entities with which it may be shared, and the procedural safeguards that apply to intelligence-sharing.156 A legal basis for intelligence-sharing is an important requirement of the rule of law, and is particularly important when personal data are exchanged, because this directly infringes the right to privacy and may affect a range of other rights and fundamental freedoms. In addition to ensuring that intelligence-sharing is based on national law, it is widely accepted as good practice that intelligence-sharing be based on written agreements or memoranda between the parties, which comply with guidelines laid down in national law.157 The elements that are commonly included in such agreements include rules governing the use of shared information, a statement of the parties' compliance with human rights and data protection, and the provision that the sending service may request feedback on the use of the shared information.158 Intelligence-sharing agreements help to establish mutually agreed standards and expectations about shared information, and reduce the scope for informal intelligence-sharing, which cannot be easily reviewed by oversight institutions". UNITED NATIONS. Human Rights Council. Compilation of good practices on legal and institutional frameworks and measures that ensure

Os segmentos de atuação governamental nos quais mais se identifica a tensão entre o dever de segurança e os direitos à privacidade e à proteção de dados pessoais são as atividades de defesa do Estado, de segurança pública e de persecução criminal, que envolvem vários aspectos e ciclos da atividade de inteligência, descritos na Doutrina Brasileira de Inteligência.[187] Numa linha crescente de restrições, devido ao incremento da intromissão e das consequências pessoais de referidas atividades do Estado, pode-se divisar que é justamente na persecução criminal que os riscos de compressão indevida de direitos fundamentais são mais significativos. O resultado do processo penal pode ser a privação da liberdade ou o confisco de patrimônio do réu, com diversos impactos sobre sua vida privada.

Na área de inteligência e de segurança pública as interferências estatais sobre o patrimônio jurídico e as liberdades públicas dos cidadãos são menos intensas do que no teatro de operações do poder punitivo do Estado. É justamente aqui que as proteções e salvaguardas a esses direitos devem ser mais robustos. Contudo, em 2018, o legislador brasileiro perdeu a oportunidade de regular de modo abrangente a proteção de dados no processo penal. Limitou-se a aprovar a Lei 13.709/2018, mas, diferentemente do que vimos na União Europeia, não lidou de modo pleno com a proteção de dados pessoais no processo penal. De fato, ao adotar o Regulamento Geral de Proteção de Dados (Regulamento 2016/679), a União Europeia aprovou também duas diretivas fundamentais, que já abordamos: a Diretiva 2016/680, sobre a proteção de dados na segurança pública e no processo penal (*LED Directive* ou Diretiva Policial),[188] e a Diretiva 2016/681, sobre o tratamento de dados de passageiros em voos intra e extra-europeus (Diretiva PNR). [189]

---

respect for human rights by intelligence agencies while countering terrorism, including on their oversight, **A/HRC/14/46**, 17 May 2010, Boa Prática 31 e § 45. Disponível em: https://documents.un.org/doc/undoc/gen/g10/134/10/pdf/g1013410.pdf.

[187] BRASIL. **Doutrina da Atividade de Inteligência,** Brasília: ABIN, 2023, p. 22. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023.

[188] UNIÃO EUROPEIA. **Diretiva (UE) 2016/680**, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados.

[189] UNIÃO EUROPEIA. **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.

Apesar dessa falha de *design*, como já ressaltamos, a legislação brasileira de PDP não se limita à LGPD. Tomemos como exemplo a Lei 9.296/1996, Lei das Interceptações; a Lei 12.037/2009, a Lei de Identificação Criminal; a Lei 7.210/1984, a Lei de Execução Penal; ou a Lei 12.965/2014, o Marco Civil da Internet (MCI), e veremos em todos esses diplomas regras sobre o tratamento de dados pessoais no ambiente processual penal. Apesar disso, nosso conjunto normativo é frágil e disperso, e até pouco tempo não dava ao País um nível de proteção adequado para o tratamento, aqui, de dados pessoais compartilhados por Estados Partes da União Europeia. Exemplo dessa deficiência estrutural, como visto, é a vedação de compartilhamento de dados pessoais para fins operacionais no contexto do Acordo de Cooperação Policial de 2017 entre a Europol e a Polícia Federal, promulgado pelo Decreto 10.364/2020:

> Artigo 1º - Finalidade
> A finalidade do presente Acordo é estabelecer relações de cooperação entre a Europol e a República Federativa do Brasil, para apoiar os Países Membros da União Europeia e a República Federativa do Brasil na prevenção e combate ao crime organizado, terrorismo e outras formas de crime internacional nas áreas criminais referenciadas no Artigo 3º, em especial por meio do intercâmbio de informações operacionais, estratégicas e técnicas entre a Europol e República Federativa do Brasil. Este Acordo não abrange o intercâmbio de dados pessoais.

Na Lei 13.709/2018, o compartilhamento de dados pessoais é uma forma de tratamento de dados. O artigo 5º, inciso XVI da LGPD define o uso compartilhado de dados como a:

> [...] 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.

Conforme o inciso III do art. 7º da LGPD, o tratamento de dados pessoais somente poderá ser realizado pela Administração Pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da Lei. Conforme o art. 23 da LGPD, o tratamento de dados pessoais pelas pessoas jurídicas de direito público deve ser realizado:

> [...] para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

Pode-se argumentar que esses dispositivos não se aplicariam a atividades de inteligência e de segurança pública e ao processo penal, por força do art. 4º, inciso III, da LGPD. Contudo,[190] a própria Lei Geral prevê, no §1º do mesmo art. 4º, que sejam assegurados em lei futura (a tal LGPD penal) o respeito aos direitos do titular e observados os princípios gerais de proteção estruturados pela lei de 2018.[191] A consequência óbvia dessa previsão, lida em conjunto com o princípio do efeito imediato das normas de direitos humanos (§1º do art. 5º da Constituição) e com o direito à PDP, consagrado no inciso LXXIX do art. 5º da CF, é a de que tais direitos e princípios já se aplicam desde logo, na medida do possível, ao tratamento de dados pessoais nas atividades dos órgãos de persecução penal.

Um desses direitos está no art. 9º da LGPD, que assegura ao titular, no âmbito da autodeterminação informacional, o direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca da finalidade específica do tratamento, e às informações acerca do uso compartilhado de dados pelo controlador e a finalidade.

9.2 Um breve panorama do compartilhamento de dados na jurisprudência

O avanço da jurisprudência constitucional sobre proteção de dados pessoais tem sido consistente nos últimos anos. Passos também têm sido dados no sistema interamericano de direitos humanos, valendo invocar mais uma vez a decisão da Corte IDH no caso *CAJAR vs. Colômbia*, quando se ressalta o direito de saber se os dados coletados pelo Estado foram ou serão objeto de compartilhamento com outrem:

> [...] da perspectiva da pessoa cujos dados constam nos arquivos públicos, é imprescindível, para garantir sua autonomia e liberdade de autodeterminação, reconhecer seu direito de acessar e controlar esses dados, com os seguintes alcances: (i) o direito de saber quais dados se encontram nos registros dos órgãos públicos, em suportes físicos, magnéticos, eletrônicos ou informáticos, de onde provêm, como foram obtidos, para que são utilizados, o prazo de

[190] ARAS, Vladimir. A aplicabilidade da LGPD às atividades de segurança pública e persecução penal. **Jota**, 30 de abril de 2024. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/aplicabilidade-da-lgpd-as-atividades-de-seguranca-publica-e-persecucao-penal-30042024?non-beta=1.

[191] ARAS, Vladimir. A título de introdução*:* segurança pública e investigações criminais na era da proteção de dados. In: ARAS, Vladimir B.; MENDONÇA, Andrey Borges de; CAPANEMA, Walter A.; SILVA, Carlos Bruno F. da; COSTA, Marcos Antônio da S. (Org.). **Proteção de dados pessoais e investigação criminal.** Brasília: ANPR, 2020, p. 14-31.

> sua conservação, se são compartilhados com outras instâncias ou pessoas, a razão para isso e, em geral, as condições de seu tratamento.[192]

Um dos dispositivos relevantes para o compartilhamento de dados entre órgãos de inteligência, de segurança e de persecução penal é o art. 3º, inciso VIII, da Lei 12.850/2013, que prevê a cooperação interinstitucional e interfederativa na luta contra o crime organizado. Segundo tal dispositivo, admite-se a cooperação entre instituições e órgãos federais, distritais, estaduais e municipais na busca de provas e informações de interesse da investigação ou da instrução criminal. Infelizmente, o legislador limitou-se a prever essa modalidade do que chama equivocadamente de "meio de obtenção de prova". Contudo, a lei não o detalhou nem estabeleceu qualquer premissa para sua articulação, o que se choca com o requisito da *quality of law,* no tocante à precisão, determinabilidade e previsibilidade do instrumento. Interpretando esse inciso, Salgado diz:

> Não há de se concordar, portanto, com autores que sustentam, com base no artigo 3º, VIII, da Lei 12.850/13, a unificação e o compartilhamento irrestrito, sem amparo legal, de base de dados entre as agências de segurança pública e de persecução penal, sob o fundamento do risco de "*feudalização*" de dados e de que *"as informações que são públicas pertencem ao Estado como um todo e não podem ser consideradas informações 'particularizadas' ou 'inacessíveis' entre os distintos órgãos estatais."* Isso não quer dizer, entretanto, que a vinculação inicial a uma determinada finalidade implica em proibição do tratamento de dados para outros fins, mas sim que a alteração de finalidade exige um baldrame legal que autorize, sob certas condições, o tratamento para outra finalidade, somado à análise dos critérios de proporcionalidade para nova intervenção. Em suma, a alteração da finalidade que originariamente sustentou o levantamento do dado, dessarte, por ser uma intervenção adicional, deve ser legalmente regrada, mesmo existindo um interesse legítimo derivado da nova necessidade de tratamento de dados.[193]

O déficit legislativo no desenho de normas de compartilhamento de dados se apresenta também no art. 15 da Lei 9.613/1998, que autoriza o COAF a comunicar "às autoridades competentes" (sem dizer quais) "para a instauração dos procedimentos cabíveis" (sem especificar se cíveis, criminais ou administrativos), "quando concluir pela existência de crimes previstos nesta Lei, de fundados indícios de sua prática, ou de qualquer outro ilícito". Nesta última parte, a norma abrange um enorme conjunto de infrações não penais, em desrespeito a critérios de proporcionalidade, determinabilidade e previsibilidade.

---

[192] CORTE IDH. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia**, Sentencia de 18 de octubre de 2023.

[193] SALGADO, Daniel de Resende. O artigo 5º, LXXIX, da Constituição Federal e o artigo 3º, VIII da Lei 12.850/13: limites ao levantamento, ao compartilhamento e à utilização secundária de dados pessoais no enfrentamento ao crime. *In*: SALGADO, Daniel de Resende; GRANDIS, Rodrigo de; BECHARA, Fábio Ramazzini (orgs.). **10 anos da Lei das Organizações Criminosas:** aspectos criminológicos, penais e processuais penais. São Paulo: Almedina Brasil, 2023, p. 687-724.

O advento da Lei 13.974/2020 não resolveu a questão, pois os incisos I e II do artigo 3º dessa Lei, ao tratarem das atribuições do Conselho de Controle de Atividades Financeiras (COAF), também usaram linguagem vaga para descrever a competência da nossa Unidade de Inteligência Financeira (UIF) na difusão de inteligência financeira. Esses dispositivos dizem apenas que cabe ao COAF "produzir e gerir informações de inteligência financeira para a prevenção e o combate à lavagem de dinheiro" e "promover a interlocução institucional com órgãos e entidades nacionais, estrangeiros e internacionais que tenham conexão com suas atividades". Isso é muito pouco num campo em que há o tratamento de dados pessoais, inclusive sensíveis, para importantes ações estatais de enfrentamento à lavagem de dinheiro, ao financiamento do terrorismo e à proliferação de armas de destruição em massa. Mais clareza e precisão não fariam mal ao legislador; e fariam bem ao aplicador da norma.

Não é por acaso que esse desenho normativo acabou provocando a controvérsia que se viu no Tema 990 da repercussão geral do STF, questão bem resolvida pela Suprema Corte ao julgar o RE 1.055.941/SP, em 2019. Na ocasião, cuidando do compartilhamento dos relatórios de inteligência financeira (RIF) pelo COAF, o STF permitiu a essa instituição enviá-los diretamente, de modo espontâneo ou a pedido, ao Ministério Público e à Polícia, para fins de persecução penal.[194] Contudo, a debilidade do marco normativo não pacificou as instâncias inferiores, tanto que a todo tempo tribunais como o STJ (vide por exemplo os RHC 196.150 e RHC 174.173, submetidos a julgamento pela 3ª Seção em 14 de maio de 2025)[195] questionaram o precedente vinculante do STF, em seus limites e escopo, ao menos quanto ao chamado RIF a pedido (por intercâmbio).

Ocorre que, em 2019, ao decidir o Tema 990, o STF inequivocamente autorizou o compartilhamento interinstitucional dos dados dos RIFs, sem necessidade de prévia autorização judicial, tanto num caso (RIF espontâneo) como no outro (RIF a pedido), em

[194] STF. Pleno, **RE 1.055.941/SP**, Tema 990 da Repercussão Geral, Rel. Min. Dias Toffoli, j. em 04/12/2019. No mesmo sentido: STF, **Recl 81.531/DF**, Rel. Min. Cármen Lúcia, d. em 15 jul. 2025.

[195] STJ: "A solicitação direta de relatórios de inteligência financeira pelo Ministério Público ao Coaf sem autorização judicial é inviável. O Tema 990 da Repercussão Geral não autoriza a requisição direta às unidades financeiras por órgão de persecução penal sem autorização judicial". (STJ, 3ª Seção, **RESP 2.150.571, RHC 174.173 e RHC 196.150**, j. em 14/05/2025.)

linha com a *soft law* pertinente, adotada pelo GAFI e pelo Grupo de Egmont.[196] No entanto, o STJ continuou em idas e vindas, como se viu no HC 147.707/PA. Este acórdão foi atacado pela Procuradoria Geral da República por meio da Reclamação 61.944/PA, relatada pelo ministro Cristiano Zanin. E o STF mais uma vez decidiu pela possibilidade de compartilhamento direto de dados, mesmo nos RIFs a pedido:

> No Tema 990/RG, o Supremo Tribunal Federal reconheceu constitucional o compartilhamento de Relatórios de Inteligência Financeira (RIF) entre o COAF e as autoridades de persecução penal sem necessidade de prévia autorização judicial, inclusive com a possibilidade de solicitação do material ao órgão de inteligência financeira.[197]

A decisão da 1ª Turma foi clara. Em consequência, o precedente vinculante de 2019 deve ser seguido por todos os tribunais brasileiros. A 2ª Turma do STF chegou ao mesmo entendimento, admitindo:

> [...] o compartilhamento de relatório de inteligência financeira, tanto de ofício quanto a pedido dos órgãos de investigação criminal, desde que o procedimento seja realizado por meio de sistema eletrônico, que garanta o sigilo e a segurança da informação e que não tenha sido realizado por encomenda contra cidadãos que não estejam sob investigação ou sem que haja um alerta previamente emitido pela unidade de inteligência.[198]

Em janeiro de 2025, na Reclamação 75.111/SC, o ministro Alexandre de Moraes, apontando como fundamento os incisos X e XII do art. 5º da CF, reafirmou que "a decisão reclamada, ao considerar ilícito o compartilhamento dos relatórios de inteligência financeira, desconsidera as conclusões do Supremo Tribunal Federal no julgamento do Tema 990 da Repercussão Geral". No mesmo sentido a Reclamação 80.818/SP, decidida pelo ministro Flávio Dino, em 17 de junho de 2025; a Reclamação 81.531/DF, decidida pela ministra Cármen Lúcia em 15 de julho de 2025; e a Reclamação 81.546/BA, decidida pelo ministro Cristiano Zanin em 8 de agosto de 2025.

Concordamos com a posição do STF. Contudo, não podemos negar que o legislador poderia ter sido mais minucioso, ao estabelecer expressamente a possibilidade de difusão dos dois tipos de RIF no art. 15 da Lei 9.613/1998, os órgãos competentes para recebê-los e as infrações-tipo objeto dos relatórios, além do prazo de retenção de tais dados.

Mais recentemente, na ADI 4906/DF, que atacou o art. 17-B da Lei 9.613/1998 sobre o compartilhamento direto de dados cadastrais, o STF também permitiu o acesso

---

[196] ARAS, Vladimir. O COAF de um paraíso fiscal. **Jota**, 19 jul. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/o-coaf-de-um-paraiso-tropical-19072019.

[197] STF, 1ª Turma, **Recl. 61.944/PA AgR**, Rel. Min. Cristiano Zanin, j. em 02/04/2024. Vide também: STF, **Recl. 81.546/BA**, Rel. Min. Cristiano Zanin, d. em 08/08/025.

[198] STF, 2ª Turma, **HC 246.060 AgR**, Rel. Min. Edson Fachin, j. em 07/04/2025.

do MP e da Polícia a esses dados sem necessidade de prévia autorização judicial. O dispositivo legal questionado é muito claro neste aspecto, permitindo ao STF afirmar que a imposição de sigilo de dados "não alcança os dados cadastrais".

Ressaltando que os direitos fundamentais à proteção de dados e à autodeterminação informativa impõem a adoção de mecanismos capazes de assegurar a proteção e a segurança dos dados pessoais manipulados pelo poder público e por terceiros, a Corte afirmou ser compatível com a Constituição "o compartilhamento direto de dados cadastrais genéricos com os órgãos de persecução penal, para fins de investigação criminal, mesmo sem autorização da Justiça".[199] Note-se que a base legal para o julgado é uma norma que cuida do compartilhamento casuístico de dados, mediante requisições vinculadas a investigações em curso.

Fora do ambiente penal, o STF tentou estabelecer parâmetros para o compartilhamento de dados entre instituições governamentais. Em 2020, no julgamento da medida cautelar na ADI 6.387/DF, o Supremo Tribunal Federal reconheceu a existência de um direito fundamental autônomo à proteção de dados pessoais e à autodeterminação informacional. A ação atacou a Medida Provisória 954/2020, que cuidava do compartilhamento de dados dos usuários de telefonia fixa e móvel, pelas empresas prestadoras, com o IBGE.[200]

Para o Tribunal, "o compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados." Entendeu-se que a norma não revelava interesse público legítimo para justificar o compartilhamento dos dados pessoais dos usuários dos serviços de telefonia, porque não definia como e para que seriam utilizados os dados coletados. Segundo a Corte, essa falta violava o princípio do devido processo legal na sua feição substantiva, "por não oferecer condições de avaliação quanto à sua adequação e

[199] STF, Pleno, **ADI 4906/DF**, Rel. Min. Nunes Marques, j. em 11/09/2024.
[200] BRASIL. **Medida Provisória 954, de 17 de abril de 2020.** Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (Covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.

necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades."[201]

Ademais, considerando que os dados seriam compartilhados em massa, a medida provisória objeto da declaração de inconstitucionalidade não tinha regras sobre "mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados".[202]

Este julgado põe em xeque o déficit legislativo na prática de compartilhamento de massas de dados (bases inteiras) para fins de inteligência e investigações cíveis ou criminais futuras, com base apenas no art. 8º da Lei Complementar 75/1993,[203] cujo alcance, para estes fins (compartilhamento em massa), é limitado. Não que essa prática seja ilegal, pois não é; a questão está na incompletude textual, diante dos princípios que regem a PDP, o que poderia minar uma atividade essencial do Ministério Público para a proteção da sociedade, a luta contra o crime e a tutela dos direitos humanos.

Já na ADI 6649/DF, julgada em 2022, que atacou o Decreto 10.046/2019, que instituiu o Cadastro Base do Cidadão e do Comitê Central de Governança de Dados,[204] a Suprema Corte brasileira estabeleceu parâmetros para o compartilhamento de dados[205] da Carteira Nacional de Habilitação entre o Serviço Federal de Processamento de Dados (SERPRO) e a ABIN:

> O compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública, pressupõe: a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018); b) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público.[206]

[201] STF, **ADI 6387 MC-Ref**, Rel. Min. Rosa Weber, Tribunal Pleno, j. em 07/05/2020.
[202] STF, **ADI 6387 MC-Ref**, Rel. Min. Rosa Weber, Tribunal Pleno, j. em 07/05/2020.
[203] BRASIL. **Lei Complementar 75, de 20 de maio de 1993**. Dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União.
[204] BRASIL. **Decreto 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.
[205] Segundo o art. 2º, inciso VIII, do Decreto 10.046/2019, compartilhamento de dados é a "disponibilização de dados pelo seu gestor para determinado recebedor de dados".
[206] STF, **ADI 6649/DF**, Rel. Min. Gilmar Mendes, Tribunal Pleno, j. em 15/09/2022.

Nessa decisão, foram descritos os princípios que devem orientar a atuação do Estado no tratamento de dados pessoais e no seu compartilhamento interinstitucional. Tal principiologia, como vimos acima, é compatível com os padrões internacionais e regionais de PDP quanto às atividades de inteligência e segurança pública. Por isso mesmo, nesse julgado, a Corte Suprema exigiu que, ao compartilhar dados, os órgãos públicos cumpram o art. 23, inciso I, da LGPD, segundo o qual deve ser assegurada publicidade para ciência de todos sobre a faculdade de tais entes públicos intercambiarem informações pessoais, nos termos da Lei de Acesso à Informação (LAI).[207] Nesta linha, o compartilhamento de dados pessoais para fins de inteligência:

> [...] deve observar a adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público; a instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário; a utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso; e a observância dos princípios gerais de proteção e dos direitos do titular previstos na LGPD, no que for compatível com o exercício dessa função estatal.[208]

Não há dúvida de que essas diretrizes pretorianas se aplicam a todo o campo das atividades de inteligência de Estado e de segurança pública. A presença da ABIN como destinatária das informações pessoais instituiu um precedente que deve ser observado por todos os órgãos do SISBIN em suas interações.

É lamentável que a Lei do SISBIN (Lei 9.883/1999) não contenha um regulamento adequado de compartilhamento de dados entre os órgãos integrantes do sistema para fins de inteligência e contrainteligência. O governo federal tentou contornar o problema por meio do Decreto 11.693/2023[209] e do Decreto 8.793/2016,[210]que institui a Política Nacional e Inteligência (PNI). O art. 6º daquele documento dispõe que os órgãos e as entidades integrantes do SISBIN poderão compartilhar dados, informações e

[207] LGPD: "Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos".

[208] STF, **ADI 6649/DF**, Rel. Min. Gilmar Mendes, Tribunal Pleno, j. em 15/09/2022.

[209] BRASIL. **Decreto 11.693, de 6 de setembro de 2023**. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência.

[210] BRASIL. **Decreto 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência.

conhecimentos e conceder acesso a bancos de dados, observadas as diretrizes baixadas pela ABIN, o princípio da segurança jurídica, a necessidade de conhecer, o interesse público e a devida motivação. Por sua vez, o art. 11 desse mesmo decreto permite aos órgãos do sistema "solicitar, obter, processar, produzir e compartilhar dados, informações e conhecimentos em conformidade com a Política Nacional de Inteligência, com os planos de trabalho e com o disposto na legislação". Essas normas não são, contudo, suficientes, porque não cobrem em detalhe as necessidades de PDP em todas as suas dimensões, ao mesmo tempo em que preservam a utilidade do SISBIN, para as importantíssimas funções que seus integrantes desempenham.

10 CONCLUSÃO

O percurso que fizemos demonstrou que a sociedade da informação deslocou o eixo probatório para o domínio dos dados, exigindo que o poder punitivo do Estado se submeta a balizas normativas claras, técnicas de investigação proporcionais e salvaguardas contra devassas estatais. O País precisa de uma LGPD Penal que incorpore, para o ambiente investigativo e para a atividade de inteligência, freios constitucionais e convencionais já reconhecidos, com regras de autorização, controle, documentação (*logs*) e exclusão, além de direitos dataprotetivos.

A tessitura externa (a Convenção 108+, o RGPD, a LED, a PNR e os Princípios da OEA) exemplifica um constitucionalismo de dados que combina finalidade, minimização, segurança e responsabilização, inclusive para fins de *law enforcement*. Para encerrar a assimetria brasileira, a LGPD Penal deve incorporar esses padrões, mediante a tipificação das operações de tratamento por autoridades competentes, a Avaliação de Impacto de Proteção de Dados (AIPD) obrigatória para novas técnicas intrusivas, limites materiais e temporais para o acesso a dados e sua retenção, governança adequada e canais de cooperação internacional que respeitem a equivalência de proteção.

Voltando os olhos para a Suprema Corte dos EUA, a evolução de *Olmstead* a *Carpenter*, passando por *Katz*, *Riley* e *Jones*, reafirma a centralidade da expectativa razoável de privacidade e da proteção de metadados e dados de localização, inclusive frente a terceiros custodiantes. A lição comparada é inequívoca: a legislação deve exigir ordem judicial e justa causa para acesso a dados sensíveis e de geolocalização, conteúdos

comunicacionais e histórico de conexões, para o emprego de novos meios especiais obtenção de provas por meio da tecnologia e de técnicas de vigilância contínua.

O mosaico normativo atual (formado pelo CPP, Lei 9.296/1996, MCI, Lei 12.850/2013, etc.) carece de unidade principiológica. A LGPD Penal deve funcionar como lei-quadro do tratamento de dados para segurança pública, inteligência e persecução, harmonizando procedimentos, padronizando cadeias de custódia digitais e prevendo sanções administrativas e penais para o tratamento abusivo de dados pessoais.

Com a EC 115/2022, a PDP tornou-se um direito fundamental autônomo. Todavia, o art. 4º, III, da LGPD deixou uma exceção aberta para a inteligência, a segurança e a persecução. A LGPD Penal deve "fechar" essa exceção com precisão, mediante a a taxatividade de bases legais, reserva de jurisdição para medidas intrusivas, restrição de finalidades, prazos de retenção e mecanismos de revisão judicial e administrativa.

A dispersão normativa produz insegurança e incentiva interpretações extensivas, que podem levar a nulidades. A futura LGPD penal deve consolidar princípios (finalidade, necessidade, proporcionalidade, minimização), prever direitos compatíveis do titular-investigado (acesso diferido, retificação, oposição limitada), instituir *logs* imutáveis, controle externo (inclusive pelo Ministério Público), dever de notificação de incidentes e um regime restrito de exclusão probatória por contaminação de dados.

Por sua vez, o SISBIN e o PNI carecem de regras densas de tratamento de dados pessoais. A LGPD Penal deve positivar o catálogo de técnicas, objetivos legítimos, os limiares de suspeita, os prazos de duração das ingerências, os procedimentos de autorização, supervisão parlamentar-jurisdicional e critérios de retenção e eliminação de dados, além de disciplina de perfis (*profiling*), tratamento de bancos multibiométricos e uso de IA com proibições a práticas de risco excessivo e avaliações de impacto prévias.

O direito à privacidade na CADH (art. 11) serviu de tronco o direito à PDP e à autodeterminação informativa, o que exige leis claras, fins legítimos e controles de necessidade e de proporcionalidade. A LGPD Penal deve incorporar expressamente esse tripé e prever remédios efetivos para o controle dos vícios e eventual responsabilização proporcional do Estado.

A decisão da Corte IDH no caso CAJAR reconheceu a autodeterminação informativa e repudiou a vigilância indiscriminada, a perfilação e a formação de dossiês

sem base legal. Em resposta, a LGPD Penal deve regular o tratamento de dados para fins de inteligência.

O trânsito transfronteiriço de dados exige equivalência de proteção, salvaguardas contratuais e, quando for o caso, controle judicial. A LGPD Penal deve prever critérios para MLATs, pedidos diretos a provedores de internet, preservação rápida de dados, e cláusulas de não uso para fins alheios ao pedido, com supervisão da autoridade dataprotetiva.

O fluxo de dados entre agências governamentais é inevitável, mas não pode ser opaco. A LGPD Penal deve impor registros de compartilhamento, avaliação de finalidade e necessidade caso a caso e condicionar o reuso a autorização judicial quando houver desvio de finalidade ou expressa previsão legal.

A efetividade do processo penal brasileiro na era digital depende de conciliar eficiência investigativa com o respeito ao direito fundamental à proteção de dados. A fragmentação legislativa atual, embora mitigada por princípios constitucionais e internacionais, é motivo de alerta. A aprovação de uma LGPD Penal e o fortalecimento institucional de mecanismos de controle representam caminhos inevitáveis para assegurar um processo penal moderno, legítimo e compatível com a ordem jurídica internacional de direitos humanos.

A exclusão do processo penal e das atividades de inteligência do escopo da LGPD foi um erro histórico de política legislativa. Tal lacuna compromete a confiança nas instituições, fragiliza a proteção de direitos fundamentais e mina a credibilidade internacional do Brasil em matéria de cooperação jurídica e policial. A jurisprudência recente da Corte Interamericana de Direitos Humanos, especialmente no caso *CAJAR vs. Colômbia*, impõe um novo patamar normativo aos Estados democráticos, exigindo controles independentes, bases legais claras e mecanismos efetivos de reparação em caso de abuso.

É recomendável que o legislador brasileiro avance na produção de lei sobre o tratamento de dados pessoais para fins penais e de segurança pública, à semelhança das Diretivas (UE) 2016/680 e 2016/681, o que contribuiria para alinhar o País aos parâmetros internacionais, dando-lhe a condição de jurisdição com nível de proteção adequado. É

fundamental também que o Brasil ingresse, por adesão, na Convenção 108+ do Conselho da Europa e no Segundo Protocolo à Convenção de Budapeste.

A conclusão a que chegamos é normativa e operacional: sem uma LGPD Penal clara, o Brasil continuará a navegar entre a urgência da eficiência e o risco da arbitrariedade. Com uma LGPD densa, técnica e coerente, poderemos proteger liberdades públicas, qualificar investigações e atividades de inteligência e dar segurança jurídica ao tratamento de dados, sem enfraquecer a defesa da sociedade e do Estado.

REFERÊNCIAS

AKKERMANS, Bram. The influence of the four (or five) freedoms on property law. *In*: ERP, Sjef van; ZIMMERMANN, Katja (Orgs.). **Research Handbook on European Property Law**. Cheltenham, UK ; Northampton, MA: Edward Elgar Publishing, 2024, p. 18–27.

ALEMANHA. Tribunal Constitucional Federal. Sentença de 15 de dezembro de 1983. **1 BvR 209, 269, 362, 420, 440, 484/83.** Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html.

ARAS, Vladimir. A aplicabilidade da LGPD às atividades de segurança pública e persecução penal. **Jota**, 30 de abril de 2024. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/aplicabilidade-da-lgpd-as-atividades-de-seguranca-publica-e-persecucao-penal-30042024?non-beta=1.

ARAS, Vladimir. A título de introdução*:* segurança pública e investigações criminais na era da proteção de dados. In: ARAS, Vladimir B.; MENDONÇA, Andrey Borges de; CAPANEMA, Walter A.; SILVA, Carlos Bruno F. da; COSTA, Marcos Antônio da S. (Org.). **Proteção de dados pessoais e investigação criminal.** Brasília: ANPR, 2020, p. 14-31.

ARAS, Vladimir. Boate Kiss: a seleção dos jurados e o direito à proteção dos dados pessoais. **Jota**, 4 de janeiro de 2022. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/boate-kiss-selecao-jurados-direito-protecao-dados-04012022.

ARAS, Vladimir. Cerco digital (*geofence*) e varredura terminológica: balizas constitucionais e legais. *In*: SALGADO, Daniel de Resende; GRANDIS, Rodrigo de; BECHARA, Fábio Ramazzini (Orgs.). **10 anos da Lei das Organizações Criminosas: aspectos criminológicos, penais e processuais penais**. São Paulo: Almedina Brasil, 2023, p. 597–662.

ARAS, Vladimir. **Direito internacional público**. 2.ed. Rio de janeiro: Método, 2023.

ARAS, Vladimir. Direito probatório e cooperação jurídica internacional. *In*: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Orgs.). **A prova no enfrentamento à macrocriminalidade**. 2.ed. Salvador: JusPodivm, 2016, p. 315–382.

ARAS, Vladimir. O COAF de um paraíso fiscal. **Jota**, 19 jul. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/o-coaf-de-um-paraiso-tropical-19072019.

BRADFORD, Anu. **The Brussels Effect:** How the European Union Rules the World. Oxford: Oxford University Press, 2020.
BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. **Nota Técnica nº 175/2023/CGF/ANPD, de 25 de outubro de 2023**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdf.
BRASIL. Câmara dos Deputados. Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados, de 26 de novembro de 2019. **Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal**. Disponível em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf.
BRASIL. Conselho Nacional de Justiça. **Recomendação nº 123, de 7 de janeiro de 2022**. Recomenda aos órgãos do Poder Judiciário brasileiro a observância dos tratados e convenções internacionais de direitos humanos e o uso da jurisprudência da Corte Interamericana de Direitos Humanos.
BRASIL. Conselho Nacional do Ministério Público. **Recomendação nº 96, de 28 de fevereiro de 2023.** Recomenda aos ramos e às unidades do Ministério Público a observância dos tratados, convenções e protocolos internacionais de direitos humanos, das recomendações da Comissão Interamericana de Direitos Humanos e da jurisprudência da Corte Interamericana de Direitos Humanos; e dá outras providências.
BRASIL. **Decreto 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.
BRASIL. **Decreto 10.364, de 21 de maio de 2020**. Promulga o Acordo de Cooperação Estratégica entre a República Federativa do Brasil e o Serviço Europeu de Polícia, firmado em Haia, em 11 de abril de 2017
BRASIL. **Decreto 10.452, de 10 de agosto de 2020**. Promulga o texto do Acordo Quadro de Cooperação entre os Estados Partes do Mercosul e Estados Associados para a Criação de Equipes Conjuntas de Investigação, firmado pela República Federativa do Brasil, em San Juan, em 2 de agosto de 2010.
BRASIL. **Decreto 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001.
BRASIL. **Decreto 11.693, de 6 de setembro de 2023**. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência.
BRASIL. **Decreto 154, de 26 de junho de 1991.** Promulga a Convenção Contra o Tráfico Ilícito de Entorpecentes e Substâncias Psicotrópicas.
BRASIL. **Decreto 5.015, de 12 de março de 2004**. Promulga a Convenção das Nações Unidas contra o Crime Organizado Transnacional, concluída em Palermo em 2000.
BRASIL. **Decreto 5.687, de 31 de janeiro de 2006**. Promulga a Convenção das Nações Unidas contra a Corrupção, adotada pela Assembleia-Geral das Nações Unidas em 31 de outubro de 2003 e assinada pelo Brasil em 9 de dezembro de 2003.
BRASIL. **Decreto 592, de 6 de julho de 1992**. Promulga o Pacto Internacional de Direitos Civis e Políticos, adotado em 16 de dezembro de 1966.
BRASIL. **Decreto 678, de 6 de novembro de 1992.** Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969.

BRASIL. **Decreto 8.506, de 24 de agosto de 2015**. Promulga o Acordo entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América para o Intercâmbio de Informações relativas a Tributos, assinado em Brasília, no dia 20 de março de 2007 ("TIEA").
BRASIL. **Decreto 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência.
BRASIL. **Decreto 8.842, de 29 de agosto de 2016.** Promulga o texto da Convenção sobre Assistência Mútua Administrativa em Matéria Tributária emendada pelo Protocolo de 1º de junho de 2010, firmada pela República Federativa do Brasil em Cannes, em 3 de novembro de 2011.
BRASIL. **Doutrina da Atividade de Inteligência,** Brasília: ABIN, 2023, p. 22. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023.
BRASIL. **Lei 14.597, de 14 de junho de 2023**. Institui a Lei Geral do Esporte.
BRASIL. **Lei 9.883, de 7 de dezembro de 1999.** Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências
BRASIL. **Lei Complementar 75, de 20 de maio de 1993**. Dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União.
BRASIL. **Medida Provisória 954, de 17 de abril de 2020.** Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (Covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.
BRASIL. **Ministério da Justiça**. Ministério da Justiça e da Segurança Pública. Brasil e União Europeia assinam acordo para cooperação entre a Polícia Federal e a Europol, Brasília, 5 de março de 2025. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/brasil-e-uniao-europeia-assinam-acordo-para-cooperacao-entre-a-policia-federal-e-a-europol.
BRASIL**. Resolução nº 2, de 2013-CN**. Dispõe sobre a Comissão Mista de Controle das Atividades de Inteligência (CCAI), comissão permanente do Congresso Nacional, órgão de controle e fiscalização externos da atividade de inteligência, previsto no art. 6º da Lei nº 9.883, de 7 de dezembro de 1999.
BRIDWELL, Scott A. The dimensions of locational privacy. *In*: MILLER, Harvey J. (Org.). **Societies and Cities in the Age of Instant Access**. Dordrecht: Springer Netherlands, 2007, p. 209–225.
BRODNER, Emily. Navigating the Terrain of Geofence Warrants. **Arizona Law Journal of Emerging Technologies**, vol. 7, issue 2, 2024, p. 1-23. https://doi.org/10.2458/azlawjet.6395.
CALABRICH, Bruno. **Proteção de Dados Pessoais na Investigação Criminal e no Processo Penal**: garantismo, eficiência e *standards* de validade. São Paulo: Editora JusPodivm, 2024.
CAMINKER, Evan H. Location Tracking and Digital Data: Can Carpenter Build a Stable Privacy Doctrine? **Supreme Court Review,** 2018, p. 411-481.

CAVALLO, G.; NOGUEIRA ALCALÁ, H. El principio favor persona en el derecho internacional y en el derecho interno como regla de interpretación y de preferencia normativa. **Revista de Derecho Público**, [*s. l.*], n. 84, p. 13–43, 2016. Disponível em: https://doi.org/10.5354/0719-5249.2016.43057.

CHEAH, W. L. Policing Interpol: The Commission for the Control of Interpol's Files and the Right to a Remedy. **International Organizations Law Review**, v. 7, n. 2, p. 375–404, Jan. 2010.

COLOMBIA. Corte Constitucional. **Sentencia C-540/12, de 1 de julio de 2012**. Disponível em: https://www.corteconstitucional.gov.co/relatoria/2012/c-540-12.htm.

CORTE IDH. **Caso de Las Masacres de Ituango vs. Colombia**. Sentencia de 1 de julio de 2006. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_148_esp.pdf.

CORTE IDH. **Caso Escher e Outros vs. Brasil.** Sentença de 6 de julho de 2009. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf.

CORTE IDH. **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia**. Sentencia de 18 de octubre de 2023. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.

CORTE IDH. **Caso Myrna Mack Chang vs. Guatemala**. Sentencia de 25 de noviembre de 2003. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_101_esp.pdf.

CORTE IDH. **Caso Tristán Donoso vs. Panamá**. Sentencia de 27 de enero de 2009. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_193_por.pdf.

COUNCIL OF EUROPE. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**, done at Strasbourg, in 28 January 1981.

COUNCIL OF EUROPE. **Explanatory Memorandum to Recommendation No. R (87) 15** of the Committee of Ministers to member states regulating the use of personal data in the police sector. Disponível em: https://rm.coe.int/168062dfd4.

COUNCIL OF EUROPE. **Recommendation No. R (87) 15** of the Committee of Ministers to member states regulating the use of personal data in the police sector, *adopted by the Committee of Ministers on 17 September 1987.* Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804e7a3c.

DEL GIOVANE, Chiara; FERENCZ, Janos; LÓPEZ-GONZÁLEZ, Javier. The Nature, Evolution and Potential Implications of Data Localisation Measures. **OECD Trade Policy Papers,** No. 278, OECD Publishing, Paris, 2023. Disponível em: https://doi.org/10.1787/179f718a-en.

EGAMBERDIYEV, D. Type of legal assistance in criminal cases creation of joint investigation teams − on the example of eu countries. **International Journal of Law and Criminology**, [*s. l.*], 2023. Disponível em: https://doi.org/10.37547/ijlc/volume03issue06-15.

EUROPEAN COURT OF HUMAN RIGHTS. **Case of Big Brother Watch and Others vs. The United Kingdom [GC]**. Judgment 25 May 2021. Disponível em: https://hudoc.echr.coe.int/fre?i=001-210077.

EUROPEAN COURT OF HUMAN RIGHTS. **Case of Klass and Others vs. Germany**. Judgment 6 September 1978. Disponível em: https://hudoc.echr.coe.int/eng?i=001-57510.

EUROPEAN COURT OF HUMAN RIGHTS**. Case of Leander v. Sweden**. Judgment 26 March 1987. Disponível em: https://hudoc.echr.coe.int/eng?i=001-57519.
EUROPEAN COURT OF HUMAN RIGHTS. **Case of Rotaru v. Rumania [GC].** Judgment 4 May 2000. Disponível em: https://hudoc.echr.coe.int/eng?i=001-58586.
EUROPEAN UNION. Council Decision authorising the opening of negotiations for Agreements between the European Union and Algeria, Argentina, Armenia, Bosnia and Herzegovina, Brazil, Colombia, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey on cooperation between the European Union Agency for Criminal Justice Cooperation (Eurojust) and the competent authorities for judicial cooperation in criminal matters of those third States. Brussels, 23 February 2021, 6153/21 + ADD1. **Council Decision adopted by written procedure on 1 March 2021 (CM 1990/21)**. Disponível em: https://www.statewatch.org/media/1972/eu-council-eurojust-agreements-negotiating-directives-6153-21-add1.pdf.
EUROPEAN UNION. **European Commission. Proposal for a Council Decision on the signing, on behalf of the European Union, of the Agreement between the European Union and the Federative Republic of Brazil on cooperation with and through the European Union Agency for Law Enforcement Cooperation (Europol) and the Federal Police of Brazi**l. Brussels, 18 December 2024. COM(2024) 581 final. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52024PC0581.
GERACI, R. Beyond mutual recognition: the rules of joint investigation teams. **Optime**, [*s. l.*], v. 13, n. 2, p. 29–40, 2022. Disponível em: https://doi.org/10.55312/op.v13i2.378.
INTERPOL**. Background Note on Interpol's Information System Safeguards for the Processing of Personal Data**. Lyon, 2019.
INTERPOL. **Commission for the Control of INTERPOL's Files (CCF).** Disponível em: https://www.interpol.int/en/Who-we-are/Commission-for-the-Control-of-INTERPOL-s-Files-CCF.
INTERPOL. **INTERPOL's Rules on the Processing of Data**. III/IRPD/GA/2011 (2024). Disponível em: https://www.interpol.int/content/download/5694/file/27%20E%20RulesProcessingData_RPD_2024.pdf.
INTERPOL. **Statute of the Commission for the Control of INTERPOL's Files**. II.E/RCIA/GA/2016. Disponível em: https://www.interpol.int/content/download/5695/file/Statute%20of%20the%20CCF-EN.pdf.
ISERTE, Jonathan Mendoza; ANGARITA, Nelson Remolina. In a Landmark Judgment, The IACHR recognized an autonomous right to informational self-determination. **FPF**, December 16, 2024. Disponível em: https://fpf.org/blog/in-a-landmark-judgment-the-inter-american-court-of-human-rights-recognized-an-autonomous-right-to-informational-self-determination/?utm_source=chatgpt.com.
KERR, Orin S. **The digital Fourth Amendment:** privacy and policing in our online world. New York: Oxford University Press, 2025.
LAUTENBACH, Geranne. **The Concept of Rule of Law and the European Court of Human Rights**. Oxford: Oxford University Press, 2014.

LUPO, Nicola; PICCIRILLI, Giovanni. European Court of Human Rights and the Quality of Legislation: Shifting to a Substantial Concept of 'Law'? **Legisprudence**, v. 6, n. 2, p. 229–242, 2012. Disponível em: https://doi.org/10.5235/175214612803596668.

MAESA, Costanza di Francesco. Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR). **Eurojusitalia**, 24/052016, p. 1-17.

MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **Revista Jurídica Luso-Brasileira**, n. 5, p. 781–809, 2019.

NEWTON, Brent E. The Real-World Fourth Amendment**. Hastings Constitutional Law Quarterly**, vol. 43, issue 4, 2016. DOI: 10.2139/SSRN.2769106.

NILSSON, Hans G. Article 85 [Eurojust]. *In*: **Treaty on the Functioning of the European Union**: a commentary. [s.l.] Springer, Cham, 2021. p. 1603–1622.

OEA. **Principios Actualizados sobre la Privacidad y la Protección de Datos Personales**. Washington: Departamento de Derecho Internacional, 2022. https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf.

ORLANDI, E. Corporate Governance in EU Agencies: The Europol Case. **Journal of entrepreneurship and business development**, [*s. l.*], v. 1, n. 1, p. 20–32, 2021. Disponível em: https://doi.org/10.18775/jebd.11.5003.

SALGADO, Daniel de Resende. O artigo 5º, LXXIX, da Constituição Federal e o artigo 3º, VIII da Lei 12.850/13: limites ao levantamento, ao compartilhamento e à utilização secundária de dados pessoais no enfrentamento ao crime. *In*: SALGADO, Daniel de Resende; GRANDIS, Rodrigo de; BECHARA, Fábio Ramazzini (orgs.). **10 anos da Lei das Organizações Criminosas:** aspectos criminológicos, penais e processuais penais. São Paulo: Almedina Brasil, 2023, p. 687-724.

ŠKRLEC, B. Eurojust and External Dimension of EU Judicial Cooperation. **Eucrim**, n. 3, p. 188–193, 2019. Disponível em: https://doi.org/10.30709/EUCRIM-2019-018.

SOUZA, Isac Barcelos Pereira. **Equipes Conjuntas de Investigação na cooperação jurídica internacional em matéria penal**. Salvador: JusPodivm, 2019.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**, Lisboa, 7 de dezembro de 2000. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=PT.

UNIÃO EUROPEIA**.** Conselho Europeu. **Dados relativos aos passageiros**. Disponível em: https://www.consilium.europa.eu/pt/policies/passenger-name-record/.

UNIÃO EUROPEIA. **Convenção da União Europeia, relativa ao Auxílio Judiciário Mútuo em Matéria Penal entre os Estados Membros da União Europei**a, assinada em Bruxelas em 29 de maio de 2000. Disponível em: https://dcjri.ministeriopublico.pt//sites/default/files/documentos/instrumentos/convencao_aux_judiciario_mutuo_mat_penal_entre_est_membros_ue.pdf.

UNIÃO EUROPEIA. **Diretiva (UE) 2016/680**, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados.

UNIÃO EUROPEIA. **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.
UNIÃO EUROPEIA. **Diretiva 95/46/CE** do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
UNIÃO EUROPEIA. **Parecer 1/15 do Tribunal de Justiça (Grande Seção), de 26 de julho de 2017.** Projeto de acordo entre o Canadá e a União Europeia. Transferência dos dados dos registos de identificação dos passageiros aéreos da União para o Canadá. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62015CV0001%2801%29.
UNIÃO EUROPEIA. **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). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679.
UNIÃO EUROPEIA. **Regulamento (UE) 2016/794** do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol). Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:32016R0794.
UNIÃO EUROPEIA. **Regulamento (UE) 2018/1727** do Parlamento Europeu e do Conselho de 14 de novembro de 2018 que cria a Agência da União Europeia para a Cooperação Judiciária Penal (Eurojust). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32018R1727.
UNIÃO EUROPEIA. Tribunal de Justiça. **Processo C-311/18**, Data Protection Commissioner contra Facebook Ireland Ltd, Maximilian Schrems et al. Acórdão de 16 de julho de 2020, § 188. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=10257253.
UNIÃO EUROPEIA. Tribunal de Justiça. **Processo C-362/14,** Maximillian Schrems contra Data Protection Commissioner [GS]. Acórdão de 6 de outubro de 2015, § 94-95. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62014CJ0362.
UNITED NATIONS. Human Rights Council. Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, **A/HRC/14/46**, 17 May 2010. Disponível em: https://documents.un.org/doc/undoc/gen/g10/134/10/pdf/g1013410.pdf.
UNITED STATES. Supreme Court. **Carpenter v. United States**, 585 U.S.___(2018).
UNITED STATES. Supreme Court. **Florida v. Jardines**, 569 U.S. 1 (2013).
UNITED STATES. Supreme Court. **Griswold v. Connecticut,** 381 U.S. 479 (1965).
UNITED STATES. Supreme Court. **Katz v. United States**, 389 U.S. 347 (1967).
UNITED STATES. Supreme Court. **Olmstead v. United States**, 277 U.S. 438 (1928).
UNITED STATES. Supreme Court. **Riley v. California**, 573 U.S. 373 (2014).
UNITED STATES. Supreme Court. **United States v. Jones**. 565 US 400 (2012).

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193–220, 1890.

ZAYAT, Rami; LUCENTE, Kate; LURQUIM, Lea. Data protection laws of the World, **DLA Piper**, 20 January 2025. Disponível em: https://www.dlapiperdataprotection.com/index.html?c=CN.