UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS TRINDADE
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

Hugo Leonardo Barboza

O reconhecimento mútuo do direito à proteção de dados pessoais pelo Brasil e pela União Europeia como forma de concretizar o acesso transfronteiriço a dados informáticos armazenados para o enfrentamento do cibercrime

Florianópolis
2023

Hugo Leonardo Barboza

O reconhecimento mútuo do direito à proteção de dados pessoais pelo Brasil e pela União Europeia como forma de concretizar o acesso transfronteiriço a dados informáticos armazenados para o enfrentamento do cibercrime

Dissertação submetida ao Programa de Pós-Graduação em Direito da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de Mestre em Direito.

Orientador: Prof. Dr. Cláudio Macedo de Souza.

Florianópolis

2023

Barboza, Hugo Leonardo
O reconhecimento mútuo do direito à proteção de dados pessoais pelo Brasil e pela União Europeia como forma de concretizar o acesso transfronteiriço a dados informáticos armazenados para o enfrentamento do cibercrime / Hugo Leonardo Barboza ; orientador, Cláudio Macedo de Souza, 2023.
149 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Programa de Pós Graduação em Direito, Florianópolis, 2023.

Inclui referências.

1. Direito. 2. Cibercrime. 3. Proteção de dados pessoais. 4. Cooperação internacional em matéria penal. I. Souza, Cláudio Macedo de. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Direito. III. Título.

Hugo Leonardo Barboza

O reconhecimento mútuo do direito à proteção de dados pessoais pelo Brasil e pela União Europeia como forma de concretizar o acesso transfronteiriço a dados informáticos armazenados para o enfrentamento do cibercrime

O presente trabalho em nível de Mestrado foi avaliado e aprovado, em 24 de fevereiro de 2023, pela banca examinadora composta pelos seguintes membros:

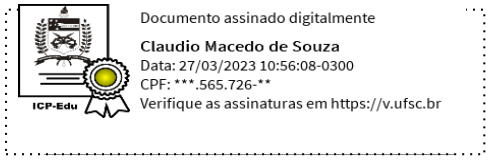
Prof. Cláudio Macedo de Souza, Dr.
UFSC

Prof. Aires José Rover, Dr.
UFSC

Prof. Gerson Faustino Rosa, Dr.
ESPC

Certificamos que esta é a versão original e final do trabalho de conclusão que foi julgado adequado para obtenção do título de Mestre em Direito.

Coordenação do Programa de Pós-Graduação



Prof. Dr. Cláudio Macedo de Souza
Orientador

Florianópolis, 2023

RESUMO

Esta dissertação busca investigar o direito à proteção de dados pessoais no contexto da possibilidade de acesso transfronteiriço a dados informáticos armazenados, prevista na Convenção de Budapeste sobre cibercrime, de 2001. Com a intensificação dos crimes cibernéticos a nível transnacional, tem se exigido dos Estados cooperação jurídica em matéria penal para o adequado enfrentamento a esta modalidade de crime. No entanto, os mecanismos de cooperação internacional relacionados ao cibercrime podem provocar riscos aos direitos fundamentais, como o direito à privacidade e à proteção de dados pessoais. Nesse sentido, propôs-se o seguinte problema de pesquisa: "O que é necessário em matéria de proteção de dados pessoais para que se concretize a possibilidade de acesso transfronteiriço a dados informáticos armazenados pela União Europeia e pelo Brasil, prevista na Convenção de Budapeste sobre cibercrime"? Diante deste questionamento, supõe-se, como hipótese, que "a existência de reconhecimento mútuo de nível adequado de proteção de dados pessoais é necessária para concretizar a possibilidade de acesso transfronteiriço a dados armazenados pelos países membros da União Europeia e pelo Brasil". Para tanto, dividiu-se a investigação em três momentos. Inicialmente, analisou-se o fenômeno da criminalidade cibernética, tendo como parâmetro a sociedade de risco. Na sequência, examina-se os quadros normativos brasileiro e europeu de proteção de dados pessoais aplicáveis ao acesso transfronteiriço a dados informáticos armazenados. Por fim, discutiu-se e propôs-se a concretização da possibilidade de acesso transfronteiriço a dados informáticos armazenados com base na necessidade de reconhecimento mútuo entre Brasil e União Europeia sobre nível adequado de proteção de dados pessoais. A pesquisa foi operacionalizada por meio de análise de fontes jurídicas primárias e de documentos oficiais relacionados ao tema, bem como pela revisão bibliográfica da doutrina pertinente.

Palavras-chave: cibercrime; proteção de dados pessoais; Convenção de Budapeste; cooperação internacional em matéria penal.

ABSTRACT

This research aimed to investigate the personal data protection right regarding the possibility of cross-border access to stored computer data, provided for in the Budapest Convention on cybercrime, of 2001. With the cybercrime increase at a transnational level, it is necessary that States cooperate in criminal matters in order to adequately combat this crime. However, international cooperation mechanisms to combat cybercrime can pose a risk to fundamental rights, including the right to privacy and the protection of personal data. In this sense, the following research problem was proposed: "What is necessary in terms of protection of personal data for the possibility of cross-border access to computer data stored by the European Union and Brazil, provided for in the Budapest Convention, to materialize"? Faced with this questioning, it is assumed, as a hypothesis, that "the existence of mutual recognition of an adequate level of protection of personal data is necessary to materialize the possibility of cross-border access to data stored by member countries of the European Union and by Brazil". Therefore, the inductive method was adopted in this dissertation. The investigation was divided into three stages. Initially, we sought to analyze the phenomenon of cybercrime, having as a parameter the risk society. Next, the Brazilian and European regulatory framework for the protection of personal data applicable to cross-border access to stored computer data is examined. Finally, it was discussed and proposed the implementation of the possibility of cross-border access to stored computer data based on the need for mutual recognition between Brazil and the European Union on an adequate level of protection of personal data. The research was operationalized through the analysis of primary legal sources and official documents related to the topic, as well as the literature review of the relevant doctrine.

Keywords: cibercrime; personal data protection; Budapest Convention; international cooperation in criminal matters.

LISTA DE ABREVIATURAS E SIGLAS

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CELAC – Comissão Econômica para a América Latina e o Caribe

CTIR – Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo

EUROPOL – Agência da União Europeia para a Cooperação Policial

GDPR – General Data Protection Regulation

GSI/PR – Gabinete de Segurança Institucional da Presidência da República

IOCTA – Internet Organised Crime Threat Assessment

LGPD – Lei Geral de Proteção de Dados Pessoais

OCDE – Organização para Cooperação e Desenvolvimento Econômico (OCDE)

UNODC – Escritório das Nações Unidas sobre Drogas e Crime

SUMÁRIO

INTRODUÇÃO

Esta dissertação investiga o direito à proteção de dados pessoais no contexto da possibilidade de acesso transfronteiriço a dados informáticos armazenados, prevista na Convenção de Budapeste sobre cibercrime, de 2001. O tema tem como enfoque a análise do reconhecimento de nível adequado de proteção de dados pessoais como garantia de segurança jurídica entre os atores envolvidos nesta modalidade de cooperação jurídica internacional.

Com a progressiva digitalização das atividades humanas, verifica-se que há aumento dos crimes praticados pela via informática. O incremento da conectividade global implica também no desenvolvimento de criminalidade cibernética em caráter transnacional, de modo que a prática dos crimes e a localização dos agentes comumente ultrapassem as tradicionais fronteiras físicas dos Estados (UNODC, 2013, p. 4).

Nesse cenário, insere-se o conceito de sociedade de risco, caracterizada essencialmente pela impossibilidade de previsão de todas as situações potenciais de perigo. Nesta, a produção social da riqueza e o desenvolvimento tecnológico são acompanhados pela multiplicação de riscos e inseguranças no meio social. Os riscos, uma vez compreendidos como ameaças, podem produzir perigos no futuro, e a antecipação desses perigos engendra um sentimento de insegurança mobilizador da busca de soluções (BECK, 2002). Sob o prisma da sociedade de risco, entende-se que o cibercrime está intimamente ligado à categoria do risco, especialmente considerando sua volatilidade e seu caráter transnacional. Nesse sentido, o avanço das tecnologias de informação e de comunicação contribuem para produção dos riscos inerentes aos ataques cibernéticos.

A natureza transnacional que ganha prevalência nos crimes cibernéticos produz novos desafios aos Estados. A Convenção de Budapeste sobre Cibercrime, de 2001, simboliza, portanto, a crescente demanda por cooperação internacional para o enfrentamento dos crimes cibernéticos em escala internacional. A adesão à Convenção poderia agilizar o acesso das instituições de investigação criminal às provas eletrônicas localizadas em território sob a jurisdição estrangeira, ao mesmo tempo em que também fortalece a cooperação jurídica internacional (VIOLA; HERINGER; CARVALHO, 2021, p. 16).

Levando em consideração a importância da temática, o Estado brasileiro manifestou interesse e foi convidado a aderir à Convenção de Budapeste, conforme nota número 309/2019 divulgada pelo Ministério de Relações Exteriores, bem como foi aprovado pelo Senado o início do processo de adesão à Convenção em 2021. Em novembro de 2022, o

Brasil depositou junto ao Conselho da Europa instrumento para adesão formal à Convenção de Budapeste (BRASIL, 2022).

A Convenção de Budapeste foi desenvolvida no âmbito do Conselho da Europa e aberta para assinatura ou adesão aos demais países interessados. O regime constante na Convenção dispõe sobre modalidades de transferência internacional de dados com a finalidade de investigação criminal por meio da cooperação jurídica internacional. Entende-se, assim sendo, que Budapeste propõe estabelecer uma modalidade de cooperação baseada no compartilhamento de informações para o enfrentamento do cibercrime.

O instrumento prevê, dentre as possibilidades de cooperação internacional a nível de assistência jurídica mútua (capítulo III, seção 2, títulos 1 e 2), a conservação e divulgação de dados informáticos; o auxílio mútuo para acesso a dados informáticos armazenados; o acesso transfronteiriço a dados armazenados em computador, mediante consentimento ou quando se trate de dados acessíveis ao público; auxílio mútuo para recolha, em tempo real, de dados de tráfego; e o auxílio mútuo para a interceptação de dados de conteúdo.

Segundo o relatório explicativo da Convenção de Budapeste, a alta volatilidade dos dados produzidos e armazenados por computadores faz com que seja necessário que os Estados garantam, a nível internacional, a disponibilidade de informações relevantes ao enfrentamento do cibercrime (CONSELHO DA EUROPA, 2001-B, p. 50). No entanto, ao retomar os pressupostos da sociedade de risco, observa-se que o compartilhamento de dados também produz riscos no século XXI, quais sejam a potencial violação ao direito à privacidade.

O artigo 32[1] da Convenção prevê o instrumento de acesso transfronteiriço a dados informáticos armazenados nas hipóteses em que haja o consentimento ou quando os dados já são acessíveis ao público. Menciona-se, a título de exemplo, a possiblidade de acesso a dados armazenados em servidor localizado no território de outro país, que se tornou possível, mediante autorização do titular legalmente reconhecido. Trata-se de mecanismo que, embora topograficamente localizado em conjunto com as demais medidas de auxílio mútuo da Convenção de Budapeste, parte de ação unilateral do Estado (ALVES, 2020, p. 27-28).

Sobre a hipótese de acesso transfronteiriço a dados informáticos armazenados, com base no ordenamento jurídico brasileiro, alguns autores argumentam que o Marco Civil da

[1] Artigo 32. Acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público. Uma Parte pode, sem autorização de outra parte: a) aceder a dados informáticos armazenados acessíveis ao público (fonte aberta), seja qual for a localização geográfica desses dados; ou b) aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra Parte, se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados, através deste sistema informático (CONSELHO DA EUROPA, 2001-A).

Internet seria suficiente para exigir que pessoa jurídica prestadora de serviço no Brasil forneça dados solicitados pelas autoridades penais, ainda que estes dados estejam armazenados em servidores no exterior (DOMINGOS; SILVA; OLIVEIRA, 2020, p. 145; DASKAL; 2016, p. 473; ABREU E SILVA, 2017, p. 115-116). Reforça-se que, nesta hipótese, fala-se de ato unilateral por parte do Estado brasileiro.

Argumenta-se que a necessidade de armazenamento, tratamento e intercâmbio de dados no âmbito da cooperação internacional para o enfrentamento do cibercrime produz impactos no direito à proteção de dados. No paradigma jurídico da União Europeia, nesse sentido, de acordo com a Diretiva n.º 2016/680,[2] ligada à *General Data Protection Regulation* (GDPR), dos Estados que participam da transferência internacional de dados são exigidas garantias à proteção de dados pessoais.

A Lei Geral de Proteção de Dados (LGPD) brasileira reconhece a possibilidade de transferência de dados pessoais na hipótese de cooperação jurídica internacional entre órgãos públicos de inteligência, investigação e persecução, exigindo, para tanto, nível adequado de proteção de dados no país estrangeiro ou no organismo internacional, que deverá ser avaliado pela autoridade nacional.[3] A adequação legislativa com a Convenção de Budapeste, destarte, ultrapassa aspectos relativos aos crimes cibernéticos, de sorte que também envolve o direito à proteção de dados e a sua aplicação aos institutos de auxílio mútuo previstos na Convenção.

Compreende-se que a coleta, o armazenamento, o tratamento e a transferência de dados adquirem valor estratégico nas diversas funcionalidades que a eles podem ser atribuídas, tanto em relação estrita à vida privada dos indivíduos, quanto em aspectos de interesse público. Nesta pesquisa, considera-se especificamente a proteção de dados pessoais, estando eles em posse de organizações públicas ou privadas, aplicada à cooperação internacional em matéria penal. A regulação sobre a transferência de dados pessoais no âmbito penal, ademais, deve ser compreendida como uma forma de integrar o Brasil aos fluxos de transferências internacionais, levando em consideração também o respeito aos direitos fundamentais (VIOLA; HERINGER; CARVALHO, 2021, p. 10).

Embora seja possível defender a possibilidade de acesso unilateral a dados armazenados em servidores localizados em território estrangeiro, nas hipóteses em que a

---

[2] 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, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.

[3] Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei (BRASIL, 2018).

pessoa jurídica presta serviços no Brasil, esta pesquisa propõe avaliar este mecanismo a partir do direito à proteção de dados. Tendo como base o instrumento previsto na Convenção de Budapeste e a legislação protetiva de dados da União Europeia, acrescidos da legislação brasileira, cumpre questionar se a concretização desta possibilidade para dados localizados em países da integração comunitária europeia dependeria de concertação internacional para além da normativa nacional.

Em síntese, a Convenção de Budapeste prevê instrumentos para o compartilhamento de dados pessoais (capítulo III, seção 2, títulos 1 e 2) entre os Estados com vistas a enfrentar o cibercrime. Ademais, para promover intercâmbio desses dados, os Estados precisam oferecer garantias ao direito à proteção de dados, as quais devem ser mutuamente reconhecidas entre as partes. No entanto, nos termos da Convenção de Budapeste, o direito à proteção de dados é apresentado de forma incipiente, sem especificações pormenorizadas, abrindo intencionalmente espaço para que as partes decidam sobre as normas protetivas de dados a serem aplicadas. Torna-se importante, destarte, que os Estados consolidem garantias à proteção de dados pessoais no âmbito da cooperação internacional em matéria penal.

Parte-se do pressuposto de que a mera adesão formal à Convenção de Budapeste não é suficiente para integrar o Brasil às possibilidades de cooperação jurídica internacional via compartilhamento de dados nela previstas. Dessa forma, o problema desta pesquisa gravita em torno da necessidade de compreender a possibilidade de o Brasil concretizar, no âmbito da Convenção de Budapeste, o acesso transfronteiriço a dados armazenados por meio da consolidação de um sistema de proteção de dados pessoais aplicado à esfera penal a ser reconhecido pelas contrapartes estrangeiras.

Diante das considerações expostas, entende-se que a adesão do Brasil à Convenção de Budapeste, ao promover incremento do diálogo e da transferência de dados com parceiros internacionais, exigirá do ordenamento jurídico brasileiro um sistema que garanta a proteção de dados pessoais no âmbito da transferência internacional aplicada ao contexto penal. Especificamente em relação ao acesso transfronteiriço de dados armazenados, a Convenção prevê a necessidade de consentimento prévio da pessoa legalmente autorizada a divulgar esses dados.

Por essa razão, questiona-se: “O que é necessário em matéria de proteção de dados pessoais para que se concretize a possibilidade de acesso transfronteiriço a dados informáticos armazenados pela União Europeia e pelo Brasil, prevista na Convenção de Budapeste sobre cibercrime?” Com base no questionamento proposto neste projeto de pesquisa, supõe-se que: “a existência de reconhecimento mútuo de nível adequado de proteção de dados pessoais é

necessária para concretizar a possibilidade de acesso transfronteiriço a dados armazenados pelos países membros da União Europeia e pelo Brasil".

Estabeleceu-se, como objetivo geral, investigar a necessidade de reconhecimento mútuo de nível adequado de proteção de dados pessoais no Brasil e na União Europeia como forma de concretizar o acesso transfronteiriço a dados informáticos armazenados para investigação criminal voltada ao enfrentamento do cibercrime.

A metodologia adotada neste estudo é baseada na pesquisa bibliográfica, fazendo-se uso de abordagem teórica e hipotética para se deduzir a necessidade de reconhecimento mútuo para a concretização do acesso transfronteiriço a dados informáticos armazenados. A pesquisa foi operacionalizada por meio de análise de fontes jurídicas primárias e de documentos oficiais relacionados ao tema, bem como pela revisão bibliográfica da doutrina pertinente, incluindo relatórios técnicos e precedentes relacionados, com vistas a ponderar o conteúdo das referidas normas com os objetivos estabelecidos nesta pesquisa.

Foram propostos os seguintes objetivos, cada qual organizado em um capítulo específico: a) inicialmente, busca-se analisar o fenômeno da criminalidade cibernética e o quadro normativo brasileiro referente aos crimes cibernéticos, tendo como parâmetro os pressupostos e as características da sociedade de risco; b) na sequência, será examinado o quadro normativo brasileiro e europeu de proteção de dados pessoais aplicável ao acesso transfronteiriço a dados informáticos, especialmente em matéria penal; c) por fim, pretende-se discutir e propor a concretização da possibilidade de acesso transfronteiriço a dados informáticos armazenados, previsto na Convenção de Budapeste, com base na necessidade de reconhecimento mútuo entre Brasil e União Europeia de nível adequado de proteção de dados pessoais.

Os instrumentos normativos apresentados foram ponderados, problematizados e qualificados por meio de revisão sistemática bibliográfica da doutrina pertinente e de publicações acadêmicas que versem sobre os temas atinentes à pesquisa, bem como de relatórios elaborados por instituições públicas e privadas, com a finalidade de investigar a concretização da possibilidade de acesso transfronteiriço a dados armazenados situados em países da União Europeia, prevista na Convenção de Budapeste.

Por fim, destaca-se que esta dissertação de mestrado é resultado do projeto "Escola de Altos Estudos em Inovações Jurídicas para o Direito das Gerações Futuras na América Latina", com fomento do CNPq.

1 RISCO, INSEGURANÇA E CRIMINALIDADE CIBERNÉTICA.

O primeiro capítulo dessa dissertação tem como objetivo examinar o fenômeno da criminalidade cibernética enquanto objeto produtor de riscos e inseguranças na sociedade contemporânea. Os crimes virtuais são compreendidos, nesse sentido, como ameaças que alcançam escala transnacional. Para tanto, adota-se como marco teórico para nortear esta avaliação a teoria da sociedade de risco, nos termos apresentados por Ulrich Beck.

Para tanto, divide-se este capítulo em 2 subtópicos, abordando 3 itens: a) inicialmente, busca-se analisar os pressupostos e as características da sociedade de risco; b) adiante, aborda-se o fenômeno da criminalidade cibernética; c) por fim, examina-se o quadro normativo brasileiro referente aos crimes cibernéticos.

1.1 RISCO E INSEGURANÇA.

Adota-se como pressuposto que os crimes cibernéticos constituem uma ameaça na sociedade contemporânea. Considerando que as tecnologias da informação e da comunicação passam a exercer papel cada vez mais importante nas relações sociais, a criminalidade praticada pela via informática representa relevante risco aos direitos humanos.

De acordo com Ulrich Beck, a produção de riqueza e, paralelamente, o incremento tecnológico, são acompanhados pela produção social de riscos. Isto é, os riscos são construídos a partir do processo de industrialização e de desenvolvimento tecnológico. Os riscos estão associados à maneira pela qual a sociedade e os indivíduos lidam com as ameaças oriundas da própria modernização (BECK, 2002).[4]

Tais ameaças correspondem às incertezas que o processo de modernização tecnológica conduziu à sociedade, de modo que "a semântica do risco significa a tematização de ameaças futuras que são, frequentemente, produto dos sucessos da civilização" (BECK,

[4] Segundo Beck: Risk is not synonymous with catastrophe. Risk means the anticipation of the catastrophe. Risks concern the possibility of future occurrences and developments; they make present a state of the world that does not (yet). […] Thus the category of risk signifies the controversial reality of the possible, which must be demarcated from merely speculative possibility, on the one hand, and from the actual occurrence of the catastrophe, on the other. […] Risks are always future events that may occur, that threaten us. But because this constant danger shapes our expectations, lodges in our heads and guides our actions, it becomes a political force that transforms the world (BECK, 2009, p. 9). Niklas Luhmann faz referência à definição de Richelieu, como uma das formas possíveis de se compreender o risco a partir de perspectiva racionalista: Whither does Richelieu cull the maxim: 'Un mal qui ne peut arriver que rarement doit etre presume n'arriver point. Principalement, si, pour l'eviter, on s'expose a beaucoup d'autres qui sont inevitables et de plus grande consequence'?" The reason is probably that there are so many causes for things going wrong in improbable ways that they cannot all be allowed for by rational calculation (LUHMANN, 1993, p. 12).

2009).[5] Para fins exemplificativos, à medida que novas tecnologias são desenvolvidas, emerge também um processo social de construção de riscos. Os riscos na sociedade contemporânea, destarte, são originados de decisões conscientes tomadas por indivíduos e organizações, sejam elas públicas ou privadas, no curso da produção de riqueza e do desenvolvimento tecnológico (BECK, 2009).

Niklas Luhmann pontua que os eventos futuros, a serem antecipados pelos indivíduos, dependem de decisões concebidas e executadas no tempo presente. Isto é, a ameaça é concretizada em razão de determinada decisão anterior. Nos termos do autor, "só é possível falar de risco se nós pudermos identificar a decisão sem a qual a perda não poderia ter ocorrido" (LUHMANN, 1993).[6] Acrescenta-se a esta perspectiva a contribuição de Zygmunt Bauman: a insegurança, que é estabelecida de maneira conjunta com os riscos, decorre do sentimento de impotência de se oferecer soluções eficazes contra as ameaças contemporâneas (BAUMAN, 2009, p. 166).

Bauman propõe a caracterização das incertezas no tempo contemporâneo em 3 dimensões. Em primeiro lugar, o sistema internacional que caracteriza como "desordem global", após o período da bipolaridade constante na Guerra Fria, constitui uma estrutura imprevisível. Na sequência, o processo de desregulamentação, com a flexibilização de direitos civis e sociais, contribui para a instituição de um sistema no qual as atividades humanas são instáveis. Por fim, o enfraquecimento de redes de segurança social e individual (BAUMAN, 1998, p. 33-35).

Ademais, nos tempos atuais, os riscos percebidos por uma sociedade são ameaças que possuem alcance global.[7] Dessa forma, o risco não está mais restringido ao local de origem específico onde é construído. O desenvolvimento tecnológico produz ameaças capazes de ameaçar toda uma coletividade ao mesmo tempo. No entanto, é preciso ressalvar, determinados grupos sociais são mais afetados pela distribuição global de riscos do que outros

---

[5] Tradução livre. Na versão original: [...] The semantics of risk refer to the present thematization of future threats that are often a product of the successes of civilization (BECK, 2009, p. 4).

[6] Tradução livre. Na versão original: On the other hand - and in addition to what has just been said - what can occur in the future also depends on decisions to be made at present. For we can speak of risk only if we can identify a decision without which the loss could not have occurred (LUHMANN, 2009, p. 16).

[7] É possível relacionar a escala global de risco com a ideia de globalização. De acordo com Zygmunt Bauman, a globalização pode ser definida a partir de sua natureza de indeterminação e de autopropulsão dos assuntos mundiais (BAUMAN, 1999). Boaventura de Sousa Santos identifica como características do fenômeno da globalização a expansão dos fluxos financeiros, a internacionalização e a nova divisão do trabalho, a ampliação das redes de comunicação e a redução das fronteiras físicas (SANTOS, 2002). Santos apresenta a seguinte definição para elucidar o conceito: Definimos globalização como os conjuntos de relações sociais que se traduzem na intensificação das interações transnacionais, sejam elas práticas interestatais, práticas capitalistas globais ou práticas sociais e culturais transnacionais. (SANTOS, 2002, p. 85). Trata-se de processo no qual há redução das distâncias entre os Estados, de modo que que sejam intensificados os fluxos que ultrapassam fronteiras (GIDDENS, 1990, p. 64).

– ainda que, segundo Beck, todos estarão suscetíveis a tais ameaças em algum momento (BECK, 2002).

Ulrich Beck exemplifica alguns dos riscos contemporâneos, tais quais o manejo de tecnologias ligadas à radioatividade, a poluição ou a presença de toxinas no meio ambiente ou na alimentação dos indivíduos. O autor os caracteriza como ameaças que dependem do conhecimento especializado para que sejam percebidos. Isto é, não são fenômenos imediatamente constados pelos indivíduos. Constitui-se, a partir destas características, um processo de construção social do risco, uma vez que grupos políticos ou midiáticos – por meio do discurso e de recursos narrativos – podem amplificar ou minimizar as ameaças e inseguranças existentes (BECK, 2002).

Assim sendo:

> O risco representa o esquema perceptivo e cognitivo de acordo com o qual a sociedade se mobiliza quando é confrontada com a abertura, com as incertezas e com as obstruções de um futuro autocriado e quando não é mais definida pela religião, pela tradição ou pelo poder superior da natureza, mas perdeu mesmo a fé nos poderes redentores das utopias (BECK, 2009, p. 4).[8]

De acordo com Beck, os riscos não devem ser compreendidos como objetos tangíveis. Uma melhor interpretação sugerida os considera como o resultado de construções sociais, nas quais elementos relacionados à cognição humana exercem papel central, como o conhecimento técnico e científico, os valores culturais e os símbolos (BECK, 2005, p. 115).

Muitos dos riscos contemporâneos não são automaticamente percebidos pelos indivíduos. Em alguns casos, são ameaças que dependem da aplicação especializada do conhecimento, por meio de teorização ou de experimentação científicas, por exemplo, para que posteriormente possam se tornar perceptíveis à sociedade. Este conhecimento é necessário para que a relação de causalidade entre a ameaça e o seu resultado se torne visível. (BECK, 2002).

Beck identifica, a partir das premissas elencadas, a possibilidade de se observar uma pluralidade de riscos, construídos a partir de definições múltiplas. Neste processo, há produção social excessiva de riscos, de modo que sejam percebidas ameaças que se somam ou se anulam. O autor justifica a existência de uma multiplicidade de riscos percebíveis na medida em que a compreensão destes (e das suas correspondentes gravidades) depende de

[8] Tradução livre. Na versão original: Risk represents the perceptual and cognitive schema in accordance with which a society mobilizes itself when it is confronted with the openness, uncertainties and obstructions of a self-created future and is no longer defined by religion, tradition or the superior power of nature but has even lost its faith in the redemptive powers of utopias (BECK, 2009, p. 4).

valores e interesses vinculados aos atores responsáveis pelo seu processo de construção (BECK, 2002).

Uma vez considerado que os riscos são construídos a partir de interesses e valores constituídos na sociedade, retoma-se o argumento de Beck segundo o qual a sociedade de risco se concentra em possibilidades futuras de ameaças ainda não concretizadas. A antecipação de um ameaça futura – o risco –, produz na sociedade novos interesses voltados à prevenção ou a tomada de medidas atenuantes contra este perigo (BECK, 2002). Dessa forma, levando em consideração também que os riscos são derivados da antecipação de ameaça que não está restrita aos limites fronteiriços, argumenta-se que estes riscos contaminam a lógica de funcionamento das instituições estatais (BECK, 2009).

No entanto, conforme explica o autor, os riscos são construídos enquanto ameaças "insaciáveis", as quais, em regra, não são integralmente solucionadas. A demanda social por maior segurança diante dos riscos percebidos pode ser reproduzida indefinidamente por meio da instrumentalização das interpretações associadas às ameaças (BECK, 2002).

Para Beck, alguns dos novos riscos presentes na atualidade não são percebidos como superáveis. Considerando, adiante, ameaças que alcançam escala global, as soluções restritas a apenas um Estado para conter e reverter as inseguranças não são mais adequadas, sendo insuficientes diante das novas demandas (BECK, 2009).

Beck apresenta 5 conclusões a respeito da sociedade de risco e das ameaças globais: a) ainda que de maneira distinta, os riscos afetam todos os grupos sociais e seus impactos podem ser percebidos por toda a sociedade; b) emerge uma "comunidade global de ameaças", na qual as ameaças não são mais assuntos internos exclusivos de determinado Estado, de modo que as soluções oferecidas por apenas um Estado são insuficientes; c) o desenvolvimento científico não parece solucionar os riscos, mas pode contribuir para acentuar a percepção dos indivíduos sobre riscos já existentes; d) à medida que a sociedade percebe os novos riscos, a preocupação com temas securitários ganha ênfase, motivando pedidos por maiores garantias de segurança, ainda que em detrimento de valores como liberdade e igualdade;[9] e e) conforme as inseguranças sociais ganham ênfase, as soluções de segurança se

[9] Depreende-se do argumento de Bauman que as demandas sociais por maior segurança contra as ameaças e as inseguranças da modernidade contribuem para o enfraquecimento de outros direitos, como a liberdade. É possível, destarte, que a flexibilização da liberdade e da igualdade para fins de ampliar os níveis de segurança, ao possa redundar na produção social de maior insegurança. Para o autor: se a Freiheit [liberdade] foi tornada vulnerável pela busca moderna inicial de segurança, garantia e certeza da ordem, a Sicherheit [segurança] é a vítima fundamental do curso tomado pela liberdade individual no estágio final da modernidade (BAUMAN, 1999).

tornam mais rentáveis tanto para o setor público quanto para a iniciativa privada (BECK, 2009).

Diante desta abordagem, Beck argumenta que as ameaças globais contemporâneas demandam uma nova resposta, a qual deve levar em consideração as suas características de incerteza e o seu caráter global. A resposta adequada contra as novas ameaças, aduz o autor, depende da cooperação internacional entre os Estados (BECK, 2009). No mesmo sentido, Bauman afirma que, no cenário da globalização, não é possível garantir a segurança geral apenas em um determinado Estado, desconsiderando as condições dos demais espaços políticos (BAUMAN, 2008).

A percepção de Beck em defesa da cooperação internacional está acentuada em "*World at Risk*":

> [...] Os Estados nacionais, independentemente de serem fracos ou poderosos, não são mais as unidades prioritárias para a solução dos problemas nacionais. A interdependência não é um flagelo da humanidade, mas uma pré-condição para a sua sobrevivência. A cooperação não é mais um meio, mas um fim [...] (BECK, 2009, p. 208).[10]

Os pressupostos apresentados permitem conectar os riscos à ideia de segurança. De acordo com Luhmann, no entanto, em sua relação com o risco, a percepção de segurança é construída a partir de uma relação dialética na qual este é reflexo daquela. Isto é, tal proposta de definição de segurança se diferencia do risco justamente por ser a sua contraposição retórica (LUHMANN, 1993).

As medidas institucionais em prol da segurança resultam da antecipação de ameaças futuras. Menciona-se, por exemplo, as ações preventivas tomadas com a finalidade de reduzir a possibilidade de que perdas derivadas dos riscos venham a ocorrer ou, ao menos, de que os danos sejam minimizados. Estas medidas voltadas à segurança, contudo, podem produzir novos riscos por si só (LUHMANN, 1993).

De acordo com Luhmann, os riscos derivados de medidas preventivas são frequentemente mais aceitos, uma vez que estes são justificáveis pela demanda social anterior de segurança. Isto é, os riscos derivados de medidas preventivas, em razão de serem originados a partir do esforço de prevenção de outros riscos primários, passam a ser considerados mais aceitáveis pela sociedade (LUHMANN, 1993, p. 30).

Bauman argumenta que a emergência de múltiplas ameaças na sociedade resulta em um sentimento generalizado de insegurança. A centralidade da preocupação com a segurança

[10] Tradução livre. Na versão original: National states, regardless of whether they are weak or strong, are no longer the primary units for solving national problems. Interdependence is not a scourge of humanity but the precondition for its survival. Cooperation is no longer a means but the end (BECK, 2009, p. 208).

e a maior exposição a riscos conduzem a uma "autopropulsão do medo", por meio da qual a percepção de perigo originada das ameaças pode ser potencializada pelas medidas de segurança de prevenção e contenção (BAUMAN, 1999). A característica autopropulsora do medo é explicada pelo referido autor a partir da premissa de que um indivíduo, constantemente exposto a inseguranças e vulnerabilidades, identifica-se constantemente ameaçado por perigos iminentes (BAUMAN, 2008, p. 12).[11]

Nos termos de Bauman, o sentimento de medo produzido pelos riscos e pelas inseguranças na sociedade leva a um acréscimo nas demandas por medidas que ao menos aparentem oferecer soluções defensivas adequadas. Tais medidas, por sua vez, podem contribuir para amplificar as ameaças ao lhes projetar como mais imediatas, tangíveis e críveis (BAUMAN, 2008, p. 171).

Assim sendo:

> [...] qualquer que seja sua origem, a pressão acumulada busca desesperadamente uma saída, e com o acesso às fontes da incerteza e da insegurança bloqueado ou fora de alcance, toda a pressão se desloca, para cair afinal sobre a finíssima e instável válvula de segurança corporal, doméstica e ambiental. Como resultado, o "problema da segurança" tende a ser cronicamente sobrecarregado de cuidados e anseios que não pode levar nem descarregar. Essa aliança resultada na sede perpétua por mais segurança, uma sede que nenhuma medida prática pode saciar, pois seu destino é deixar intactas as fontes primárias e prolíficas da incerteza e da falta de garantias, as principais provedoras da ansiedade (BAUMAN, 2001, p. 226).

Conclui-se que os riscos constituem ameaças à sociedade e, atualmente, são derivados do próprio avanço econômico e tecnológico. A antecipação de um prejuízo futuro motiva os indivíduos a demandaram medidas de segurança, com finalidade preventiva. No entanto, tais medidas podem constituir elas próprias novos riscos aos indivíduos, ainda que estes sejam mais aceitáveis.

1. 2 A CRIMINALIDADE CIBERNÉTICA.

A partir deste ponto, busca-se analisar o fenômeno da criminalidade cibernética, tendo como fundamento a sua inserção no conceito de risco previamente apresentado. Ademais, apresenta-se brevemente e de maneira cronológica o quadro normativo brasileiro de tipificação da criminalidade cibernética.

Pretende-se identificar uma definição possível para os crimes cibernéticos, evidenciando a relevância destes na sociedade contemporânea, notadamente em relação aos

[11] Bauman identifica 3 tipos de perigos ou ameaças capazes de produzir insegurança aos indivíduos: a) aqueles que constituem ameaças físicas ou aos bens de uma pessoa; b) aqueles que ameaçam a própria ordem social vigente da qual o estilo de vida do indivíduo depende, como sua origem de renda; e c) perigos que ameaçam o "lugar da pessoa no mundo", isto é, o seu espaço na hierarquia social e sua identidade (BAUMAN, 2008, p. 12).

riscos a eles vinculados. Evidencia-se, igualmente, o caráter transnacional da criminalidade cibernética e a importância da cooperação jurídica internacional neste cenário.

1.2.1 Os crimes cibernéticos.

O desenvolvimento tecnológico produz impactos na vida humana. As inovações técnicas viabilizaram novas relações sociais e, dessa forma, também promoveram desafios ao Direito. À medida que surgem novas interações no tecido social, com impactos sobre a vida humana, vislumbram-se também novas demandas ao Direito.

Com o avanço da era digital as tecnologias de informação e de comunicação ampliaram a conectividade global, de modo que os riscos produzidos pela sociedade também ultrapassam as tradicionais fronteiras físicas dos Estados (BECK, 2015, p. 27), conforme destacado no tópico anterior. É possível afirmar, portanto, que a velocidade na circulação de informações amplia a escala e diversifica a incidência geográfica da criminalidade.

Estes novos riscos podem ser caracterizados a partir de sua deslocalização, imprevisibilidade e incompensabilidade. Em primeiro lugar, a deslocalização indica que as causas e efeitos das condutas não mais se limitam a um espaço geográfico restrito, na medida em que ato praticado em determinado espaço pode produzir consequências em outros. Adiante, os riscos são imprevisíveis porque partem de uma percepção hipotética cujos resultados são incalculáveis. Por fim, a incompensabilidade diz respeito ao fato de que se torna progressivamente mais difícil – quando não impossível – compensar ou anular os efeitos nocivos produzidos por um risco (BECK, 2015, p. 94).

Com a integração da sociedade aos meios informacionais e às redes sociais, as condutas praticadas no ambiente virtual – ou por meio de sistemas informáticos – passam a envolver conflitos e danos que não são mais desprezíveis. De acordo com José Roberto Wanderley de Castro, nesse sentido, “a repercussão de um dano gerado por uma injúria em uma rede social não é o mesmo de outrora” (CASTRO, 2018, p. 102). O rápido crescimento e a popularização das telecomunicações desde os anos 1980, bem como a proliferação da *world wide web* a partir da década de 1990, estão ligados à maior disseminação de condutas ilegais no espaço virtual (SIEBER, 1998, p. 39).

O paulatino aumento das relações sociais intermediadas pelo espaço virtual promove uma alta concentração de dados armazenados em sistemas computacionais. Por essa razão, condutas como a invasão de dispositivo informático e a espionagem cibernética se tornam potencialmente mais perigosas, na medida em que podem comprometer sistemas com

informações estratégicas ou sigilosas, seja no âmbito público ou no privado (SIBER, 1998, p. 47-48).

As novas fronteiras tecnológicas, dessa forma, ampliaram as possibilidades de condutas humanas e lhes proporcionaram um alcance em escala global. A internet viabilizou o compartilhamento de informações em tempo quase simultâneo, construindo novas formas de relações sociais, incluindo modalidades criminosas, tais quais a invasão de banco de dados ou o estelionato e a extorsão praticados pela via digital. A internet, dessa forma, contribui para alterar a compreensão do espaço e do tempo e promove novos desafios aos legisladores, uma vez que facilita a circulação de informações para além das fronteiras estatais, enquanto as normas penais internas possuem limitações de ordem espacial (CASTRO, 2018, p. 102).

De acordo com o relatório sobre cibercrime do Escritório das Nações Unidas sobre Drogas e Crime (UNODC), de 2013, o aumento da conectividade global está intrinsecamente associado ao desenvolvimento do fenômeno contemporâneo do cibercrime. Verificou-se, nos termos do relatório, que os crimes cibernéticos são operacionalizados por meio do uso de tecnologias informacionais, as quais possibilitam alcance transnacional às condutas (UNODC, 2013, p. 4).

A origem dos crimes computacionais, conforme Ulrich Sieber, data dos anos 1960. À época, as condutas criminosas incluíam, sobretudo, a sabotagem de computador, a espionagem pela via informática e o uso ilegal de sistemas de computadores. As investigações e os estudos produzidos no período indicavam a incidência de uma grande quantidade de crimes cibernéticos não detectados ou não registrados. Nas décadas seguintes, as condutas criminosas praticadas por meio de computadores se multiplicaram, englobando também a pirataria, a manipulação de caixas eletrônicos e os abusos em redes de telecomunicação (SIEBER, 1998, p. 19-20).[12]

[12] Nesse sentido, para Sieber: A percepção pública e científica sobre os crimes computacionais mudou radicalmente nos anos 1980, quando a imprensa publicou casos chocantes sobre hacking, vírus e Worms. Ademais, uma onda abrangente de programas de pirataria, de manipulação de caixas eletrônicos e de abusos de telecomunicação revelaram para um público amplo a vulnerabilidade de uma sociedade de informação e também a necessidade de uma nova estratégia de segurança e controle do crime. Também revelou que o crime computacional não estava mais limitado aos crimes econômicos, mas incluía ataques contra todos os tipos de interesses, tais quais a manipulação de um sistema hospitalar ou violações de privacidade praticadas por meio do uso de computadores, as quais eram originalmente debatidas separadamente dos "crimes computacionais". Tradução livre da versão original: The public and scientific view of computer crime radically changed in the 1980's, when the press published astonishing cases about hacking, viruses and worms. Furthermore, a broad wave of program piracy, cash dispenser manipulation and telecommunication abuses revealed to a broad public the vulnerability of an information society and such also the need for a new strategy of DP-security and crime control. It also appeared that computer crime was no longer limited to economic crime, but included attacks against all kinds of interest, such as the manipulation of a hospital computer or computer-related infringements of privacy, which were originally discussed separately from "computer crime" (SIEBER, 1998, p. 20).

Ainda que de difícil definição, uma abordagem possível compreende os crimes computacionais como as condutas ilegais, antiéticas ou sem autorização, que envolvam o processamento automático ou a transmissão de dados (SIEBER, 1998, p. 20-21). Trata-se de definição relativamente abrangente sobre o fenômeno dos crimes cibernéticos, ainda que deixe de englobar, de maneira expressa, crimes relacionados ao conteúdo veiculado no meio cibernético.

Observando as manifestações do crime, o conceito de cibercrime deve alcançar um corpo amplo de condutas possíveis. De acordo com o UNODC:

> [...] incluindo fraudes relacionadas ao uso do computador e roubos de identidade; produção computadorizada, distribuição e armazenamento de pornografia infantil; tentativas de phishing; e acesso ilegal a sistemas de computadores, incluindo hacking (UNODC, 2013, p. 8).[13]

A Convenção de Budapeste, nesse sentido, apresenta 4 modalidades abrangentes para abarcar os crimes cibernéticos: a) infrações contra a confidencialidade, integridade, e disponibilidade de sistemas informáticos e dados informáticos; b) infrações relacionadas com computadores; c) infrações relacionadas com o conteúdo; d) infrações relacionadas com a violação do direito de autor e direitos conexos (CONSELHO DA EUROPA, 2001-A).

Ainda assim, as definições sobre os crimes cibernéticos, considerados em sentido amplo, dependem do propósito para o qual se utiliza a terminologia. Verificou-se que a definição destes crimes – ou a mera opção pela escolha de denominação específica –, pode estar dividida em 2 grupos: o primeiro, com maior ênfase ao elemento computacional dos dados e dos sistemas de informações; e, o segundo, com maior ênfase no elemento informacional, relacionando a conectividade e os dados e informações (UNODC, 2013, p. 11).

A criminalidade que se manifesta no ciberespaço pode ser compreendida como criminalidade cibernética. Embora a terminologia a ser adotada para qualificar tal fenômeno criminoso não seja consensual, opta-se, neste trabalho, pela utilização dos termos "criminalidade cibernética" e "cibercrime", ou mesmo "crimes virtuais". Inicialmente, destaca-se que o uso destas expressões se justifica na medida em que a ênfase atribuída está no uso das redes e da internet no escopo do crime, bem como na conectividade global promovida pela inovação tecnológica (WANG, 2016, p. 7). Todavia, algumas considerações sobre outas terminologias adotadas se fazem relevantes para se obter clareza sobre o objeto em análise.

---

[13] Tradução livre da versão original: [...] including computer-related fraud and identity theft; computer-related production, distribution, or possession of child pornography; phishing attempts; and illegal access to computer systems, including hacking (UNODC, 2013, p. 8).

Segundo Marco Túlio Viana, a denominação do tipo penal se faz em razão do bem jurídico afetado. Seguindo esta premissa, o termo "delitos virtuais" não seria coerente, uma vez que o meio virtual não corresponde ao bem jurídico afetado, mas apenas ao meio em que se manifesta o delito. Sob tal perspectiva, considerando que o bem jurídico lesado pelas condutas em análise é a inviolabilidade de informações automatizadas e de sistemas informáticos, a denominação mais apropriada seria "delitos informáticos ou computacionais". (VIANA, 2003, p. 32-34).[14]

Vladimir Chaves Delgado esclarece que a principal problemática em torno da definição da terminologia a ser adotada reside na possibilidade de os dados e sistemas informáticos representarem tanto o objeto de uma conduta – ou o bem jurídico em questão – quanto o instrumento utilizado para a comissão do crime (DELGADO, 2007, p. 19). Sob essa dualidade, as modalidades possíveis de crimes cibernéticos se expandem não só para aquelas que atuam diretamente contra sistemas informáticos, mas também para outros delitos quando praticados pela via informática.

A transição de termos como "crimes computacionais" ou "crimes informáticos" para "crimes virtuais", "crimes digitais" ou "crimes cibernéticos" se dá pela ênfase no envolvimento da internet e da conectividade das redes informacionais. Assim, enquanto expressões como "crime informático" priorizam o envolvimento de computadores ou de sistemas informáticos como parte principal do delito, denominações como "crimes cibernéticos" ou "virtuais" atribuem maior valor às redes e à conectividade no ciberespaço. Essa mudança de realce ganha sentido conforme a internet é popularizada e passa a exercer cada vez mais importância nas relações sociais, e a Convenção de Budapeste sobre Cibercrime, de 2001, é considerada um marco importante dessa tendência (WANG, 2016, p. 5-7).[15]

Nesse sentido, embora se ressalte a contribuição de Viana, reitera-se a opção, nesta pesquisa, pelo uso do termo "crimes cibernéticos" em razão de que se pretende conferir maior elevo ao elemento da internet e da fluidez das informações no paradigma da conectividade a nível global (CASTRO, 2018, p. 112-116). Ademais, é importante ressalvar que os termos "crimes cibernéticos" e "crimes virtuais" podem ser intercambiáveis enquanto objeto de

[14] Nos termos apresentados por Marco Túlio Viana: A simples utilização, por parte do agente, de um computador para a execução de um delito, por si só não configuraria um crime informático, caso o bem jurídico afetado não fosse a informação automatizada. Ocorre, no entanto, que muitos autores acabaram, por analogia, denominando crimes informáticos os delitos em que o computador serviu como instrumento da conduta (VIANA, 2003, p. 37).

[15] Para Wang, a adoção do termo cibercrime pela Convenção de Budapeste contribuiu para que esta denominação ganhasse prevalência nas tipificações legislativas. Isto porque as condutas tipificadas pela Convenção, definidas pelo termo cibercrime, contemplam as demais condutas associadas aos crimes informáticos que já eram previstas pelas legislações nacionais (WANG, 2016, p. 7).

estudo. Não havendo amplo consenso sobre a terminologia a ser adotada, entende-se que o termo "crime informático" também poderá ser utilizado para representar o fenômeno em análise.

Paulo Ernani Bergamo dos Santos afirma que os bens jurídicos ofendidos pelos crimes cibernéticos podem incluir tanto o próprio sistema informático, quanto outros bens jurídicos lesados em razão de conduta que se manifesta no meio cibernético. Cita-se, a título de exemplo, crimes provocados pela veiculação de conteúdo ilícito, como a pornografia infantil (SANTOS, 2018, p. 164).

Castro esclarece:

> [...] o bem jurídico é visto por meio desse critério econômico. Para pensar no bem jurídico e qual será tutelado, deve-se dividir em dois grupos devidamente percebidos na construção dos crimes cibernéticos no mundo: a) O crime cometido por meio informático. Nesse caso o bem jurídico será o bem jurídico tutelado pelo crime praticado. No caso do estelionato, seria o patrimônio; no peculato, o bem jurídico seria a administração pública, e assim por diante. b) Os crimes praticados contra o sistema de informação (CASTRO, 2018, p. 114).

Como já antecipado, as condutas criminosas praticadas no domínio virtual são complexas e potencialmente atentam contra bens jurídicos diversos e que nem sempre são de simples definição. Menciona-se, nesse sentido, a dificuldade de se determinar quais bens jurídicos compõem, na prática, um sistema de informações. Por essa razão, o esforço de tipificação legislativa encontra obstáculos para descrever os crimes cibernéticos. Uma solução possível é propor que o bem jurídico a ser tutelado seja o próprio sistema informacional. Castro menciona, entre os crimes cibernéticos que atentam especificamente contra dados e sistemas informacionais, condutas como a manipulação de dados, a espionagem e a sabotagem – as quais produzem impactos contra a confidencialidade, a disponibilidade e a integridade dos dados e informações contidos em um sistema informacional (CASTRO, 2018, p. 108-114).

Conforme aduz Vladimir Chaves Delgado, a confidencialidade diz respeito à proteção ao conteúdo dos dados e informações armazenados, processados ou transmitidos por sistemas informáticos. A disponibilidade denota a facilidade de acesso e de recuperação de dados e informações em sistemas informáticos. Por fim, a integridade prevê a manutenção do conteúdo dos dados e informações de maneira integral (DELGADO, 2007, p. 26).[16]

[16] Santos, de maneira similar, argumenta: A segurança da informação passa a bem jurídico-penal de natureza difusa, segundo o trinômio "perda de confidencialidade (quebra de sigilo de senha) – perda de integridade (manipula-se uma informação de acesso restrito) – perda de disponibilidade (erro no sistema causado por intrusão de terceiros e causando impossibilidade de acesso à informação por quem precisa dela)" (ROSSINI *apud* SANTOS, 2018, p. 164).

Em sua pesquisa, Castro apresenta classificação dos crimes cibernéticos em crimes próprios e impróprios, sendo diferenciados a partir do bem jurídico a ser tutelado. Os crimes cibernéticos próprios são aqueles em que o bem jurídico ofendido é a "tecnologia da informação em si" (CASTRO, 2018, p. 115). Para Marco Túlio Viana, nos crimes cibernéticos próprios o bem jurídico a ser lesado e, portanto, que é protegido pela legislação penal, é a inviolabilidade das informações automatizadas (VIANA, 2003, p. 42).

Ainda em relação aos crimes cibernéticos próprios, em que o bem jurídico tutelado é a proteção aos sistemas informáticos, Delgado resgata que proteção engloba também a segurança informática de um sistema, considerada objeto independente dos direitos da personalidade. A segurança informática, de maneira similar ao conceito de segurança digital, compreende a manutenção da confidencialidade, da disponibilidade e da integridade dos dados e informações constantes no sistema informático (DELGADO, 2007, p. 26).[17]

Nesse caso, para Delgado, o sistema informático e os dados nele armazenados, processados ou transmitidos, são o objeto material da conduta criminosa. Dentre as práticas possíveis, destacam-se o acesso não autorizado a sistema informático, a reprodução divulgação ou transmissão de informações, a coleta ou interceptação não autorizada de dados e a interferência no funcionamento do sistema (DELGADO, 2007, p. 20-21).

Para Viana, os crimes informáticos – ou cibernéticos – impróprios são "aqueles nos quais o computador é usado como instrumento para execução do crime, mas não há ofensa ao bem jurídico inviolabilidade da informação automatizada (dados)" (VIANA, 2003, p. 38-39). Nesse ponto, a característica definidora de um crime cibernético impróprio é a ausência de ofensa à inviolabilidade do sistema informacional ou das informações automatizadas.[18] Castro

[17] Não há consenso sobre a definição de segurança cibernética, mas é possível identificar características comuns. Segundo relatório "A Caminho da Era Digital no Brasil", publicado pela OCDE, a segurança digital pode ser conceituada como a "gestão de riscos econômicos e sociais resultantes de violações em relação a disponibilidade, integridade e confidencialidade de hardware, software, redes e dados" (OCDE, 2020). De maneira similar, os padrões ISO/IEC a relacionam com a "preservação da confidencialidade, integridade e disponibilidade de informações no ciberespaço" (HUREL, 2021). Outra definição possível, identificada por Louise Hurel, é adotada pela União Europeia: A União Europeia, por outro lado, adota uma definição mais abrangente na qual segurança cibernética é definida como as atividades necessárias para proteger redes e sistemas de informação, os usuários desses sistemas e outras pessoas afetadas por ameaças cibernéticas. Nesse caso, a segurança não tem como objetivo final a segurança do ciberespaço, mas dos sistemas, usuários e informações que compõem, atuam e são afetados por ameaças e ataques cibernéticos (HUREL, 2021). Segundo o Glossário de Segurança da Informação elaborado pelo Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), define-se segurança cibernética como: Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis (BRASIL, 2022).

[18] Nos termos de Delgado, os crimes tradicionais, quando praticados pela via informática, possuem inovação apenas no modus operandi adotado. Segundo o autor: Muitas dessas condutas podem representar delitos tradicionais, cometidos através da utilização de um sistema informático. Isso pode significar simplesmente a

entende que os crimes cibernéticos impróprios são aqueles em que a tecnologia da informação é instrumentalizada para que outros bens jurídicos – já tutelados pelo ordenamento penal – sejam lesados. Sobre esses crimes, Castro defende que a legislação atual é suficiente, uma vez que os bens jurídicos tutelados já são contemplados pelo ordenamento jurídico (CASTRO, 2018, p. 115).[19]

Conforme Viana ressalva, em tal hipótese de crime não se exige do agente conhecimento técnico sobre informática. Para o autor:

> Esta simplicidade, aliada à facilidade da publicação anônima das páginas criadas em servidores gratuitos, é responsável por uma expressiva quantidade de casos de publicação de fotos pornográficas de crianças na Internet, o que em nossa legislação é crime de pedofilia, previsto no art. 241 do Estatuto da Criança e do Adolescente (ECA – Lei nº 8.069 de 13 de julho de 1990) (VIANA, 2003, p. 39).

Castro, em referência à Damásio de Jesus e José Antônio Milagre, também inclui a categoria dos crimes informáticos mistos, segundo a qual a conduta criminosa é compreendida por dois tipos penais ao mesmo tempo. Isto é, atinge o bem jurídico informático, tal qual a inviolabilidade de dados, e, concomitantemente, bem jurídico diverso (JESUS; MILAGRE *apud* CASTRO, 2018, p. 115).

Destaca-se, ainda, que o bem jurídico contemplado pelos crimes informáticos pode estar expresso na realidade na forma de *software* ou de *hardware*. Por essa razão, os crimes em análise também podem ser cometidos por meio do uso ferramentas físicas, como o uso de dispositivo para contaminar um sistema operacional com *software malicioso* (UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES, 2012, p. 11).

Outra classificação possível divide os crimes cibernéticos em 3 categorias: os crimes em que um computador ou uma rede de computadores é o objetivo final da conduta criminosa, tais quais a invasão ou o comprometimento de um sistema; adiante, os crimes tradicionais que são instrumentalizados por meio de ferramentas de computador, como fraudes online ou pornografia infantil; finalmente, os crimes em que o elemento informático

---

utilização das novas tecnologias informáticas para viabilizar a prática de condutas já tradicionalmente sancionadas pelo Direito Penal. Portanto, ao ser utilizado como mero instrumento, o sistema informático pode constituir apenas um novo modus operandi para a prática de condutas já tradicionalmente tipificadas pelo Direito Penal dos Estados, como, por exemplo, o homicídio de um paciente provocado pela adulteração intencional da dosagem de medicamentos prescrita no prontuário eletrônico do sistema informático de uma unidade de terapia intensiva de um hospital, ou mesmo a alteração de dados ou a manipulação de sistemas que controlem o pouso e a decolagem de aviões, o tráfego aéreo, as rotas de trens e de metrô, os semáforos, podendo provocar, portanto, colisões e mortes. (DELGADO, 2007, p. 20).

[19] Acrescenta-se, ainda, a abordagem de Aires José Rover apresentada por Castro: Aires José Rover, tentando definir o que seriam esses crimes cibernéticos impróprios, afirma que eles são todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta para a perpetração de crime comum, tipificável na lei penal. Dessa forma, o sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta. (ROVER *apud* CASTRO, 2018, p. 122).

apresenta menor relevância na comissão do delito, mas que a partir dele possam ser extraídas evidências do crime praticado, como informações sobre o cometimento de um assassinato (WANG, 2016, p. 9-10).

Conforme já apresentado, são múltiplas as condutas capazes de serem qualificadas como crime cibernético. Ao mesmo tempo, com o avanço das tecnologias informacionais, os procedimentos adotados se transformam, de modo que recorrentemente surjam novas possibilidades para a prática desta modalidade de crime.

Assinalando a relevância da proteção de dados pessoais neste contexto, é importante apontar que atividades potencialmente cibercriminosas contribuem para a coleta e para o armazenamento de informações pessoais. Apresentam-se, portanto, como um desafio para a garantia da autodeterminação informática dos indivíduos. Sobre esse aspecto, destaca-se a contribuição de Pessoa:

> Nesse ínterim, diversos mecanismos contribuem com a coleta e armazenamento de dados informacionais de usuários na rede, destacando-se, dentre outros, os *cookies*, *web beacons*, *spywares*, *tagging* e *tracking*. Por meio de tecnologias de todos os tipos, inclusive de técnicas de *doxxing* e *hacking*, torna-se possível criar perfis de usuários, identificar quais e quantos usuários estão engajados em rede, mapear como ocorre o comportamento dessas pessoas. E, atualmente, esses mecanismos estão espalhados nos mais diversos ambientes e espaços, por meio dos dispositivos móveis pessoais inteligentes, utilizados ao redor do globo por bilhões de pessoas, como, por exemplo, celulares, tablets, notebooks, relógios, televisores, dentre outros (PESSOA, 2020, p. 39; destacar os termos em itálico é de minha autoria).

Na sequência, esta pesquisa apresenta informações sobre a incidência e o crescimento da criminalidade cibernética, levando em consideração, especificamente, o cenário brasileiro. É relevante fazer ressalvas, no entanto, sobre as limitações metodológicas relacionadas ao uso de informações que procuram quantificar a comissão de crimes cibernéticos em determinado sistema jurídico.

O relatório *Internet Organised Crime Threat Assessment* (IOCTA), publicado pela Agência da União Europeia para a Cooperação Policial (EUROPOL) em 2020, indica algumas das referidas limitações. Em primeiro lugar, nem sempre é possível realizar o registro de todas as modalidades de crimes cibernéticos que ocorrem em um sistema jurídico. Além disso, as próprias regras de registro e de notificação divergem de um Estado para outro. Ademais, um Estado pode concentrar várias espécies de condutas dentro de um mesmo tipo penal, enquanto outro prevê tipos penais distintos. Em segundo lugar, as vítimas nem sempre noticiam os crimes virtuais pelos quais sofreram. Desse modo, registros oficiais podem representar uma incidência de crimes inferior à que efetivamente ocorre na realidade. Em terceiro, quando polícias locais não especializadas realizam o registro dos crimes e iniciam a

investigação, não necessariamente obtêm todas as informações adequadas para a posterior quantificação e qualificação dos delitos (EUROPOL, 2020, p. 19).

Para Sieber, em razão da variedade de crimes cibernéticos possíveis e da relevante incidência de crimes não registrados a nível judicial, os números normalmente divulgados sobre estes crimes não permitem conclusões profundamente acertadas sobre o estado da arte da criminalidade cibernética. No mesmo sentido, em termos de progressão histórica, as divergências em termos de definição ou de tipificação também produzem resultados limitados sobre a trajetória da criminalidade cibernética ao longo do tempo (SIEBER, 1998, p. 22). Quando examinada a incidência dos crimes cibernéticos a nível internacional, tal problemática parece ainda mais sensível, na medida em que as divergências de tipificação e de procedimentos de registros podem promover distorções nas conclusões sobre a criminalidade.

Segundo relatório da União Internacional de Telecomunicações, as dificuldades para representar a criminalidade cibernética de maneira quantitativa prejudicam a mensuração do impacto de tais crimes na sociedade (UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES, 2012, p. 14). Contudo, as informações registradas e representadas quantitativamente não devem ser desprezadas na análise da criminalidade no ciberespaço. Conforme se argumentará, é possível identificar tendências sobre os crimes cibernéticos, tais quais a natureza transnacional do delito e o aumento da incidência dos crimes nos últimos anos.

O relatório "A Caminho da Era Digital no Brasil", desenvolvido pela Organização para Cooperação e Desenvolvimento Econômico (OCDE), verificando dados produzidos pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) e pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR), aponta que o Brasil é um alvo cada vez mais frequente de ataques e ameaças à segurança digital (OCDE, 2020, p. 108).

Em relatório, a EUROPOL constatou que o Brasil é um dos principais alvos de ataques cibernéticos com origem na América Latina. Ademais, 54% dos ataques à segurança digital no Brasil possuem origem dentro do território nacional (EUROPOL *apud* OCDE, 2020, p. 108). Em termos quantitativos, pesquisa desenvolvida pela Norton Survey indicou que 70,4 milhões de brasileiros foram vítimas de crimes cibernéticos em 2017 (NORTON apud OCDE, 2020, p. 108). Assinala-se, diante das informações apresentadas, que pouco menos da metade dos ataques contra à segurança cibernética no Brasil são originados de condutas praticadas fora do território nacional.

Segundo levantamento Castro, os crimes cibernéticos se multiplicam em razão de sua rentabilidade e da falta de clareza sobre a tipificação criminal destas condutas. Dessa forma, para o autor:

> Os crimes mais rentáveis do Brasil estão hoje no campo virtual e os lucros são mais altos que os obtidos no narcotráfico, segundo a Abeat (Associação Brasileira de Especialistas em Alta Tecnologia) e a PF (Polícia Federal). Sem legislação própria, condutas ilícitas na internet estão atraindo quadrilhas que antes atuavam em crimes como roubo a bancos e tráfico de drogas, segundo a PF. Desse modo, a tendência é o aumento dos crimes cibernéticos por consequência das novas formas de tecnologia e a omissão da legislação encoraja a migração das operações da criminalidade para a internet (BELCHIOR *apud* CASTRO, 2018, p. 103).

Além desse aspecto, o relatório IOCTA, de 2020, acentua que os cibercrimes também se tornam mais comuns à medida que os indivíduos e as empresas estão progressivamente se inserindo nos espaços virtuais (EUROPOL, 2020, p. 13). Conforme multiplicam-se as relações sociais que se desenvolvem no domínio cibernético, também aumentam as condutas criminosas neste campo.

O crescimento dos crimes cibernéticos produz desafios a nível nacional e internacional, considerados de maneira genérica. No paradigma doméstico, destaca-se o fato de as tipificações tradicionais não contemplarem novas modalidades da criminalidade cibernética, o caráter transnacional dos crimes e, por consequência, eventuais conflitos de jurisdição. Quando analisados em escala internacional, as divergências em termos de harmonização legislativa sobre a tipificação criminal entre os países da sociedade internacional constituem igualmente desafios (WANG, 2016, p. 17).

Jonathan Clough apresenta seis desafios impostos pelos crimes cibernéticos: a) escala; b) acessibilidade; c) anonimato; d) portabilidade e transferibilidade; e) alcance global; e f) ausência de guardiões capazes. Os desafios relacionados à escala dizem respeito ao fato de que a internet possibilita comunicações entre múltiplas pessoas de maneira rápida e barata. Sob este prisma, considerando o imenso número de indivíduos conectados à internet, há enorme número de pessoas potencialmente sujeitas a ofensas cibernéticas. Conecta-se com o desafio anterior a questão da acessibilidade, na medida em que o acesso à internet se tornou mais popular, sem exigir expertise técnica para o seu manejo (CLOUGH, 2010, p. 5-8).

Na sequência, o anonimato é percebido como desafio uma vez que implica em uma vantagem ao criminoso, dificultando a sua identificação pela vítima e pelas instituições de persecução criminal. Ao mesmo tempo, rastrear informações que percorrem várias jurisdições distintas contribui para complexificar as formas de identificação do sujeito criminoso. A portabilidade e transferibilidade de dados impõe desafios pois, com o desenvolvimento

tecnológico, tornou-se viável armazenar e transferir dados (imagens, sons, frases) a um baixo custo, exportando-os rapidamente para *sites* na *web* (CLOUGH, 2010, p. 5-8).

O alcance global, já referido anteriormente, apresenta-se como um desafio uma vez que as redes de computadores ultrapassam as fronteiras jurisdicionais onde os crimes são praticados ou onde suas consequências ocorrem. Dessa forma, um crime pode ser praticado e produzir resultados em qualquer local onde haja conexão de internet. Por fim, a ausência de guardiões capazes é destacada como um desafio. Trata-se da percepção do agente que pratica o crime cibernético de que há um baixo risco de ser identificado e que a persecução penal tenha continuidade. Segundo Clough, este elemento é um obstáculo em razão de a natureza dos dados eletrônicos, por meio dos quais se verifica o crime cibernético, exigir técnicas forenses sofisticadas e, ao mesmo tempo, comunicações rápidas entre autoridades responsáveis pela persecução criminal de jurisdições distintas (CLOUGH, 2010, p. 5-8).

Ressalta-se, ademais, a natureza transnacional dos crimes cibernéticos. O fato de a conduta criminosa e os seus efeitos facilmente se manifestarem em múltiplos Estados gera conflitos positivos de jurisdição, nos quais há disputa sobre qual país é competente para processar criminalmente o agente da conduta. Os crimes cibernéticos, portanto, são fatos que ocorrem dentro de um território nacional, ainda que potencialmente provoquem impactos a nível internacional (WANG, 2016, p. 17).[20]

Procurou-se apresentar nesta seção definições possível sobre o crime cibernético, buscando ressaltar, igualmente, a crescente relevância deste crime para os Estados no tempo contemporâneo. Observou-se que o termo cibercrime engloba um rol amplo de condutas possíveis, de modo que produza desafios relacionados a sua compreensão e tipificação. Assinala-se, por fim, a relevância dos dados computacionais para as condutas que implicam no crime cibernético, de modo que esses devam ser examinados atentamente quando da investigação da abordagem estatal de enfrentamento aos referidos crimes.

---

[20] A título de exemplo da potencialidade transnacional da delinquência cibernética, menciona-se o "Love Bug", destacado por Qianyun Wang: Em 2000, o vírus do "Love Bug" surgiu em Hong Kong e percorreu o mundo dentro de 2 horas. Ao destruir documentos e roubar senhas, o vírus comprometeu milhões de computadores, incluindo máquinas utilizadas pela *US National Aeronautics,* pela *Space Administration* (doravante NASA) e pelo Parlamento britânico. As perdas provocadas por esse vírus foram estimadas na faixa de 10 bilhões de dólares, com vítimas em mais de 20 países. Tradução livre da versão original: The most frequently cited case – the 'Love Bug' virus case – illustrates this problem. In 2000, the Love-Bug virus appeared in Hong Kong and had raced around the world within two hours.57 By destroying files and stealing passwords, it impaired millions of computers, including computers used by the US National Aeronautics and Space Administration (hereafter NASA) and the UK Parliament.58 The losses caused by this virus have been estimated to be in the region of $10 billion, with victims in as many as 20 countries (WANG, 2016, p. 17).

1.2.2 Os crimes cibernéticos na legislação brasileira.

Na seção anterior foi abordada uma definição possível para os crimes cibernéticos a partir da perspectiva doutrinária, bem como se observou uma primeira classificação em torno do bem jurídico afetado: crimes cibernéticos próprios e impróprios. Nesta seção, pretende-se avançar na investigação sobre os crimes cibernéticos a partir da citação dos dispositivos legais que tipificam tais condutas, com a finalidade de observar a relevância dos dados computacionais para este fenômeno criminoso.

Inicia-se esta seção ressaltando a importância da tipificação no Direito Penal para a racionalização da tutela criminal. Conforme aduz Castro, "a construção de uma dogmática própria do sistema de crimes cibernéticos passa, necessariamente, pelo crivo do princípio da legalidade e da teoria do tipo penal" (CASTRO, 2018, p. 111).

Ademais, ressalta-se o pressuposto anteriormente aduzido de que a temática da segurança cibernética tem se tornado progressivamente mais importante na atualidade. No caso brasileiro, identifica-se a crescente institucionalização deste tema para além da abordagem a nível do Direito Penal.

Observa-se, em escala nacional, que o Brasil tem desenvolvido um marco institucional com vistas a defesa da segurança digital. A Estratégia Nacional de Segurança Cibernética, de 2020, é um indicativo importante da importância que passa a ser associada à temática. Não se trata, contudo, de novidade. As políticas direcionadas à segurança digital datam desde o início dos anos 2000, com maior ou menor intensidade (OCDE, 2020, p. 109). Salienta-se como marcos importantes da institucionalização da segurança cibernética no Brasil a promulgação do Marco Civil da Internet, de 2014, no contexto dos escândalos de espionagem envolvendo os Estados Unidos da América (EUA), e dos novos estímulos que surgiram a partir da celebração de grandes eventos internacionais na década de 2010 (HUREL; LOBATO, 2018, p. 3).[21]

[21] O relatório publicado pela OCDE organiza as políticas brasileiras no setor da segurança digital em 3 momentos, a serem brevemente apresentados. O fio condutor que organiza a divisão pode ser representado pela transição da ênfase das políticas públicas de segurança digital de uma perspectiva técnica, entre 2000 e 2011, para uma dimensão de segurança nacional. O primeiro, entre 2000 e 2012, é caracterizado pela ênfase ao setor público, em que alguns dos marcos institucionais são a criação do Comitê Gestor da Segurança da Informação no âmbito da administração pública federal, do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CITR Gov), em 2004, e designação do Gabinete de Segurança Institucional da presidência da República como órgão principal para questões de segurança. Assinala-se, ainda, o Livre Verde sobre Segurança Cibernética, de 2010, que pode ser considerado um precedente da Estratégia Nacional de 2020. No segundo momento, entre 2012 e 2017, a segurança cibernética é alçada a assunto de segurança nacional, especialmente diante do fato de o Brasil sediar megaeventos (Rio +20, Copa do Mundo de Futebol de 2014 e Olimpíadas de 2016) e do escândalo de espionagem cibernética revelado por Edward Snowden, em que um dos marcos é a criação do Centro de Monitoramento Cibernético. Por fim, a partir de 2018, há compreensão mais ampla da segurança cibernética, englobando a cooperação entre o setor público e privado, e buscando garantir a segurança

A garantia de uma segurança cibernética – ou segurança da informação, a depender da opção terminológica – passa por desafios multifacetados para o Estados. Conforme apresenta o relatório "A Caminho da Era Digital no Brasil", a segurança cibernética abrange, pelo menos, quatro dimensões: a segurança nacional; a prosperidade econômica e social; a tecnologia; e a aplicação da lei. Cada espectro englobado, no entanto, tende a mobilizar interesses difusos ou mesmo conflitantes, produzindo contextos de maior complexidade (OCDE, 2020, p. 119).[22]

De acordo com o relatório elaborado pelo Instituto Igarapé, a institucionalização da segurança cibernética no Brasil possui 4 características:

> [...] (i) a excessiva securitização[23] e a acentuada militarização da segurança cibernética; (ii) a exclusão de atores não estatais da definição dos termos relevantes da agenda política; (iii) a ainda maior preferência por soluções que procuram bloquear aplicações ou remover conteúdos; e (iv) a contínua dificuldade de coordenar ações no nível da Administração Pública Federal (HUREL; LOBATO, 2018, p. 3).[24]

---

nos ambientes digitais do Brasil como um todo. A Estratégia Brasileira para a Transformação Digital, de 2018, é instrumento que indica a transição para esta nova fase, a qual reafirma a necessidade de se pensar a segurança cibernética como prioridade à defesa nacional. Menciona-se também a Política Nacional de Segurança da Informação, publicada em 2018 e desenvolvida pelo Gabinete de Segurança Institucional da Presidência da República (OCDE, 2020, p. 109-118).

[22] Sobre o assunto, assinala-se o exemplo mencionado pelo Relatório "A Caminho da Era Digital no Brasil", da OCDE: A política da criptografia é um exemplo típico de objetivos conflitantes: empresas, organizações e consumidores, promovem o uso não regulado da criptografia para gerar confiança, facilitar o e-commerce e apoiar governos digitais e inovação on-line, enquanto agentes da lei e de inteligência, pedem mais regulamentos para facilitar o acesso a dados criptografados, a fim de combater criminosos e terroristas (OCDE, 2020, p. 119).

[23] É relevante apresentar brevemente o conceito de securitização e sua aplicação à segurança cibernética. Trata-se de processo explorado com base na contribuição da Escola de Copenhague para os estudos de segurança internacional (HANSEN, NISSENBAUM, 2009; LOBATO; KENKEL, 2015; VALES, 2016; VALERIANO, MANESS, 2018). parte-se do pressuposto de que as ameaças de segurança são construídas socialmente, mediante importante papel do ato discursivo (WAEVER, 2012). É possível, portanto, que determinado assunto seja elevado à agenda de segurança como ameaça nacional em razão de construção social na qual o discurso possui papel fundamental (LOBATO; KENKEL, 2015). A projeção de um risco ao nível de ameaça à segurança nacional pode ser realizada pelos atores que possuem a autoridade necessária a nível discursivo, tais quais líderes políticos e burocratas. Nesse processo, o ato discursivo qualifica uma ameaça, seja ela real ou não, enquanto objeto de securitização (BUZAN; WAEVER; DE WILDE, 1998). Especificamente em relação ao processo de securitização no ciberespaço, Lene Hansen e Helen Nissenbaum definem características comuns que vinculam os objetos, as ameaças e os atores de securitização: a) a hipersecuritização, fazendo referência à expansão da securitização para além dos níveis considerados normais de ameaça; b) prática diária de segurança, segundo a qual as ameaças à segurança digital estão ligadas a aspectos da vida cotidiana dos indivíduos e das organizações; e c) tecnificação, de modo que o discurso técnico ganha ênfase em razão de as ameaças serem constituídas no campo hipotético – isto é, a tecnificação contribui para a validação do discurso de securitização ao dar-lhe maior autoridade. Dessa forma, o discurso de securitização frequentemente parte de suposições sobre os possíveis danos em caso de as medidas adequadas de segurança não serem tomadas (HANSEN; NISSENBAUM, 2009).

[24] Tradução livre. Na versão original: We identified at least our major effects resulting from the accelerated institutionalization process and the mega events in Brazil, that is: (i) the excessive securitization and accentuated militarization of cybersecurity; (ii) the exclusion of non-state actors from the definition of terms relevant to the political agenda; (iii) the ever-greater preference for solutions which seek to block applications, remove content; and (iv) the continuous difficulty of coordinating action at the level of the Federal Public Administration. (HUREL; LOBATO, 2018, p. 3).

O relatório supramencionado destaca que destas características resulta um aparente conflito entre medidas proibicionistas e de criminalização com políticas pautadas na defesa de direitos no âmbito virtual. Outro efeito delineado é a baixa integração entre agentes governamentais, sociedade civil, setor privado e academia na formulação de políticas públicas voltadas à segurança cibernética, bem como a baixa integração entre as instituições responsáveis pelo tema a nível nacional (HUREL; LOBATO, 2018, p. 3).

A partir de 2018, contudo, mediante iniciativas baseadas na Estratégia Brasileira para a Transformação Digital, de 2018, e na Estratégia Brasileira de Segurança Cibernética, de 2020, houve incentivos normativos para a priorização também da colaboração entre os setores público e privado, de modo a ser incentivada a coordenação entre instituições voltada à temática (OCDE, 2020, p. 109-118).

Destacam-se, especificamente, os objetivos propostos pela Estratégia Nacional de Segurança Cibernética. O documento manifesta o interesse de transformar o Brasil em um país de "excelência em segurança cibernética", com a finalidade de o tornar um espaço mais próspero e confiável no ambiente digital, de incrementar as capacidades brasileiras contra as ameaças cibernéticas e de fortalecer a atuação brasileira no cenário internacional no que tange a temática (BRASIL, 2020). Ponto relevante concebido na Estratégia, dentre os objetivos previstos no documento que pretende nortear a atuação brasileira no tema, é inclusão da atuação a nível internacional para se atender ao tema da segurança cibernética.

Observou-se, portanto, a crescente importância da temática para o Estado brasileiro. Dessa forma, a segurança cibernética é percebida como relevante para a segurança nacional, de modo que transformações institucionais procurem refletir a crescente importância do assunto no corpo jurídico nacional.

No ordenamento jurídico brasileiro, os esforços para a tipificação dos crimes cibernéticos datam dos anos 1990. A Lei nº 9.504, de 24 de julho de 1996, que estabelece normas para as eleições, prevê como crimes puníveis com reclusão condutas inseridas no escopo dos crimes cibernéticos que atentem contra a lisura do processo eleitoral. Os crimes previstos nesta legislação incluem o acesso ao tratamento automático de dados utilizado pelos serviços eleitorais, com a finalidade de alterar a contagem de votos, e o desenvolvimento de software capaz de comprometer o sistema de tratamento automático de dados utilizado pelo serviço eleitoral (BRASIL, 1996).[25]

[25] Nos termos da legislação mencionada: Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos: I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos; II - desenvolver ou introduzir comando, instrução, ou programa de

A Lei nº 9.983, de 14 de julho de 2000, insere, dentre outros, os artigos 313-A e 313-B no Código Penal, os quais incluem igualmente condutas classificáveis como crimes cibernéticos contra a seguridade social (BRASIL, 2000).[26] Na sequência, a Lei nº 10.695, de 01 de julho de 2003, inclui tipificação no que tange à pirataria cibernética, com ênfase na defesa dos direitos autorais (BRASIL, 2003).[27]

Adiante, menciona-se a Lei nº 11.829, de 25 de novembro de 2008, que altera o Estatuto da Criança e do Adolescente com o objetivo de aprimorar o combate à pornografia infantil. Tal inovação legislativa ampliou a tipificação já existente no ordenamento jurídico pátrio e aumentaou pena para os referidos crimes. Inclui-se, nesse sentido, a reprodução ou o registro, por exemplo, de cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente, por qualquer meio. A legislação também amplia a responsabilidade criminal nas condutas do artigo 241-A ao incluir nas penas os agentes que assegurem os meios ou serviços para o armazenamento do conteúdo ou que assegurarem, por qualquer meio, o acesso por rede de computadores ao conteúdo associado à pornografia infantil (BRASIL, 2008).

Em 2012, houve importante desenvolvimento da temática com a publicação da Lei nº 12.735. Trata-se de legislação que tipifica os crimes cibernéticos próprios, já apresentados na seção anterior. A referida Lei tipifica o crime de invasão de dispositivo informático[28] e insere

---

computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral; III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes (BRASIL, 1996).

[26] Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano; Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente (BRASIL, 2000).

[27] Art. 184. Violar direitos de autor e os que lhe são conexos: § 3o Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente (BRASIL, 2003).

[28] Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita [...]; § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput; § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico; § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave; § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos; § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

o parágrafo primeiro do artigo 266 do Código Penal, que trata da interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (BRASIL, 2012-A).

Recentemente, em 2021, a Lei nº 14.155 alterou o Código Penal ao ampliar as penas destinadas aos crimes de violação de dispositivo informático, furto e estelionato praticados pela via eletrônica ou pela internet. Esta lei também inova em alterar o dispositivo previsto na Lei nº 12.737 de 2012, retirando a exigência de que o crime de invasão de dispositivo informático ocorra mediante violação indevida de mecanismo de segurança. Há, portanto, ampliação da abrangência deste tipo penal (BRASIL, 2021).

Segundo determinado pela Lei nº 14.155 de 2021, o crime de fraude eletrônica é definido a partir da conduta de estelionato cometida mediante uso de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo (BRASIL, 2021). Dessa forma, conclui-se que a inovação legislativa de 2021 aprofunda a criminalização dos crimes cibernéticos

A temática da segurança no espaço cibernético ganha relevância no cenário atual, de modo a produzir novas demandas para fins de contenção da criminalidade cibernética. Verifica-se, em síntese, que houve esforço por parte do legislador brasileiro em tipificar condutas criminosas praticadas pela via informática para oferecer repostas mais adequadas a este fenômeno.

2 A TUTELA JURÍDICA DA PROTEÇÃO DE DADOS PESSOAIS E O ENFRENTAMENTO AOS CRIMES CIBERNÉTICOS

A progressiva digitalização das atividades sociais ampliou a produção, o armazenamento e o intercâmbio de dados e informações entre diferentes agentes, sejam elas públicos ou privados. Esse processo ampliou a importância dos dados pessoais a ponto de torná-los relevantes aos estudos jurídicos.

Nesse contexto, desenvolve-se o conceito e as aplicações do direito à proteção de dados, o qual possui reflexos amplos em diversas dimensões do estudo jurídico. Nesta dissertação, concentra-se os esforços na análise do direito à proteção de dados quando aplicado à cooperação internacional em matéria penal, com vistas ao enfrentamento dos crimes cibernéticos. Busca-se avaliar sua inserção nos instrumentos de auxílio mútuo presente na Convenção de Budapeste sobre Cibercrime, de 2001, especialmente a medida de acesso transfronteiriço a dados informáticos armazenados.

Diante desta proposta, faz-se necessário examinar, inicialmente, a posição do direito à proteção de dados enquanto Direito Humano, bem como sua aplicação no contexto do Direito Processual Penal. Para tanto, pretende-se fazer uso de revisão da literatura produzida sobre o tema, especialmente na doutrina brasileira, com a finalidade de identificar o panorama contemporâneo do direito à proteção de dados no paradigma da cooperação jurídica internacional penal.

Enquanto fontes primárias, são analisados os marcos jurídicos fundamentais sobre a temática no ordenamento jurídico brasileiro, quais sejam a Constituição Federal, o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD). Ademais, considerando a importância da harmonização legislativa a nível internacional para o aprofundamento da articulação entre as instituições responsáveis pelas atividades de investigação e de cooperação jurídica internacional, a análise também integrará o *General Data Protection Regulation* (GDPR), de 2016, e a Diretiva n.º 2016/680, a qual aborda especificamente a proteção de dados pessoais para efeitos de prevenção, investigação, detenção ou repressão de infrações penais ou execução de sanções penais.

Levando em consideração os termos apresentados, procura-se examinar, neste capítulo, a aplicação do direito à proteção de dados no contexto do Direito Penal Transnacional. Uma vez assentadas as bases doutrinárias e normativas atreladas ao direito à proteção de dados pessoais aplicado à cooperação internacional em matéria penal para o

enfrentamento dos crimes cibernéticos, a investigação procederá para o estudo específico dos mecanismos previstos na referida Convenção de Budapeste, no capítulo seguinte.

2. 1 A REGULAMENTAÇÃO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

Com a finalidade de apresentar os fundamentos em que se insere o direito à proteção de dados pessoais no contexto da cooperação jurídica internacional em matéria penal, é necessário, preliminarmente, identificar o processo de regulamentação do direito à proteção de dados pessoais, sobretudo no regime jurídico brasileiro.

Levando em consideração que o objeto de estudo desta pesquisa está centrado na cooperação entre o Brasil e os países membros da União Europeia, amplamente considerada, aborda-se também a regulamento do direito à proteção de dados pessoais no âmbito da integração europeia.

2.1.1 A privacidade e a proteção de dados pessoais

O direito à proteção de dados pessoais ganha maior relevância à medida que se complexifica o processo de digitalização das atividades sociais. Mais dados e informações são produzidos, armazenado e intercambiados, aos quais são atribuídos maior importância em razão de suas aplicações, tanto por agentes públicos quanto privados, a nível nacional e internacional.

Na era digital, a informação assume espaço como instrumento de poder. Os avanços tecnológicos inserem os dados e informações como objetos que provocam implicações aos indivíduos, às organizações e aos Estados (PINHEIRO, 2013, p. 42-25), afetando, destarte, as novas concepções e aplicações do direito à privacidade e à intimidade.

Sobre a denominada era digital, Andrew Burt realça o aspecto de transformação digital em múltiplos aspectos da vida cotidiana. O autor menciona, de maneira exemplificativa, a ampliação da quantidade de câmeras de segurança capitando um imenso volume de imagens, ou, ao mesmo tempo, como os meios de comunicação passam a envolver cada vez mais o uso de computadores ou de protocolos de internet (BURT, 2020, p. 1). Nesse sentido, trata-se de "um mundo que é crescentemente e irresistivelmente digital, e que a sua digitalização produz impactos profundos na nossa vida cotidiana" (BURT, 2020, p. 1-2).[29]

Por um lado, a progressiva digitalização produz benefícios, podendo tornar o mundo "mais conveniente". Isto é, facilitando formas de pagamento, de comunicação e de

[29] Tradução livre. Na versão original: The lesson? We live in a world that's increasingly and irresistibly digital, and this digitization is having deep and profound impacts on our daily lives (BURT, 2020, p. 1-2).

deslocamento. Por outro, a ampliação do uso de softwares e de outros sistemas computacionais permitiu que os grupos que desenvolvem e controlam estas tecnologias sejam capazes de influenciar o comportamento de dispositivos conectados e, inclusive, a "estrutura da vida online" (BURT, 2020, p. 2).

O desenvolvimento tecnológico contribuiu para a construção de um ambiente em que se combinam a abundância de dados, amplamente produzidos na era digital, as capacidades computacionais mais baratas e mais rápidas e as novas técnicas de identificação pessoal. Por essa razão, o incremento das formas de coleta e de armazenamento de dados, bem como a capacidade de processamento destes, faz com que as possibilidades e a escala de identificação pessoal também cresçam (BURT, 2020, p. 4). Trata-se de contexto produz amplos desafios para o direito à privacidade.

O direito à proteção de dados pessoais, por sua vez, está ligado ao direito à privacidade. No entanto, se a proteção de dados se torna relevante à medida que os avanços tecnológicos produzem novas possibilidades no mundo cibernético e integram cada vez mais pessoas ao seu escopo, o direito à privacidade encontra bases mais antigas.

O direito à privacidade, nos termos de Stefano Rodotà, é definido a partir de duas frentes principais: o direito de deter o controle sobre as informações que dizem respeito a si próprio, bem como o direito de determinar a construção da esfera privada pessoal (RODOTÀ, 1995, p. 122). Percebe-se, nesse sentido, a relevância do conteúdo das informações pessoais de cada indivíduo e a sua conexão com a própria expressão da esfera privada individual.

Ressalva-se, preliminarmente, que a forma de se compreender a privacidade – inserida em um paradigma maior de "público" e "privado" – parte da composição significados que se somaram ao longo de um processo histórico, que não apresentam necessariamente aproximações precisas para explicar as relações humanas. Seguindo esta hipótese, a definição de privacidade em si, assim como suas extensões, pode não constituir o cerne do debate (HABERMAS *apud* DONEDA, 2020, p. 78-79). Entende-se, todavia, que a relevância normativa atribuída à privacidade, conforme se destacará neste capítulo, acrescida de sua correlação com a proteção de dados, contribui para construir um caminho lógico coerente para se apresentar o direito à proteção de dados enquanto direito fundamental.

Mesmo a proposição de um conceito de privacidade, nesse sentido, parte da relação entre o indivíduo e a sociedade. Insto é, encontra fundamento no "estabelecimento de uma esfera privada livre das ingerências" do ente público que se formava no contexto de origem dos Estados modernos (DONEDA, 2020, p. 87).

De acordo com a contribuição de Danilo Cesar Maganhoto Doneda, o direito à privacidade faz parte dos direitos da personalidade, sendo aplicável a ideias como a igualdade entre os indivíduos, a liberdade de escolha e a não-discriminação (DONEDA, 2020, p. 31). A origem do direito à privacidade não se traduz imediatamente às aplicações e interpretações contemporâneas – uma vez que aqui se considera, dentre outros fatores, as novas possibilidades e funcionalidades produzidas pelos avanços tecnológicos. Há um processo de desenvolvimento da maneira de se compreender a privacidade que ainda está em curso. O direito à proteção de dados pode ser inserido em parte deste processo.

O clássico artigo de Louis Brandeis e de Samuel Warren, de 1890, apresentava uma ideia de privacidade lastreada no "direito de ser deixado em paz". Os autores imaginavam um cenário onde a intensidade e a complexidade das novas relações sociais tornaram necessário algum nível de isolamento, de modo a implicar em uma valorização da privacidade. Trata-se, portanto, do direito de os indivíduos poderem determinar a extensão máxima que seus pensamentos, sentimentos e emoções seriam comunicadas publicamente (WARREN, BRANDEIS, 1890, p. 196-198).

Inicialmente, o direito à privacidade estava intrinsecamente conectado a uma perspectiva de "individualismo exacerbado". Esta concepção, no entanto, trazia como paradigma o pressuposto de que a privacidade poderia ser concebida como a ausência de comunicação entre um indivíduo e os demais. O passo seguinte do amadurecimento das interpretações sobre o direito à privacidade é marcado pela sua inclusão como um "aspecto fundamental da realização da pessoa e do desenvolvimento da sua personalidade" (WARREN; BRANDEIS *apud* DONEDA, 2020, p. 31-32).[30]

Doneda indica alguns elementos determinantes para a transformação na forma de se compreender o direito à privacidade:

> Vários motivos contribuíram para uma inflexão dessa tendência, e entre tantos citamos os desdobramentos de um modelo de Estado liberal que se transmudava no *welfare state*, a mudança do relacionamento entre cidadão e Estado, uma demanda mais generalizada de direitos como consequência dos movimentos sociais e das

[30] Sobre a contribuição de Warren e Brandeis, Doneda explica: O artigo "*The right to privacy*", geralmente citado como uma solitária referência histórica, é na verdade parte de um contexto bem mais amplo no qual a sociedade norte-americana e o sistema capitalista se encontravam. A expansão para o oeste, que influenciou fortemente a simbologia, cultura e os costumes dos norte-americanos, tinha acabado – o historiador F. J. Turner declarara "encerrada a era das fronteiras" em 1893. O artigo de Warren e Brandeis reflete a tendência a uma fundamentação diversa para a proteção da privacidade, desvinculada do direito de propriedade. Um de seus pontos centrais é a observação de que o princípio a ser observado na proteção da privacidade (no caso específico, na publicação de escritos pessoais) não passa pela propriedade privada, porém pela chamada *inviolate personality* (DONEDA, 2020, p. 90). A privacidade, enquanto um direito, se desvinculava da noção de propriedade, de modo a se caracterizar como de natureza pessoal. O contexto em que se inseria estava visão de ruptura é a ascensão das novas tecnologias associadas à comunicação, como a fotografia e os jornais, em um cenário onde a comunicação de massa ganhava relevância (DONEDA, 2020, p. 90-91).

> reivindicações da classe trabalhadora, assim como o aludido crescimento do fluxo de informações, consequência do desenvolvimento tecnológico – ao qual correspondia uma capacidade técnica cada vez maior de recolher, processar e utilizar a informação (DONEDA, 2020, p. 33; a diferenciação do trecho para o itálico é de minha autoria).

Para o referido autor, a maior demanda pelo reconhecimento ampliado de direitos, no contexto de desenvolvimento do *welfare state*, bem como o aumento do fluxo de informações, resultante, dentro outros aspectos, do aperfeiçoamento tecnológico, são elementos que expandem a compreensão do direito à privacidade. Neste contexto, novas atribuições e utilidades são dotadas às informações pessoais, as quais assumem progressivamente maior importância (DONEDA, 2020, p. 33-34).

James Whitman identifica duas correntes no mundo Ocidental para compreender o direito à privacidade, cada qual fundamentada na própria história e na produção de ideias de cada região. Ressalta-se, neste momento, que a divisão de "mundo Ocidental" proposta pelo autor considera apenas 2 trajetórias: a dos Estados Unidos e a da Europa ocidental. De um lado, o desenvolvimento europeu sobre o tema atrela a privacidade ao princípio da dignidade humana. De outro, a doutrina estadunidense correlaciona a privacidade ao direito à liberdade, levando em consideração, especialmente, ameaças de abuso por parte do governo (WHITMAN, 2003, p. 91).

A privacidade, mais do que produto de um esforço lógico-filosófico insulado, nos termos de Whitman, é o resultado de "ideias e ansiedades locais" de cada região. No paradigma estadunidense, tais ideais buscam garantir a segurança em favor da liberdade dos indivíduos frente o Estado. Segundo a lógica europeia, o foco está no desejo de garantir a "honra" e a dignidade dos indivíduos na sociedade (WHITMAN, 2003, p. 92).

Embora faça-se esta distinção, Whitman entende que as diferenças na maneira de valorar a privacidade devem ser encaradas de forma relativa e não definitiva. Não há, segundo o raciocínio apresentado pelo autor, contradição em perseguir a concretização da privacidade com base nas duas formas em que é compreendida (WHITMAN, 2003, p. 92). Nesse sentido:

> É perfeitamente possível advogar tanto pela privacidade contra o Estado quanto pela privacidade contra coletores de informações não estatais – ao argumentar que proteger a privacidade significa, ao mesmo tempo, resguardar a expressão do eu e inibir excessos de investigação e de regulação por parte do Estado (WHITMAN, 2003, p. 92).[31]

Rob van den Hoven Genderen resgata, em sua abordagem sobre o tema, 4 dimensões relativas ao conceito de privacidade: a privacidade da pessoa, relacionada a integridade do

[31] Na versão original: It is perfectly possible to advocate both privacy against the state and privacy against non-state information gatherers—to argue that protecting privacy means both safeguarding the presentation of self and inhibiting the investigative and regulatory excesses of the state (WHITMAN, 2003, p. 92).

corpo de determinado indivíduo, de modo a resguardar, por exemplo, a esterilização compulsória ou a retira da amostras sanguíneas; a privacidade relacionada a comportamentos pessoais, tais quais a orientação sexual, preferências políticas ou práticas religiosas; a privacidade relacionada às comunicações pessoais; e a privacidade de dados pessoais, envolvendo dados que não deveriam estar "automaticamente disponíveis para outros indivíduos ou organizações" e aos quais os titulares devem possuir controle sobre o seu uso (CLARCKE *apud* GENDEREN, 2008, p. 6-7).

São múltiplas as formas de se compreender a privacidade. Estas, ainda, modificam-se ao longo do tempo e apresentam disparidades a depender do espaço onde são concebidas. Contudo, a percepção da privacidade como um valor fundamental inserido no rol de direitos humanos não deve ser afastada do estudo das bases do direito à proteção de dados.

2.1.2 Dados e informações pessoais em relação ao direito à privacidade

Identificou-se, nesta pesquisa, algumas definições possíveis para o termo "informações pessoais".[32] Em primeiro lugar, cabe apresentar o conceito de dado antes de avançar para uma definição de informação. Segundo Valdemar Setzer, um dado é "uma sequência de símbolos quantificados ou quantificáveis", o que inclui, por exemplo, letras, imagens e sons, ainda sejam estes ininteligíveis para determinado interlocutor. Na medida em que se trata de símbolos quantificáveis, os dados podem ser armazenados e processados por computadores (SETZER, 1999, p. 1-2). O termo "dado" é definido por Doneda como uma pré-informação, que apresenta um sentido "primitivo" e "fragmentado", estando em uma etapa anterior ao processo de interpretação e de elaboração (DONEDA, 2020, p. 139).

As informações são "abstrações informais", na forma de textos, imagens, sons ou animações, que apresentam alguma significação para um interlocutor. Uma informação, assim sendo, não poderia ser processada por um computador – seria necessário, antes, reduzi-la a estrutura de dado quantificável. Todavia, as informações podem ser representadas por meio de dados, que, por sua vez, podem ser processados por computadores, embora esse fato não implique no processamento da significação atribuída à informação (SETZER, 1999, p. 2). Nos termos de Pierre Catala, a informação "pode ser definida como a formação de uma mensagem comunicável" (CATALA, 1998, p. 224).[33]

---

[32] A Lei nº 12.527, de 2011, considera a seguinte definição para informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato (BRASIL, 2011).

[33] Tradução livre. Na versão original: L'information peut se définir comme la formulation d'un message communicable (CATALA, 1998, p. 224).

Para Setzer, quando os dados inteligíveis são observados por um interlocutor, eles assumem a qualidade de informação, uma vez que a eles são atribuídos um significado. Dessa forma, os dados se distinguem-se das informações ao se considerar que estes possuem um conteúdo "semântico", enquanto aqueles são "puramente sintáticos". Isto é, o dado é puramente "objetivo", enquanto a informação é "objetiva-subjetiva" (SETZER, 1999, p. 2-5). A informação, destarte, se difere dos dados em razão do elemento cognitivo que a ela é atribuído (DONEDA, 2020, p. 139). Segundo Norbert Wiener, a informação é o "termo que designa o conteúdo daquilo que permutamos com o mundo exterior ao ajustar-nos a ele, e que faz com que nosso ajustamento seja nele percebido" (WIENER, 1954, p. 17). Por consequência, "a pura ideia abstrata não é informação antes de estar fundida com signos inteligíveis" (CATALA, 1998, p. 228).[34]

Embora exista uma distinção técnica entre as definições de "dado" e de "informação", Doneda reconhece que a legislação brasileira frequentemente utiliza os dois termos de maneira indistinta (DONEDA, 139). Opta-se por utilizar, nesta pesquisa, o rigor previsto na legislação brasileira ao longo do texto.

As informações podem ser classificadas de acordo com o seu conteúdo. Segundo Catala:

> Pierre Catala, ao traçar um esboço de uma teoria jurídica da informação, classificou-a em quatro modalidades: (i) as informações relativas às pessoas e seus patrimônios; (ii) as opiniões subjetivas das pessoas; (iii) as obras do espírito; e, finalmente, (iv) as informações que, fora das modalidades anteriores, referem-se a "descrições de fenômenos, coisas, eventos". A nós interessa, precisamente, a primeira delas [...]. Novamente, é Pierre Catala que identifica uma informação pessoal quando o objeto da informação é a própria pessoa: "Mesmo que a pessoa em questão não seja a 'autora' da informação, no sentido de sua concepção, ela é a titular legítima dos seus elementos. Seu vínculo com o indivíduo é por demais estreito para que pudesse ser de outra forma. Quando o objeto dos dados é um sujeito de direito, a informação é um atributo da personalidade" (CATALA *apud* DONEDA, 2020, p. 141).

A legislação brasileira considera, pela Lei de Acesso à Informação, o termo informação pessoal como "aquela relacionada à pessoa natural identificada ou identificável" (BRASIL, 2011). De maneira idêntica, a Lei Geral de Proteção de Dados Pessoais define como dado pessoal a "informação relacionada a pessoa natural identificada ou identificável" e, adiante, qualifica como dado pessoal sensível aquela que tem como conteúdo a "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico" (BRASIL, 2018). Esta última categoria de dados, em razão de seu conteúdo, a

[34] Na versão original: La pure idée abstraite n'est pas information avant d'être coulée en signes intelligibles (CATALA, 1998, p. 228).

depender do tipo de uso ou tratamento ao qual forem submetidos, pode redundar em uma ação discriminatória ou lesiva aos titulares ou demais pessoas relacionadas, motivo pelo qual possui abordagem diferenciada (DONEDA, 2020, p. 144).[35]

A definição constante no ordenamento jurídico brasileiro está em consonância com a definição presente na Convenção 108 do Conselho da Europa, segundo a qual os dados pessoais são qualquer informação relativa a um indivíduo identificado ou identificável (CONSELHO DA EUROPA, 1981).[36]

Reforça-se a necessidade de que o dado seja identificável a um indivíduo, de sorte que seja possível nomear a(s) pessoa(s) a ele relacionadas. Por essa razão, na hipótese de determinado dado fazer referência a pessoa indeterminada, este será qualificado como um dado anônimo, e, portanto, distinto do dado pessoal ou da informação pessoal (DONEDA, 2020, P. 142).

Destaca-se o entendimento de Doneda sobre o alcance do vínculo entre indivíduo e informação para a caracterização desta como pessoal:

> A informação pessoal, em um certo sentido, pode ser desvinculada da pessoa: ela pode circular, submeter-se a um tratamento, ser comunicada, etc. Contudo, até o ponto em que continua sendo uma informação "pessoal", isto é, identificando a pessoa a qual se refere, a informação mantém um vínculo indissolúvel com a pessoa, e sua valoração específica deve partir basicamente dela ser uma representação direta da pessoa. Por força do regime privilegiado de vinculação entre a informação pessoal e a pessoa à qual ela se refere – como representação direta de sua personalidade –, tal informação deve ser entendida, portanto, como uma extensão da sua personalidade (DONEDA, 2020, p. 146-147).

As informações pessoais apresentam um vínculo objetivo com o indivíduo ao qual se referem. Isto é, podem dizer respeito a uma característica ou a uma ação de determinada pessoa. No primeiro caso, cita-se como exemplo o próprio nome civil do indivíduo ou o seu domicílio. No segundo, dados relacionados ao comportamento de consumo ou sobre opiniões manifestadas pelo indivíduo. Consoante Doneda, é essencial a conformação de um vínculo objetivo entre a informação e a pessoa, com a finalidade de afastar outras informações que, embora relacionadas ao indivíduo, não devem ser caracterizadas propriamente como informações pessoais, tais quais a opinião de outrem sobre o indivíduo em questão (DONEDA, 2011, p. 93).

---

[35] Letícia Mulinari Gnoatton identificou na plataforma Google alguns do que se configuraria como dado pessoal no ambiente virtual: Utilizando como exemplo a plataforma Google, são considerados como dados pessoais, para fins de aplicação do Regulamento: i) nome completo; ii) informações pessoais inseridas quando do cadastro no Google (documento de identidade, naturalidade, sexo, endereço); iii) IP dos eletrônicos; iv) sites favoritados nos buscados do Google; e v) perfil comportamental e de consumo gerado pelo Google quando da utilização de seus serviços e aquisição de produtos (GNOATTON, 2021, p. 20).

[36] Nos termos originais: "personal data" means any information relating to an identified or identifiable individual (CONSELHO DA EUROPA, 1981).

Tais informações, cujo conteúdo representa alguma característica referente a uma pessoa, assim sendo, ganham maior relevância, tanto para o Estado, quanto para entes privados. Conforme o argumento apresentado por Doneda, "a importância da informação aumenta à medida que a tecnologia passa a fornecer meios para, a um custo razoável, torná-la útil" (DONEDA, 2020, p. 34). À medida que as informações pessoais se tornam mais estratégicas e relevantes para finalidades específicas, novas formas de se compreender o direito à privacidade e a sua extensão são desenvolvidas.

No domínio das atividades da Administração Pública, tendo em vista a necessidade de se obter um conhecimento preciso sobre a população, as informações pessoais se tornam um objeto de destaque, de modo que os Estados passem a demandá-las cada vez mais. Doneda argumenta que a maior disponibilidade de informações sobre os indivíduos sob a jurisdição de um Estado potencializa as formas de controle social e de influência do poder público sobre a população. Dessa forma, os estados passam a solicitar mais dados pessoais sobre temas mais diversos. Por consequência, também se tornam centrais as iniciativas de regulamentação da proteção de dados (DONEDA, 2020, p. 34).[37]

Houve, por parte dos Estados, em um primeiro momento, predominância na coleta e na gestão do uso de informações pessoais. No entanto, com o desenvolvimento tecnológico e com a difusão das técnicas de coleta e de processamento de dados no âmbito das instituições privadas, as referidas informações também se tornaram objeto de interesse do setor privado (DONEDA, 2020, p. 34).

Conforme já apresentado, a difusão das tecnologias atreladas ao uso de informações pessoais promoveu a ampliação no rol de possibilidades e aplicações atreladas a essas informações (DONEDA, 2020, p. 34). Ressalva-se que, com as rápidas modificações tecnológicas, bem como com o desenvolvimento de pesquisa e tecnologia neste campo, torna-se complexo inclusive delimitar quais são (ou serão) as aplicações possíveis no presente e no futuro.

Um ponto deve ser resguardado. Mencionou-se que à medida que as informações pessoais passaram a ser consideradas estratégicas, o Estado as demandou em maior volume e ampliou os mecanismos de controle sobre estas. Contudo, Doneda pondera que, para além desta demanda, o elemento central de transformação está no pressuposto de que, em razão do

[37] Menciona-se, nesse sentido, exemplo identificado por Doneda: na década de 1960, o departamento do Censo dos Estados Unidos passou a colher dados dos cidadãos norte-americanos sobre suas habitações privadas e sobre a história pessoal dos próprios ocupantes. Mais tarde, na década seguinte, cresceu a "curiosidade" desse órgão, que passou a exigir que os cidadãos que tivessem rompido seu matrimônio esclarecessem quais foram os motivos (DONEDA, 2020, p. 34).

desenvolvimento tecnológico, tornou-se possível obter e gerir grandes quantidades de informações. Dessa forma, foi atribuída uma utilidade real a este conteúdo (DONEDA, 2020, p. 35).

A maior relevância atribuída às informações pessoais, associada a crescente presença do Estado e das instituições privadas em atividades de coleta, de armazenamento e de uso de dados, contribui para que sejam desenvolvidos novos contornos ao direito à privacidade.

De acordo com Doneda:

> Assim, no momento que ruía o mito que relacionava aprioristicamente o progresso tecnológico com o bem-estar, abriu-se o leque de situações não patrimoniais sobre as quais a tecnologia poderia ter fortes implicações, causando, primeiramente, insegurança. Quanto aos problemas relacionados à privacidade – inicialmente associados a superestruturas obscuras como a do big brother de Orwell –, eles foram de início interpretados como uma ameaça: alarmes, mais ou menos fatídicos e sensacionalistas, foram correntes na literatura, jurídica ou não, que examina o problema das informações pessoais. Notícias sobre "o fim da privacidade" ou sobre a formação de uma "sociedade de dossiers" chamaram atenção para novos problemas e situações, porém por vezes vinham acompanhadas de uma tendência para o fantástico, chegando a sobrevalorizar o papel da tecnologia em um mundo no qual o arsenal de controles democráticos ainda não fora exaurido (DONEDA, 2020, p. 36).

Nesse contexto, há uma transformação na forma de se compreender o direito à privacidade. Stefano Rodotà propõe se tratar de interpretação que identifica a privacidade em um paradigma envolvendo o indivíduo, as informações de interesse, a circulação destas e os mecanismos de controle destes que se impõem na sociedade. Extrapola-se, destarte, o regime inicialmente aduzido, na qual a essência da privacidade estava restrita a uma perspectiva individualizada, lastreada no indivíduo e em seus "segredos" pessoais (RODOTÀ, 1995, p. 102).[38]

O direito à proteção de dados, a partir da perspectiva da privacidade, insere-se como norma com a finalidade de propiciar aos indivíduos as condições necessárias para o estabelecimento de uma esfera privada própria. A tutela da privacidade, portanto, passa a ser um elemento central para a própria expressão pessoal dos indivíduos (DONEDA, 2020, p. 39).[39] Desta feita:

---

[38] Nesse sentido, acrescenta-se a contribuição de Doneda na identificação de diferentes graus de manifestação da privacidade: a esfera da intimidade ou do segredo; a esfera privada e, em torno delas, a esfera pessoal, que abrangeria a vida pública (HUBMANN *apud* DONEDA, 2020, p. 79). Sobre outro prismo, fazendo referência ao já mencionado artigo de Warren e Brandeis, esta perspectiva da privacidade trazia tendências individualistas, próprias do período, e era compreendida como um direito negativo (LUGATI; ALMEIDA, 2020, p. 4)

[39] Sobre a relevância que assume o direito à privacidade em um contexto de crescente relevância das informações pessoais para agentes públicos e privados, ressalta-se a constatação de Doneda: A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento indutor da autonomia, da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Nesse papel, ela é pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos (DONEDA, 2020, p. 93). E acrescenta: A privacidade assume, então, um caráter relacional, que deve determinar

> [...] a proteção da privacidade na sociedade da informação, a partir da proteção de dados pessoais, avança sobre terrenos outrora improponíveis e nos induz a pensá-la como um elemento que, mais do que garantir o isolamento ou a tranquilidade, serve a proporcionar ao indivíduo os meios necessários à construção e consolidação de uma esfera privada própria, dentro de um paradigma de vida em relação e sob o signo da solidariedade – isto é, de forma que a tutela da privacidade cumpra um papel positivo para o potencial de comunicação e relacionamentos do indivíduo (DONEDA, 2020, p. 39).

De acordo com Kriangsak Kittichaisaree, há diferença sútil entre o direito à privacidade e o direito à proteção de dados pessoais. Enquanto o primeiro tem como objetivo a proteção da esfera privada dos indivíduos contra interferências estatais, o segundo tem a finalidade de regulamentar o uso de dados pessoais de determinado sujeito por parte de agentes públicos ou privados distintos do titular (KITTICHAISAREE, 2017, p. 59).

De maneira semelhante, Alexandra Maria Rodrigues Araújo concorda com a definição de que o direito à proteção de dados pessoais oferece tutela aos indivíduos "contra o uso indevido das Tecnologias da Informação no tratamento das informações pessoais que lhes digam respeito". Para a autora, o direito à proteção de dados pessoais pode tanto ser mais amplo quanto mais restrito do que o direito à privacidade. Por um lado, pode ser mais abrangente na medida em que é aplicável às informações pessoais de um indivíduo que não se restringem ao conteúdo de sua vida privada. Por outro, pode estar mais restrito, por critérios de forma, uma vez que se aplica apenas aos dados pessoais total ou parcialmente automatizados (RODRIGUES ARAÚJO, 2017, p. 208).

Em um contexto de profunda digitalização das atividades humanas, considerando também a relevância das informações pessoais nas atividades públicas, novas formas de controle e de vigilância são desenvolvidas. Para além da vigilância física e psicológica, a vigilância de dados pessoais passa a ser verificada como um novo elemento nas relações entre as instituições públicas e a população. Nestas relações, não se deve desconsiderar a existência de práticas abusivas ligadas ao uso de dados e informações pessoais (DONEDA, 2020, p. 40).[40]

---

o nível de relação da própria personalidade com as outras pessoas e com o mundo exterior – pela qual a pessoa determina sua inserção e de exposição; esse processo tem como resultado o fortalecimento de uma esfera privada do indivíduo – esfera que não é a de Hubman, mas uma que torne possível a construção da individualidade e o livre desenvolvimento da personalidade sem a pressão de mecanismos de controle social (DONEDA, 2020, p. 96).

[40] Burt destaca alguns exemplos de subversão da privacidade. O autor menciona situações que levam em consideração práticas corriqueiras dos indivíduos, como caminhar, escrever ou mesmo de possuir um *smartphone*. Relatório da Associated Press de 2018 alegou o uso, por parte do governo chinês, de análise de dados para identificar indivíduos com base na forma como eles moviam seus corpos para caminhar. Em relação a escrita, pesquisadores observaram que, baseando-se em uma quantidade suficiente de exemplos de escrita, a autoria de um texto poderia ser identificada a partir de aplicações de dados. Por fim, no que tange os

Paul Timmers afirma que, ao mesmo tempo em que as tecnologias da informação e da comunicação viabilizam maior controle das atividades governamentais, também se verifica o maior controle dos indivíduos por parte do Estado por meio delas (TIMMERS, 2020, p. 126). O direito à privacidade, destacado como um direito fundamental, deve implicar também na proteção jurídica dos dados pessoais. Diante das novas possibilidades e da crescente relevância dos dados e informações pessoais, a partir do direito à privacidade, verificou-se o direito à proteção de dados pessoais (DONEDA, 2020, p. 39-41).

Segundo José Adércio Leite Sampaio:

> [...] o homem tem um direito a controlar informação sobre ele mesmo, decidindo quando, como, em que extensão e para que finalidade tais informações serão conhecidas pelos outros. Em conceito envolve uma "senhoria" sobre todo o processo informativo, desde a sua obtenção por outros até seu uso ulterior. Diz-se assim que o direito à intimidade concede um poder ao indivíduo para controlar a circulação de informações a seu respeito. (SAMPAIO, 1998, p. 368-369).

A proteção das informações armazenadas passa a incluir, para além do direito de manter em segredo os fatos pessoais, também a capacidade de os indivíduos conhecerem quais informações sobre si estão armazenadas e sendo utilizadas. De igual maneira, torna-se relevante que os indivíduos tenham o direito de manter o conteúdo das informações armazenadas atualizado e verdadeiro (SMITH, 1979, p. 11).

Retomando a contribuição de Burt, verifica-se perspectiva que merece atenção. Para o autor, a privacidade – segundo os parâmetros apresentados – estaria "morta", uma vez que o imenso volume de dados produzidos diariamente e os novos usos proporcionados pelo desenvolvimento da técnica permitem a identificação dos indivíduos e de detalhes cada vez mais precisos de sua personalidade e de seus comportamentos (BURT, 2020, p. 3-6).

Por essa razão, é relevante reforçar, nesta pesquisa, o papel do direito à proteção de dados enquanto direito fundamental e inexoravelmente conectado com o direito à privacidade. Passa-se a abordar, no próximo item, os fundamentos do direito à proteção de dados como um direito humano.

2.1.3 O direito à proteção de dados enquanto direito humano

A quantidade massiva de dados utilizados e armazenados por instituições públicas e privadas contendo conteúdos sobre aspectos diversos, incluindo da vida pessoal dos indivíduos, e com múltiplas finalidades, faz com que seja necessária a existência de

---

smartphones, os dados coletados em razão do fato de mantê-los ligados permitiu a identificação pessoal de indivíduos e de seus padrões de vida (BURT, 2020, p. 4-5).

mecanismos no ordenamento jurídico que garanta a proteção de dados pessoais enquanto direito fundamental.

Conforme já destacado nesse capítulo, não é possível prever todos os avanços tecnológicos futuros e suas aplicações. O direito, por sua vez, não pode desconsiderar os impactos da tecnologia na vida humana em razão da imprevisibilidade destes (DONEDA, 2020, p. 46-47). Assim sendo, "a evolução das ciências e das técnicas não é indiferente ao direito" (EDELMAN *apud* DONEDA, 2020, p. 47). Este aspecto reforça a necessidade de adaptação – ou de extensão – da percepção tradicional de privacidade diante dos desafios impostos pelos novos usos atribuídos às informações pessoais.

Segundo Norberto Bobbio, o rol do que se considera (ou que se considerava) como direitos humanos se modificou e continua se modificando ao longo da história. As novas demandas que surgem ao decorrer do tempo, bem como as novas possibilidades produzidas pelas transformações na tecnologia condicionam este processo de modificação dos direitos humanos (BOBBIO, 2004, p. 13).[41]

Mesmo os direitos nominalmente considerados como fundamentais pelas constituições civis apresentam exceções em sua aplicação. Bobbio propõe que "o importante não é fundamentar os direitos do homem, mas protegê-los" (BOBBIO, 2004, p. 21). Nesse sentido, para além da positivação de determinada norma jurídica em defesa de um direito humano, é necessário que sejam construídas medidas "imaginadas e imagináveis" para garantir a efetiva proteção dos direitos a serem tutelados (BOBBIO, 2004, p. 14-21).

Para Bobbio:

> [...] quando falamos de proteção jurídica e queremos distingui-la de outras formas de controle social, pensamos na proteção que tem o cidadão, quando a tem no interior do Estado, ou seja, numa proteção que é fundada *na vis directiva* e da *vis coactiva* quanto à eficácia, é um problema complexo, que não pode ser abordado aqui. Limito-me à seguinte observação: para que a *vis directiva* alcance seu próprio fim, são necessárias, em geral, uma ou outra destas duas condições, melhor sendo quando as duas ocorrem em conjunto: a) o que a exerce deve ter muita autoridade, ou seja, deve incutir, se não temor reverencial, pelo menos respeito; b) aquele sobre o qual ela se exerce deve ser muito razoável, ou seja, deve ter uma disposição genérica a considerar como válidos não só os argumentos da força, mas também os da razão (BOBBIO, 2004, p. 22).[42]

[41] A título de exemplo, Bobbio destaca: Direitos que foram declarados absolutos no final do século XVIII, como a propriedade *sacre et inviolable*, foram submetidos a radicais limitações nas declarações contemporâneas; direitos que as declarações do século XVIII nem sequer mencionavam, como os direitos sociais, são agora proclamados com grande ostentação nas recentes declarações [...] O que parece fundamental numa época histórica e numa determinada civilização não é fundamental em outras épocas e em outras culturas (BOBBIO, 2004, p. 13).

[42] A efetiva proteção dos direitos humanos, na maneira como aduzida por Bobbio, inclui pressupostos na dimensão interna dos Estados e no campo internacional. A proteção, em cada um dos domínios mencionados, possuis características e condicionantes próprias. Nos termos do autor: Mesmo partindo-se dessa distinção, resulta claro que existe uma diferença entre a proteção jurídica em sentido estrito e as garantias internacionais: a

O direito à proteção de dados pessoais está inserido em um contexto de sensíveis transformações sociais motivadas pelo desenvolvimento tecnológico. A regulamentação deste nos ordenamentos jurídicos, dessa forma, deve estar atenta aos desafios produzidos pelos riscos contemporâneos.

2.1.3.1 O reconhecimento da proteção de dados como direito humano no âmbito da União Europeia.

Uma vez identificada a importância da proteção de dados enquanto direito humano, cumpre destacar a contribuição do sistema europeu, haja vista o interesse desta pesquisa em investigar a cooperação internacional em matéria penal entre o Brasil e os países da União Europeia. A nível de integração regional, o continente europeu desenvolveu as primeiras medidas destinadas a estabelecer um sistema de proteção de dados pessoais na década de 1980.

A Convenção nº 108 do Conselho da Europa, denominada Convenção de Estrasburgo – "Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal" –, é considerada como um dos principais documentos a considerar a proteção de dados sob o prisma dos direitos humanos (DONEDA, 2011, p. 102). Conforme apresenta o Conselho da Europa, a Convenção é identificada como sendo o "primeiro instrumento internacional vinculante que protege o indivíduo contra os abusos que podem acompanhar a coleta e o processamento de dados pessoais e que procura regular no mesmo tempo o fluxo transfronteiriço de dados pessoais" (CONSELHO DA EUROPA, 1981)[43].

A Convenção foi fortemente influenciada pelas "Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais", publicadas em 1980 pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE). Inicialmente, as Diretrizes e a Convenção tinham como finalidade orientar os países relativamente à matéria,

---

primeira serve-se da forma de controle social que é o poder; as segundas são fundadas exclusivamente na influência. Tomemos a teoria de Felix Oppenheim, que distingue três formas de influência (a dissuasão, o desencorajamento e o condicionamento) e três formas de poder (a violência física, o impedimento legal e a ameaça de sanções graves). O controle dos organismos internacionais corresponde bastante bem às três formas de influência, mas estanca diante da primeira forma de poder. Contudo, é precisamente com a primeira forma de poder que começa aquele tipo de proteção a que estamos habituados, por uma longa tradição, a chamar de jurídica. Longe de mim a ideia de promover uma inútil questão de palavras: trata-se de saber, substantivamente, quais são as possíveis formas de controle social e, com base nessa tipologia, estabelecer quais são as empregadas e empregáveis atualmente pela comunidade internacional; e depois, distinguindo formas mais ou menos eficazes com relação ao fim, que é o de impedir ou reduzir ao mínimo os comportamentos desviantes, perguntar qual seria — com relação à tutela dos direitos do homem — o grau de eficácia das medidas atualmente aplicadas ou aplicáveis no plano internacional (BOBBIO, 2004, p. 23).

[43] Informação disponível no site da Convenção: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

sem possuir força vinculativa ou mecanismos coercitivos. Todavia, já representavam uma mudança na percepção dos atores internacionais envolvidos sobre necessidade de proteção de dados pessoais (GNOATTON, 2021, p. 24-25).[44]

Doneda evidencia, a partir de análise da Convenção nº 108 do Conselho da Europa e das Diretrizes da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), 5 princípios atinentes à proteção de dados: a) o princípio da publicidade, ou da transparência, segundo o qual deve ser publicizada a existência de um banco de dados contendo informações pessoais; b) o princípio da exatidão, o qual preceitua que os dados pessoais armazenados devem ser "fiéis à realidade"; c) o princípio da finalidade, que fundamenta a necessidade de que qualquer uso atribuído aos dados pessoais deva "obedecer à finalidade comunicada ao interessado antes da coleta de seus dados"; d) o princípio do livre acesso, que permite ao indivíduo o acesso aos bancos de dados que armazenam as suas informações pessoais; e e) o princípio da segurança física e lógica, que busca promover a proteção dos dados contra riscos de "extravio, destruição, modificação, transmissão ou acesso não autorizado" (DONEDA, 2011, p. 101).

Adiante, a Diretiva 95/46/CE da União Europeia, de 1995, também estabelece como objetivo que os "Estados-membros assegurarão, em conformidade com a presente directiva, a protecção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais" (UNIÃO EUROPEIA, 1995)[45].

A Diretiva 95/46/CE estimulou os Estados da União Europeia a estabelecerem normas domésticas com a finalidade de oferecer tutela adequada aos dados pessoais, levando em consideração os padrões estabelecidos pela Diretiva (GNOATTON, 2021, p. 27). Destaca-se, nesse sentido, a previsão constante no artigo 28 da Diretiva, a qual dispõe que os Estados-

---

[44] Reforça-se este ponto uma vez que todos os Estados-membros ratificaram a Convenção n.º 108 até 1999 (COLOMBO, 2015, p. 10-11).

[45] É relevante mencionar o acórdão Lindqvist, julgado pelo Tribunal de Justiça da União Europeia em 2003, e considerado um dos precedentes mais importantes sobre a temática de proteção de dados na internet (CALABRICH, 2019, p. 2-7). No caso, discutiu-se interpretação da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, tendo como situação fática a acusação de que Bodil Lindqvist teria violado a legislação sueca de proteção de dados em razão de publicação em seu site, na internet, informações pessoais de outras pessoas que com ela trabalhavam (UNIÃO EUROPEIA, 2003, p. 31). As informações publicadas por Lindqvist incluíam "nome, atividades exercidas, hobbies, situação familiar e número de telefone" (CALABRICH, 2019, p. 2). Nos termos do julgamento, o Tribunal de Justiça da União Europeia reconheceu que "As medidas adoptadas pelos Estados-Membros para assegurar a protecção dos dados de carácter pessoal devem estar em conformidade quer com as disposições da Directiva 95/46 quer com o seu objectivo de manter um equilíbrio entre a livre circulação dos dados de carácter pessoal e a protecção da vida privada. Em contrapartida, nada se opõe a que um Estados-Membro alargue o alcance da legislação nacional que procede à transposição da Directiva 95/46 a domínios não incluídos no seu âmbito de aplicação, desde que nenhuma outra disposição do direito comunitário a tal obste" (UNIÃO EUROPEIA, 2003, p. 39).

membros deverão estabelecer uma ou mais autoridades públicas com a responsabilidade de resguardar a aplicação da Diretiva a nível interno, as quais possuirão independência em suas funções (UNIÃO EUROPEIA, 1995).[46]

De acordo com Orla Lynskey, a Diretiva 95/46/CE foi um importante instrumento ao estabelecer propriamente um regime de proteção aos dados pessoais. No entanto, diante das transformações tecnológicas e sociais, a Diretiva passou a sofrer críticas sob a fundamento de supostamente estar ultrapassada (LYNSKEY, 2015, p. 4). Segundo a autora:

> Essa mudança sísmica no cenário desde 1995 apresenta desafios fundamentais para a regulamentação da proteção de dados. A diretiva estabelece uma estrutura de obrigações e de salvaguardas que devem ser respeitadas por entidades envolvidas no processamento de dados pessoais, bem como estabelece direitos a serem exercidos pelos indivíduos. Essa resposta regulatória ao fenômeno de processamento de dados pessoais pode parecer antiquada à luz das mudanças tecnológicas e sociais acima aludidas (LYNSKEY, 2015, p. 4).[47]

Destaca-se, ademais, o artigo 8º da Carta dos Direitos Fundamentais da União Europeia, que garante o direito à proteção de dados pessoais a todas as pessoas. Acordou-se em prol da necessidade de tratamento leal dos dados pessoais, voltado apenas para finalidades específicas e mediante o consentimento do indivíduo interessado (UNIÃO EUROPEIA, 2000).[48] O ímpeto da União Europeia de construir um sistema de proteção de dados pessoais também está presente em suas normativas estruturantes. O artigo 16 do Tratado sobre o Funcionamento da União Europeia prevê que "todas as pessoas têm direito à proteção de dados de caráter pessoal que lhes digam respeito" (UNIÃO EUROPEIA, 2012).[49]

Segundo Manuel David Masseno, a presença do direito à proteção de dados pessoais na Carta dos Direitos Fundamentais e no Tratado sobre o Funcionamento da União Europeia significam a constitucionalização da tutela jurídica do tema no regime da integração europeia. Em 2018, ao entrar em vigor, o Regulamento 2016/679 do Parlamento Europeu e do Conselho, denominado *General Data Protection Regulation* (GDPR), em substituição à

---

[46] Artigo 28º, Autoridade de controlo. 1. Cada Estado-membro estabelecerá que uma ou mais autoridades públicas serão responsáveis pela fiscalização da aplicação no seu território das disposições adoptadas pelos Estados-membros nos termos da presente directiva. Essas autoridades exercerão com total independência as funções que lhes forem atribuídas (UNIÃO EUROPEIA, 1995).

[47] Tradução livre. Na versão original: This seismic shift in landscape since 1995 poses fundamental challenges for data protection regulation. The Directive sets out a framework of obligations and safeguards which must be respected by entities engaging in personal data processing, as well as rights to be exercised by individuals. Such a regulatory response to the personal data processing phenomenon may seem antiquated (LYNSKEY, 2015, p. 4).

[48] Segundo Doneda, a Carta contempla duas formas de se compreender o direito à privacidade. Em primeiro lugar, no artigo 7º, a partir do prisma de tutela do indivíduo contra "intromissões exteriores"; na sequência, com vistas à proteção dos dados pessoais em suas diversas aplicações (DONEDA, 2020, p. 41).

[49] Em comunicação da Comissão Europeia ao Parlamento Europeu e ao Conselho, o ex-presidente da Comissão Jean-Claude Juncker declarou: [s]er europeu significa ter o direito a que os nossos dados pessoais sejam protegidos por legislação europeia eficaz. [...] Porque, na Europa, as questões da privacidade são importantes. Trata-se de uma questão de dignidade humana (COMISSÃO EUROPEIA, 2016).

Diretiva 95/46/CE, contribuiu ainda mais para consolidar o sistema de proteção de dados pessoais no âmbito da União Europeia (MASSENO, 2020, p. 127). Nesse sentido:

> O Regulamento Geral de Proteção de Dados se propôs a atualizar a legislação europeia sobre o assunto, a consolidar conceitos e a unificar a legislação entre os Estados-Membros, criando mecanismos mais efetivos para garantir o cumprimento de suas disposições, tanto internamente como em relação aos Estados terceiros e às organizações internacionais. Dessa forma, ainda que contenha conceitos e princípios similares aos dispostos na Diretiva 95/46/EC, os efeitos do Regulamento sobre a tutela dos dados pessoais são maiores (GNOATTON, 2021, p. 31).

O GDPR traz de regras sobre a proteção das pessoas "no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados" e reafirma o direito à proteção de dados pessoais como um fundamental aos indivíduos (UNIÃO EUROPEIA, 2016-A). O regulamento é aplicável ao tratamento de dados pessoais quando o indivíduo é identificado ou potencialmente identificável (MASSENO, 2020, p. 129-130)[50] e, em termos territoriais, ao tratamento "efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União" (UNIÃO EUROPEIA, 2016-A).[51]

O sistema de proteção de dados pessoais estabelecido pela União Europeia foi utilizado como fonte de inspiração – ou mesmo como base – para regimes protetivos em dezenas de Estados no Ocidente. A autora estimou que, de 39 Estados não europeus com regimes de proteção de dados analisados, 33 possuíam um sistema regulatório que seguia os "padrões europeus" (LYNSKEY, 2015, p. 41-44).

Anu Bradford, em análise da difusão dos "padrões europeus" na sociedade internacional, identificou que a relevância econômica da União Europeia gera a necessidade

---

[50] Sobre a aplicabilidade aos dados relativos a pessoas identificadas ou identificáveis, ressalta-se o Considerando 26 do GDPR: Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação (UNIÃO EUROPEIA, 2016-A).

[51] Sobre a aplicação territorial, William Long, Géraldine Scali, Francesca Blythe e Alan Raul assinalam: The GDPR only applies when the processing is carried out in the context of an establishment of the controller or processor in the EU, or, where the controller or processor does not have an establishment in the EU, but processes personal data in relation to the offering of goods or services to individuals in the EU; or the monitoring of the behaviour of individuals in the EU as far as their behaviour takes place within the EU (LONG; SCALI; BLYTHE; RAUL, 2019, p.).

de que companhias estrangeiras e Estados interessados em ampliar relações econômicas com os países da integração busquem se adequar aos parâmetros europeus. No mesmo sentido, a autora elenca como áreas globalmente afetadas pela difusão dos padrões europeus a saúde e a segurança de consumidores, a proteção do meio ambiente e a economia digital (BRADFORD, 2012, p. 5-32).

Observa-se, portanto, a relevância da contribuição do sistema europeu, a nível de integração regional, no reconhecimento do direito à proteção de dados como direito fundamental, bem como na promoção e na difusão do interesse de tutela dos dados pessoais. Adiante, no próximo item, passa-se a analisar a inserção do direito à proteção de dados na legislação brasileira.

2.1.3.2 O reconhecimento da proteção de dados como direito humano no ordenamento jurídico brasileiro.

No ordenamento jurídico brasileiro, a dignidade da pessoa humana é fundamento da República e a privacidade é um direito fundamental expresso no artigo 5º. A proteção da intimidade e da vida privada integram, dessa maneira, o rol constitucional de direitos fundamentais. O direito à proteção de dados, por sua vez, passou a ser incluído em diplomas normativos nacionais e internacionais. Menciona-se, preliminarmente, a referência à Constituição Federal Brasileira, a qual, a partir da Emenda Constitucional nº 115, de 2022, inseriu no artigo 5º o direito à proteção dos dados pessoais, inclusive nos meios digitais (BRASIL, 1988).

Doneda, em atenção aos dispositivos constitucionais de tutela da intimidade e da vida privada, destaca a importância de compreendê-los de maneira conjunta. Embora cada um desses termos possua um campo semântico próprio, a lente interpretativa deve considerá-los no contexto dos direitos fundamentais a serem protegidos (DONEDA, 2020, p. 80). Para o autor:

> A terminologia da Constituição brasileira deve, porém, ser lida em razão do contexto no qual se encontram os direitos fundamentais que visa proteger. Nesse prisma, consideramos não ser frutífero insistir em uma conceitualística que intensifique as conotações e diferenças dos dois termos. Cada um deles possui um campo semântico próprio: na "vida privada" identificamos um discurso sobre a distinção entre as coisas da vida pública e da vida privada, no estabelecimento de limites, numa lógica que também é de exclusão. Cada um deles possui um campo semântico próprio: na "vida privada" identificamos um discurso sobre a distinção entre as coisas da vida pública e da vida privada, no estabelecimento de limites, numa lógica que também é de exclusão. [...] O outro termo utilizado pelo constituinte, "intimidade", aparenta referir-se a eventos mais particulares e pessoais, a uma atmosfera de confiança. Evoca, mais do que outra coisa, o aspecto do direito à tranquilidade, do *right to be let alone*. Avaliar tal amplitude com a consistência necessária ao discurso jurídico,

> porém, não nos parece possível a partir da distinção linguística, senão por meio de artifícios retóricos. (DOENADA, 2020, p. 80).

A proteção da vida privada e da intimidade, portanto, deve ser compreendida de acordo com a finalidade de tutela dos direitos fundamentais dos indivíduos (DONEDA, 2020, p. 80-81). Ambos os institutos jurídicos se conectam como formas possíveis de se compreender a privacidade e, nesse sentido, para fins desta pesquisa, são percebidos como inerentes aos direitos humanos.

O marco central da proteção de dados no ordenamento jurídico brasileiro é a Lei Geral de Proteção de Dados Pessoais (LGPD), a Lei nº 13.709/2018. Antes desta, a temática da proteção de dados já era indiretamente tratada por outros diplomas legais, ainda que de modo esparso. Em primeiro lugar, de maneira indireta já é possível perceber a proteção de dados na Constituição Federal quando se observa as referências ao direito à liberdade de expressão (art. 5º, IX, CF), à informação (art. 5º, XIV, CF), à inviolabilidade da vida privada e intimidade (art. 5º, X, CF), bem como o habeas data e os direitos relacionados à intercepção das comunicações telefônicas, telegráficas ou de dados (art. 5º, LXXII, CF). Menciona-se, ademais, previsões constantes no Código de Defesa do Consumidor,[52] a Lei do Cadastro Positivo (Lei nº 12.414/2011)[53] e o Marco Civil da Internet.[54] Não havia, no entanto, legislação sistematizada que tratasse sobre o assunto até a contribuição da LGPD (LUGATI; ALMEIDA, 2020, p. 2-10).

Cumpre acentuar, adicionalmente, o instituto do *habeas data*. Trata-se de um mecanismo útil para a concretização do direito à proteção de dados. Por meio deste, o indivíduo é capaz de acessar e retificar seus dados pessoais em bancos de dados pertencentes a entidades governamentais ou de caráter público (DONEDA, 2011, P. 104).

Nos termos de Marcelo Crespo:

> Com efeito, uma lei de proteção de dados pessoais, em regra, constitui um marco regulatório que estabelece direitos para o cidadão sobre seus dados, independente de quem realize o tratamento deles. Esses direitos visam proteger o cidadão, disponibilizando ferramentas que o garantam exercer, efetivamente, o controle sobre os seus dados pessoais. O grande desafio, no entanto, trata-se em conciliar a

[52] A seção VI da referida lei versa sobre os Bancos de Dados e Cadastros de Consumidores e, em seu artigo 43, dispõe que: O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes (BRASIL, 1990).

[53] Há relevante avanço nesta lei no desenvolvimento da aplicação do princípio da autodeterminação informativa, em razão de tornar o consentimento necessário para a licitude do compartilhamento de dados (LUGATI; ALMEIDA, 2020, p. 11).

[54] O Marco Civil da Internet busca regular o uso da internet e dispõe sobre direitos e garantias dos indivíduos nas relações desempenhadas no espaço virtual (BIONI *apud* LUGATI; ALMEIDA, 2020, p. 11). Esta lei incluiu o indivíduo no processo de tratamento de dados, consolidando a relevância do consentimento (MALHEIROS *apud* LUGATI; ALMEIDA, 2020, p. 11).

> persecução dos objetivos consagrados em tais legislações, sem que se impeça a inovação (CRESPO, 2021, p. 19).

A LGPD é desenvolvida e promulgada no contexto em que outros países, a nível doméstico e à nível de integração internacional, também implementavam legislações específicas para a proteção de dados. Ressalta-se o exemplo da União Europeia, no qual o *General Data Protection Regulation* (GDPR), de 2016, é marco normativo referencial dentro de um processo em que já foram instituídos documentos precedentes como a Convenção n.º 108 e a Diretiva 95/46, ambas previamente mencionadas neste capítulo. A LGPD, portanto, insere o Brasil no rol de países com legislações amplas e sistemáticas sobre a proteção de dados pessoais (LUGATI; ALMEIDA, 2020, p. 2-3).[55]

Consta no artigo 1º da Lei 13.709/2018 disposição sobre o objeto do diploma legal. Refere-se ao "tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade", mencionando-se, adicionalmente, a proteção ao livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Conforme explica Crespo, a LGPD dispõe sobre aplicações tanto para a iniciativa privada quanto para o setor público. Em relação à dimensão privada, o pressuposto da legislação é não impedir a inovação tecnológica e o desenvolvimento econômico. Para o setor público, a regulamentação sistemática da proteção de dados pessoais busca "estabelecer um equilíbrio entre a proteção dos dados dos cidadãos e o tratamento desses dados para a elaboração e execução de políticas públicas" (CRESPO, 2021, p. 19).

É importante destacar, enquanto elementos basilares da LGPD brasileira, o consentimento e o princípio da autodeterminação informativa. Por meio deste último, e em consonância com a relevância do consentimento, o titular dos dados assume a direção do controle e da proteção de seus próprios dados (LUGATI; ALMEIDA, 2020, p. 3). O princípio da autodeterminação informativa, nesse sentido, pressupõe a participação do titular dos dados para além do mero consentimento no início do tratamento de dados, para que este

---

[55] Embora seja possível compreender a LGPD em um contexto de tutela do direito humano à proteção de dados, outras interpretações são possíveis sobre a temática. Menciona-se, por exemplo, a contribuição de José Luiz de Moura Faleiros Júnior: Em linhas conclusivas, pode-se anotar que o propósito da edição de uma legislação especificamente voltada para a proteção de dados pessoais, no que concerne ao papel do Poder Público para a estipulação de medidas de governança de dados, é fruto de uma materialização transversal que visa mitigar riscos regulatórios. A LGPD brasileira é o epítome de uma tendência há muito vislumbrada e que vem mobilizando o Estado, em todos os seus âmbitos, à edição de regramentos próprios e voltados às particularidades de suas esferas de atuação. Não por outra razão, a União editou o Decreto nº 9.203/2017 – analisado neste breve ensaio – bem antes da promulgação da própria LGPD e, avançando no tema, delineou sua política de governança de dados (Decretos nº 10.046 e 10.047 de 2019), ainda durante o período de *vacatio legis* da festejada norma (FALEIROS JÚNIOR, 2021, p. 133).

também tenha participação, com maior controle, sobre o tratamento as suas informações pessoais (DONEDA apud LUGATI; ALMEIDA, 2020, p. 23). O consentimento se insere no domínio do direito à proteção de dados na medida em que é por meio deste que o indivíduo manifesta sua "permissão, anuência, aprovação para determinada forma de tratamento de seus dados" (LUGATI; ALMEIDA, 2020, p. 15).

O artigo 5º da LGPD define o consentimento como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018). Embora o consentimento possa ser identificado como um dos fundamentos do sistema brasileiro de proteção de dados, a LGPD prevê possibilidades de flexibilização, por meio de determinadas hipóteses de dispensa. Neste caso, a legislação busca equilibrar os direitos e a vontade do titular dos dados com os desígnios daqueles que efetivamente controlam os dados (LUGATI; ALMEIDA, 2020, p. 21).[56]

Crespo compreende a LGPD como uma lei principiológica, de modo que não estabelece de maneira pormenorizada os procedimentos e atividades que as instituições devem executar para atingir a conformidade. Dessa forma, a legislação não indica expressamente (e detalhadamente) quais são as "ferramentas técnicas adequadas" que as instituições devem aplicar na proteção de dados (CRESPO, 2021, p. 17-19).

Cumpre assinalar que a LGPD dispõe sobre os cenários não incluídos em seu alcance normativo, no que diz respeito ao tratamento de dados pessoais. São eles: o tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos; o tratamento de dados pessoais realizado para fins exclusivamente: jornalísticos, artísticos e acadêmicos; o tratamento de dados pessoais realizado para fins exclusivos de: segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (BRASIL, 2018).

---

[56] As hipóteses em que o consentimento não é necessário para o tratamento de dados pessoais previstas no artigo 7º da LGDP são as seguintes: II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

A última hipótese apresentada exclui a aplicação dos termos da LGDP no contexto de investigação e repressão de infrações penais. Considerando que esta pesquisa pretende abordar especificamente o direito à proteção de dados no contexto do Direito Penal Transnacional, a compreensão desta lei poderia ser considerada subsidiária. Contuso, com o objetivo de compreender os fundamentos do direito à proteção de dados quando aplicada à cooperação internacional em matéria penal, especificamente à Convenção de Budapeste, a LGPD não pode ser desconsiderada.

As inovações normativas no ordenamento jurídico brasileiro são acompanhadas de manifestações do Supremo Tribunal Federal. A partir da Ação Direta de Inconstitucionalidade 6.387/DF e da Arguição de Descumprimento de Preceito Fundamental 722/DF, pretende-se melhor compreender a inserção do direito à proteção de dados pessoais no sistema jurídico brasileiro.

O acórdão da Ação Direta de Inconstitucionalidade 6.387/DF, que referenda Medida Cautelar da Relatora Ministra Rosa Weber, é um precedente importante para a temática de proteção de dados pessoais no ordenamento jurídico brasileiro (BRASIL, 2020-A). Por meio da Medida Cautelar, suspendeu-se a eficácia do ato normativo que exigia o compartilhamento de dados pessoais armazenados pelas companhias telefônicas para uso do Instituto Brasileiro de Geografia e Estatística (IBGE), no contexto da pandemia de COVID-19 (TOSCHI; LOPES, 2020, p. 104-105).

No acórdão, reafirmou-se o direito à privacidade e à autodeterminação informática, ambos constantes na Lei Geral de Proteção de Dados (ainda que o julgamento seja anterior à entrada em vigor da LGPD), como fundamentos da proteção de dados pessoais. Uma vez que se tratem dados com capacidade de identificar uma pessoa natural, o tratamento e a manipulação destes estão abarcados pela tutela constitucional à proteção de dados. Nesse sentido, certas aplicações aos dados como o compartilhamento com entidade pública devem levar em consideração, enquanto princípio orientador, a garantia da proteção e da segurança desses dados (BRASIL, 2020-A, p. 2).[57] Tal precedente, assim sendo, reconheceu à proteção de dados pessoais como direito fundamental autônomo, "extraído a partir de leitura

[57] Em seu voto, a Ministra Rosa Weber argumentou: Assim como o exigir que automóveis sejam providos de freios, airbags e espelhos retrovisores não significa criar obstáculos para a indústria automobilística, o exigir que normas que envolvam direitos fundamentais e da personalidade observem requisitos mínimos de adequação constitucional tampouco pode ser lido como embaraço à atividade estatal (BRASIL, 2020-A, p. 17). A Ministra complementa, trazendo a referência de Clarissa Long: a história nos ensina que uma vez estabelecidos, é improvável que poderes governamentais de vigilância e coleta de dados de seus cidadãos e residentes retrocedam voluntariamente. E a história também tem nos ensinado que uma vez que dados são coletados para um propósito, é muito difícil evitar que sejam usados para fins outros não relacionados (LONG *apud* BRASIL, 2020-A, p. 18-19).

sistemática do texto constitucional brasileiro" (MENDES; JÚNIOR; FONSECA, 2021, p. 116), mesmo anteriormente à Emenda Constitucional n.º 115 de 2022.

Segundo Aline Seabra Toschi e Herbert Emílio Araújo Lopes:

> O julgamento da ADI n. 6.387 foi uma decisão de importância ímpar para a questão do tratamento de dados pessoais no Brasil, principalmente pelo fato de ter ocorrido anteriormente à entrada em vigor da LGPD. Além disso, tornou-se paradigmática ao reconhecer que a Constituição Federal de 1988 assegura aos brasileiros o direito à autodeterminação informativa, conforme destaca a ministra: Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. (TOSCHI; LOPES, 2020, p. 107).

A decisão proferida no referido acórdão considera que, na medida em que os dados capazes de identificar um indivíduo podem ser utilizados para a formação de perfis informacionais valiosos para entidades públicas e privadas, estes devem ser destinatários da devida proteção constitucional. Ademais, observa-se haver opção por interpretação ampla da tutela constitucional existente quando da decisão, uma vez que tal direito fundamental pode ser aplicado a diversas situações envolvendo a coleta, o processamento ou a transmissão de dados pessoais (MENDES; JÚNIOR; FONSECA, 2021, p. 121).[58]

No acórdão relativo à Arguição de Descumprimento de Preceito Fundamental 722/DF, concernente à suposto relatório do Ministério da Justiça constando a compilação de dados pessoais de determinados indivíduos, o Supremo Tribunal Federal, em consonância com o voto da Relatora Ministra Cármen Lúcia, decide por suspender:

> Todo e qualquer ato do Ministério da Justiça e Segurança Pública de produção ou compartilhamento de informações sobre a vida pessoal, as escolhas pessoais e políticas, as práticas cívicas de cidadãos, servidores públicos federais, estaduais e municipais identificados como integrantes de movimento político antifascista, professores universitários e quaisquer outros que, atuando nos limites da legalidade, exerçam seus direitos de livremente expressar-se, reunir-se e associar-se [...] (BRASIL, 2020-B, p. 1-2).

Os dois acórdãos proferidos pelo Supremo Tribunal Federal em 2020 reafirmam a necessidade de observância do direito o à proteção de dados pessoais por parte das entidades do setor público. Ao direito à intimidade e à vida privada, nesse sentido, é atribuída maior

[58] Ressalta-se, ademais, a relevância conferida por Laura Schertel Mendes, Otavio Luiz Rodrigues Júnior e Gabriel Campos Soares da Fonseca: O significado histórico da decisão do STF pode ser equiparado ao clássico julgamento do Tribunal Constitucional Federal alemão, em 1983, relativamente à Lei do Recenseamento. Ao fazer referência ao julgado, o STF expressamente mencionou o conceito de autodeterminação informativa, já positivado na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados), a fim de ressaltar o necessário protagonismo exercido pelo cidadão no controle do que é feito com seus dados. Assim, pôs-se em destaque a existência de finalidades legítimas para seu processamento, bem como da necessidade de implementação de medidas de segurança para tanto (MENDES; JÚNIOR; FONSECA, 2021, p. 124).

relevância no que tange o tratamento de dados pessoais sensíveis (TOSCHI; LOPES, 2020, p. 107).

Conclui-se, desta feita, que o direito à proteção de dados pessoais se consolidou formalmente como direito fundamental, a princípio a partir de leis esparsas e pela atuação da jurisprudência pátria, e, finalmente, com presença expressa na Constituição Federal. Trata-se de aspecto central para a concretização do direito à privacidade e para a livre expressão da personalidade na sociedade contemporânea.

2.2 A INTERVENÇÃO NA PROTEÇÃO DE DADOS PESSOAIS NO CONTEXTO DA PERSECUÇÃO PENAL

Analisou-se ao longo do primeiro item deste capítulo que o direito à proteção de dados se desenvolveu em razão das inovações tecnológicas que impunham uma nova forma de se compreender o direito à privacidade. Trata-se de contexto em que o armazenamento, o uso e compartilhamento dos dados por parte das entidades públicas e privadas se tornou mais rápido e menos custoso, de modo que a eles foram conferidas novas atribuições estratégicas.

Conforme já se abordou no último tópico, o desenvolvimento das tecnologias de informação e de comunicação foi capaz de ampliar e de aprofundar os mecanismos de vigilância dos cidadãos por parte de um Estado. Cabe mencionar, enquanto exemplo, as possibilidades de interceptação de dados pessoais, os quais assumiram progressivamente maior relevância estratégica nos últimos anos (PESSOA, 2020, p. 27).

O uso cada vez mais frequente das tecnologias eletrônicas de informação e de comunicação propiciou a origem de um cenário com possibilidades amplas – e, por vezes, imprevisíveis – de usos e valoração de dados. Esta conjuntura produz, segundo Eduardo Viana, Lucas Montenegro e Orlandino Gleizer, um "sentimento difusamente ameaçador de vigilância, que perturba um dos pressupostos fundamentais para o livre desenvolvimento humano: a sensação de inexistência de espaços livres de observação" (VIANA; MONTENEGRO; GLEIZER, 2020, p. 3).

Para João Pedro Seefeldt Pessoa, desde o século XVIII, a vigilância tem se tornado uma das principais formas de efetivação do exercício do poder por parte de uma instituição. Na segunda metade do século XX, diante das já mencionadas transformações tecnológicas, os mecanismos de vigilância e de controle social também se ampliaram. Para fazer referência a uma utilidade específica, ao longo da 2ª Guerra Mundial, agências estatais e outras instituições capacitadas tiveram importante papel na interceptação e na análise de informações

trocadas entre as partes envolvidas no conflito. Trata-se do fenômeno da espionagem (PESSOA, 2020, p. 29-30).[59]

As constatações de Pessoa reafirmam a instrumentalização, por parte das instituições de Estado, de mecanismos de armazenamento e de uso de dados com a finalidade de ampliar a rede de inteligência. Há, para tanto, um discurso que busca legitimar esta ação estatal. Nos termos do autor, a principal justificativa para legitimar o incremento de zonas e de atividades de monitoramento de informações dos indivíduos é o combate ao terrorismo (PESSOA, 2020, p. 31). O fundamento da legitimidade do exercício de vigilância, portanto, está na garantia de uma suposta segurança à sociedade.

Destaca-se a caracterização desenvolvida por Pessoa:

> Diante desse cenário, depara-se com a obtenção em larga escala de uma quantidade exorbitante de dados, a qual possui especial importância, uma vez que, a partir da coleta, do armazenamento, da manipulação e da transferência de tais dados, é possível criar padrões e vigiar indivíduos e massas (PESSOA, 2020, p. 38).

Sob a justificativa de garantir a segurança social, impõe-se medidas de vigilância que fazem uso de dados pessoais em prol do dito interesse público (PESSOA, 2020, p. 40). Trata-se, de forma clara, de assunto ainda aberto a amplos debates sobre a licitude da coleta e do tratamento de dados pessoais por parte de instituições públicas.

Pessoa menciona o recente caso "*Big Brother Watch and Others v. The United Kingdom (applications nº. 58170/13, 62322/14 and 24960/15)*", julgado pela Corte Europeia de Direitos Humanos em relação a temática da vigilância e da ingerência de autoridades públicas sob a justificativa de "segurança nacional" (PESSOA, 2020, p. 40-41). A decisão da Corte entendeu que programas de vigilância executados pelo Estado no desempenho de suas funções podem violar direitos fundamentais dos indivíduos, entre outros motivos, em razão da "falta de garantias adicionais a setores específicos que podem ser objeto de investigação e da falta de publicidade relacionada aos programas, nos seus limites, já que suas existências foram relevadas sob polêmicas internacionais" (PESSOA, 2020, p. 41).

De maneira semelhante, em análise da jurisprudência da Corte Europeia de Direitos Humanos, Kriangsak Kittichaisaree identificou que a coleta e o armazenamento sistemáticos

[59] Pessoa destaca, ademais, a rede de troca de informações formalizada entre Estados Unidos da América e reino Unido: Então, o marco de cooperação de inteligência secreta UKUSA, liderado substancialmente pela Agência de Segurança Nacional dos Estados Unidos (*National Security Agency*, em inglês), entidade também mantida em sigilo por décadas, fez criar um sistema de vigilância global, denominado *Echelon*, com capacidade para captar e analisar, virtualmente, informações advindas de chamadas telefônicas e mensagens de fax, telex, e-mail e outros dispositivos, enviadas de qualquer lugar do mundo [...]. Conforme uma investigação realizada pelo Parlamento Europeu, divulgado no Relatório de 11 de julho de 2011, no âmbito do sistema *Echelon*, dados brutos de comunicação captados pelas agências de inteligência, tanto de voz, telex, fax e internet, puderam ser interceptados, registrados, analisados, trocados, vendidos e classificados por meio de filtros, permitindo a elaboração fácil de perfis e outros relatórios pelas partes interessadas (PESSOA, 2020, p. 30).

de informações pessoais por instituições públicas pode configurar uma invasão à vida privada dos indivíduos. Para além disso, a interceptação de comunicações privadas por parte de autoridades públicas com a finalidade de estruturar um perfil individual igualmente pode configurar uma violação ao direito à privacidade (KITTICHAISAREE, 2017, p. 54).

No contexto em que um enorme volume de dados é coletado e processado por entidades privadas, ao mesmo tempo em que o fluxo de informações alcança escala global, as autoridades policiais e de persecução penal se interessam cada vez mais em acessar informações produzidas e armazenadas por grandes companhias de tecnologia (CARRERA; STEFAN, 2020, p. 3). O valor dos dados para fins de investigação criminal tem se torna progressivamente mais estratégico às instituições públicas.

Reforça-se o argumento apresentado até este ponto, em combinação com o item anterior. Conforme argumenta Vladimir Aras, a proteção de dados está ligada aos direitos humanos, entre eles o direito à privacidade – e, por extensão, a não ser conhecido e a poder ser esquecido. Nesse sentido, oferecer garantias adequadas à proteção de dados pessoais também implica na prevenção de práticas abusivas empreendidas pelas entidades que coletam e armazenam dados. Cita-se, por exemplo, perseguições motivadas por questões religiosas, políticas, de origem nacional ou de orientação sexual – todas motivadas por informações potencialmente reveláveis por dados pessoais sensíveis (ARAS, 2020, p. 22).

Assim como mencionado no capítulo anterior, a LGPD não contempla em seu texto as situações de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (BRASIL, 2018). No entanto, uma análise abrangente do ordenamento jurídico brasileiro identifica que o direito à privacidade e suas aplicações à proteção de dados pessoais não estavam excluídos do rol de direitos fundamentais (ARAS, 2020, p. 23-23). Nesse sentido:

> Com a entrada em vigor da LGPD em 2020, o Brasil adotou sua primeira lei geral de proteção de dados. No entanto, já havia um razoável nível de proteção aos direitos de privacidade em nossa jurisdição, a começar pelo art. 5º, X, da Constituição, que considera invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando-se o direito à indenização pelo dano material ou moral decorrente de sua violação. O inciso XII do mesmo artigo também garante a inviolabilidade do sigilo postal, de dados e das comunicações telefônica salvo por ordem judicial para fins de investigação criminal ou instrução processual penal, na forma prevista na Lei n. 9.296/1996 (ARAS, 2020, p. 22-23).

Conforme visto, a aplicação de mecanismos de "coleta, guarda, processamento, utilização e disseminação ou transferência de dados pessoais", no âmbito penal, pode produzir impactos ao titular de dados, seja ele o autor da infração (investigado) ou a vítima. Não

obstante, informações pessoais de testemunhas, peritos e de terceiros igualmente podem ser submetidas ao controle estatal (ARAS, 2020, p. 24).

Não se trata de assunto novo ou amplamente negligenciado pelo ordenamento jurídico brasileiro. Aras exemplifica retomando legislações que produzem impactos nas atividades de coleta, armazenamento, uso de informações pessoais no curso da persecução penal: Lei de Interceptação Telefônica (Lei n. 9.296/1996); Lei da Identificação Criminal (Lei n. 12.037/2009); artigos 17-B e 17-E da Lei de Lavagem de Dinheiro (Lei n. 9.613/1998); artigos 15 e 17 da Lei do Crime Organizado (Lei n. 12.850/2013); artigos 13-A e 13-B do Código de Processo Penal (ARAS, 2020, p. 24).

Segundo Mario Viola, Leonardo Heringer e Celina Carvalho, em relatório do Instituto de Tecnologia e Sociedade do Rio, "a investigação e repressão do crime dependem cada vez mais da possibilidade de coletar, acessar e transferir informações e dados pessoais mantidos por empresas fora das fronteiras nacionais" (VIOLA; HERINGER; CARVALHO, 2021, p. 1).

De maneira similar, Luiz Fernando Rodrigues destaca que, em um período no qual a troca de informações é essencial para as forças de inteligência na contenção da criminalidade, as instituições de segurança pública deveriam adotar medidas que facilitem as comunicações. O autor destaca, como exemplo, a instituição de um sistema de dados unificado com permissão de acesso às autoridades de segurança pública nas situações que envolvessem questões criminais (RODRIGUES, 2020, p. 442).

No mesmo sentido, Borka Jerman-Blažič e Tomaž Klobučar apontam que há enorme quantidade de evidências produzidas nos meios eletrônicos e armazenadas em provedores diversos, como servidores de nuvem. A investigação criminal passa a demandar cada vez mais informações armazenadas pelos provedores técnicos (JERMAN-BLAŽIČ; KLOBUČAR, 2019, p. 271).

Conforme argumentam Paulo Rubens Carvalho Marques, Pablo Coutinho Barreto e Octávio Celso Gondim Paulo Neto, o compartilhamento de bancos de dados[60] entre instituições de persecução penal e de segurança pública é uma expressão do princípio da eficiência. Para os autores, a imposição de restrições desproporcionais ao compartilhamento de dados entre as autoridades competentes não seria razoável, tendo em vista que prejudicaria a ação das forças de segurança (MARQUES, BARRETO, NETO, 2020, p. 591-592).

[60] Segundo Carlos Alberto Heuser, define-se banco de dados como o "conjunto de dados integrados que tem por objetivo atender a uma comunidade de usuários" (HEUSER, 1998, p. 2).

Embora o uso dos dados pessoais tenha se tornado estratégico na sociedade contemporânea, incluindo para as atividades de investigação criminal, existem limitações a serem ponderadas. Mesmo nas hipóteses em que a coleta, o uso ou o compartilhamento de dados forem relevantes para o interesse público, o tratamento aplicado aos dados deve estar pautado pelo princípio da proporcionalidade. Para tanto, o juízo de proporcionalidade deve levar em consideração a finalidade para a qual os dados seriam úteis, os direitos fundamentais e os interesses do titular (TOSCHI; LOPES, 2020, p. 102). De maneira similar, Viana, Montenegro e Gleizer argumentam que a regulação da proteção de dados aplicada ao setor público deve ter como parâmetro os interesses dos indivíduos sobre os dados e, ao mesmo tempo, os "efeitos estatais pretendidos como tratamento de dados pessoais" (VIANA; MONTENEGRO; GLEIZER, 2020, p. 3).

Sobre o assunto, Aline Seabra Toschi e Herbert Emílio Araújo Lopes, retomam a *General Data Protection Regulation*:

> Quanto aos dados pessoais passíveis de tratamento para o interesse da segurança pública, também não abarcados pela proteção no tratamento de dados, o art. 23, item 1, d, do GDPR dispõe que as limitações à proteção no tratamento de dados para o fim de prevenir, investigar, detectar e reprimir infrações penais e de prevenir ameaças à segurança pública devem levar em consideração os direitos e liberdades fundamentais e a proporcionalidade da medida, principalmente em se tratando de uma sociedade democrática. (TOSCHI; LOPES, 2020, p. 102).

Para Toschi e Lopes, a violação do princípio da proporcionalidade sob a justificativa de interesse público ligado à segurança pode produzir abusos contra o direito à proteção de dados pessoais. A permissão do uso de dados de maneira abusiva pode implicar na perda de controle do titular sobre as suas próprias informações pessoais e sobre os usos posteriores feitos a partir delas (TOSCHI; LOPES, 2020, p. 102), comprometendo o princípio da autodeterminação informativa.

A Comissão de Direito Internacional identificou que as justificativas para intervenção na vida privada dos indivíduos são legítimas nas hipóteses em que estiverem em conformidade com a lei, quando forem necessárias para a sociedade democrática e quando não forem desproporcionais para a finalidade a qual a intervenção está vinculada (COMISSÃO DE DIREITO INTERNACIONAL, 2006, P. 224).

O direito à proteção de dados implica, ademais, para além da regular tutela dos dados dos indivíduos, a proteção contra as consequências que as informações podem produzir para seus titulares (VIANA; MONTENEGRO; GLEIZER, 2020, p. 3). Trata-se de uma dupla finalidade que sinaliza duas perspectivas à proteção de dados: de um lado, a autodeterminação informativa – já abordada nesta pesquisa -, que garante o controle dos dados pessoais ao

titular; de outro, proteção ante os impactos que o uso das informações pode produzir contra o titular.

No entanto, dada a relevância de dados informáticos na sociedade contemporânea, é igualmente necessário garantir que o Estado seja capaz de instrumentalizar tais informações, em hipóteses legalmente determinadas, ainda que contra o interesse individual do titular. É preciso compatibilizar a ação legítima do Estado no uso e no compartilhamento de dados, com o pressuposto de que o indivíduo tenha as condições necessárias para "autodeterminar-se suficientemente enquanto o Estado age" (VIANA; MONTENEGRO; GLEIZER, 2020, p. 4). Reforça-se a necessidade de as hipóteses restritivas estarem legalmente previstas no ordenamento jurídico. Nesse sentido:

> Por isso, erigir as barreiras próprias de um direito fundamental no entorno dos dados pessoais obriga o Estado, de forma geral, a só adentrar este espaço quando expressamente autorizado a tanto e apenas quando necessário para a realização de suas legítimas funções. Daí dizer que, em relação às informações individuais, cada uma das ramificações estatais (como a polícia, o Ministério Público, os tribunais etc.) só pode levantá-las na medida em que sejam necessárias para, e apenas para, a realização de suas tarefas. E que, tão logo cumpridas essas tarefas, qualquer manutenção das informações levantadas carece de nova fundamentação, tanto formal quanto material. São essas as razões que fundamentam a ideia de vinculação finalística: o uso dos dados (ou seja, das informações nele contidas) está vinculado à finalidade de seu levantamento, e qualquer uso para outro fim, que não este inicial, representa, portanto, outra autônoma intervenção do Estado (VIANA; MONTENEGRO; GLEIZER, 2020, p. 4).

A lógica apresentada é de uma política de abstenção.[61] Dessa forma, considerando que o direito à proteção de dados possui caráter constitucional e faz parte da esfera pessoal protegida, o Estado, em regra, não poderia intervir nesse domínio. As exceções para intervenção do Estado, assim, devem ser legalmente previstas e regularmente justificadas. Para Viana, Montenegro e Gleizer, "é o paradigma da abstenção que deve orientar a proteção de dados nas áreas da segurança pública e do processo penal" (VIANA; MONTENEGRO; GLEIZER, 2020, p. 6).[62]

---

[61] Viana, Montenegro e Gleizer esclarecem que a "clássica e primordial função dos direitos fundamentais, enquanto direito de defesa, é exigir atitude geral de abstenção do Estado" (VIANA; MONTENEGRO; GLEIZER, 2020, p. 7)".

[62] Sobre a distinção entre os usos de dados no âmbito da persecução penal e das atividades de segurança pública, Viana, Montenegro e Gleizer ponderam: não é possível falar em proteção de dados na Segurança Pública e no Processo Penal de forma geral, sem uma necessária distinção precisa entre as atuações estatais em cada um desses âmbitos. Elas se orientam por finalidades distintas e com maior ou menor garantia ao indivíduo. É possível estabelecer certas ideias gerais de validade comum a ambos, mas não é possível, por exemplo, estabelecer hipóteses comuns de levantamento de dados pessoais para os dois. Enquanto um está voltado à prevenção de perigos, outro está interessado na punição de crimes. E, diferentemente do que ocorre nas relações cíveis, nas quais os indivíduos trocam seus dados de forma consentida, é no levantamento sem consentimento que reside o ponto crucial de toda a análise a seguir. É a forma como os dados chegam às mãos do Estado, contrariamente à vontade de seus titulares, o que definirá toda a estratégia de equilíbrio entre os interesses postos em ponderação (VIANA; MONTENEGRO; GLEIZER, 2020, p. 5).

Sob a égide do Estado de Direito, na qual se insere a República brasileira, os poderes Executivo e Judiciário, em atenção aos direitos fundamentais, devem atuar de maneira proporcional em cada caso concreto, dentro dos limites legalmente autorizados. Incumbe, portanto, ao legislador a autorização de intervenções sobre aspectos da vida humana abarcados pelos direitos fundamentais, desde que realizada de forma clara e reservando o mínimo essencial a ser protegido (VIANA; MONTENEGRO; GLEIZER, 2020, p. 8-9).

No âmbito da regulação da proteção de dados pessoais no contexto do processo criminal, segundo Viana, Montenegro e Gleizer, o fundamento a ser observado é a "defesa intransigente da reserva de lei e da reserva parlamentar na confecção das normas autorizativas de tratamento de dados, enquanto salvaguardas essenciais dos direitos da personalidade" (VIANA; MONTENEGRO; GLEIZER, 2020, p. 9-10).

Aproxima-se, assim sendo, do princípio da legalidade aplicado ao direito penal. De acordo com a contribuição de Antonio Coêlho Soares Junior, este princípio tem como objetivo de limitar o poder de punir estatal (JUNIOR, 2002, p. 74-75).[63] O princípio busca garantir um padrão mínimo de segurança jurídica ao indivíduo, tendo como referência a previsibilidade na intervenção do poder punitivo. A partir desta concepção, elenca-se 4 reflexos: a proibição de leis criminalizadoras posteriores ao fato; a possibilidade de que o indivíduo conheça previamente sobre os crimes e as penas; a garantia de que o indivíduo, quando acusado, não seja submetido à coerção penal distinta daquela prevista em lei; a possibilidade de retroatividade da lei penal nas hipóteses em que for favorável ao acusado (JUNIOR, 2019, p. 173-174).

Segundo este pressuposto, é necessário que a atividade legiferante, em atenção ao princípio da reserva de lei, autorize expressamente as ações de intervenção estatal para fins penais relacionadas à proteção de dados, tais quais a intercepção e o armazenamento. No mesmo sentido, o uso de dados para esta finalidade deve estar vinculado a um propósito legítimo para que não sejam utilizados para finalidades diversas (VIANA; MONTENEGRO; GLEIZER, 2020, p. 9-10).

Para Viana, Montenegro e Gleizer, o levantamento de dados configura "a pedra angular da proteção de dados pessoais no âmbito estatal" diversas (VIANA;

[63] Junior desdobra o princípio da legalidade, em referência a teoria de Maurach, em 4 regras: a) proibição de retroatividade da lei penal que fundamente ou agrave o direito de punir (*nullum crimen, nulla poena sine lege praevia*); b) proibição de recorrer aos costumes para a identificação de práticas criminosas e suas respectivas penas (*nullum crimen, nulla poena sine lege scripta*); c) proibição do uso da analogia em relação às normas incriminadoras (*nullum crimen, nulla poena sine lege stricta*), e d) proibição da existência de normas penais em linguagem vaga, ambígua ou indeterminada (*nullum crimen, nulla poena sine lege certa*) (MAURACH apud JUNIOR, 2002, p. 74-75).

MONTENEGRO; GLEIZER, 2020, p. 9-10). Por essa razão, ressalta-se novamente a adequação da finalidade vinculada para a realização de instrumentos de persecução penal relacionados com o armazenamento, o uso e o compartilhamento de dados pessoais.

A autorização normativa mencionada deve determinar as exceções ao direito à proteção de dados em cada situação de tratamento dos dados:

> Cada outra forma de processamento – o uso, o armazenamento e o compartilhamento – configura uma intervenção autônoma que estará vinculada ao propósito determinado na norma de levantamento. Por isso, diferencia-se entre determinação da finalidade e vinculação à finalidade. Enquanto autônomas intervenções, cada uma dessas quatro fases do processamento necessita de uma autorização (legislativa) específica, ainda que disciplinada no mesmo dispositivo (VIANA; MONTENEGRO; GLEIZER, 2020, p. 12).

Tal é a justificativa para que direitos fundamentais como o direito à proteção de dados pessoais e, em uma perspectiva mais rigorosa, a inviolabilidade do sigilo de dados, sejam compatíveis com suas exceções quando necessário à tutela de outras demandas relevantes, como a segurança pública e o processo penal (VIANA; MONTENEGRO; GLEIZER, 2020, p. 14).

Sobre o tema, o Conselho da Europa recomenda que intervenções no direito à privacidade, como a vigilância ou a interceptação de comunicações, sejam autorizadas apenas nas hipóteses que a lei determinar. Ao mesmo tempo, a intervenção deverá constituir uma medida necessária para resguardar, alternativamente ou cumulativamente, a segurança estatal, a segurança pública, os interesses monetários do Estado, a repressão de ofensas criminais ou a proteção de direitos e garantias fundamentais (CONSELHO DA EUROPA, 2018, p. 276).

No entanto, o ordenamento jurídico brasileiro apresenta lacunas em matéria de tratamento de dados no contexto da segurança pública e do processo penal. Viana, Montenegro e Gleizer identificaram a deficiência em normas que "autorizem e regulem intervenções no âmbito protegido dos dados pessoais", especialmente quando se trata de aspectos distintos da inviolabilidade de sigilo, como medidas de infiltração online ou de observações prolongadas (VIANA; MONTENEGRO; GLEIZER, 2020, p. 17).

Adiante, a insuficiência destas normas regulatórias também é constante nas demais formas de tratamentos de dados, como o arquivamento, a alteração, a utilização e o compartilhamento. Estas lacunas produzem inseguranças jurídicas no domínio do uso de dados nas atividades de segurança pública e de persecução penal no Brasil (VIANA; MONTENEGRO; GLEIZER, 2020, p. 17).[64]

[64] Viana, Montenegro e Gleizer exemplificam, nesse sentido, atividades que não possuem regulação adequada voltada ao uso de dados no âmbito da segurança pública e da persecução penal: Controle de identidade, emprego de câmeras de vigilância em espaços públicos ou das denominadas Body-Cams, observações prolongadas,

A conclusão de Viana, Montenegro e Gleizer indica que as formas de tratamento de dados pessoais a serem praticadas pelas autoridades de segurança pública e de persecução penal exigem regulamentação legal. As intervenções no domínio da proteção de dados, ademais, como já destacado, estão vinculadas a finalidades específicas e legítimas (VIANA; MONTENEGRO; GLEIZER, 2020, p. 44).

Há, todavia, problemática constante no compartilhamento de dados. Isto é, na medida em que dados são transferidos de uma instituição para outra, é possível que finalidade distinta para a qual originalmente foram coletados e armazenados seja a eles aplicada. Por esse ângulo, o compartilhamento de dados envolve 2 intervenções diferentes: a primeira, trata-se do fornecimento de acesso a dados já coletados e armazenados; a segunda, por sua vez, refere-se ao armazenamento e ao uso de dados pelo controlador secundário. Neste processo, são atribuídas novas finalidades aos dados diante das necessidades das instituições envolvidas no compartilhamento. Por essa razão, tratando-se de mais de uma intervenção, cada uma delas deve possuir autorização legal própria (VIANA; MONTENEGRO; GLEIZER, 2020, p. 44-45).

Considerando que o armazenamento e o compartilhamento de dados também se tornaram instrumentos utilizado para fins de segurança pública, o direito à proteção de dados pessoais também deve ser aplicado a este contexto. Entende-se, portanto, que na era digital, o direito à proteção de dados pessoais também deve ser observado no âmbito da persecução penal.

Segundo Luigi Ferrajoli, a intervenção penal remete a uma relação entre o Estado e o indivíduo, na qual entram em choque as liberdades privadas e o poder público. Esta intervenção é fundamentada em elementos internos e externos: a legitimação interna é baseada em princípios que conformam o ordenamento jurídico, também denominados "intra-jurídicos"; a externa, por sua vez, é fundada em valores morais, políticos ou de utilidade, distintos do direito positivo, denominados "meta-jurídicos" (FERRAJOLI, 2010, p. 210-213).[65]

Utilizando como referência a compreensão de que o crime é a execução de um risco presente em uma sociedade, argumenta-se, nos termos de Claus Roxin, que a finalidade do Direito Penal é a contenção dos riscos apresentados contra os bens jurídicos dos indivíduos e

---

levantamento de dados de telecomunicação, criação de bancos de dados etc., para tudo isso há carência de uma adequada regulação em lei (VIANA; MONTENEGRO; GLEIZER, 2020, p. 18).

[65] Para Ferrajoli, contudo, os valores morais e políticos não podem estar vinculados estritamente com os interesses punitivos de uma classe específica. O Direito Penal, nesse sentido, deve ser lastreado na utilidade em que este possa oferecer aos indivíduos, levando em consideração os seus direitos e as necessidades de segurança (FERRAJOLI, 2010, p. 222).

da sociedade (ROXIN, 2000, p. 45). Adiante, Luis Gracia Martín sintetiza em poucas palavras:

> Em resumo, a função do Direito penal consiste [...] na proteção dos bens jurídicos por meio da conservação dos valores ético-sociais da consciência, da formação do juízo ético-social dos cidadãos e do fortalecimento de sua consciência de permanente fidelidade (legal) ao Direito" (MARTÍN, 2007, p. 45).

Para Ferrajoli, é possível elencar que o Direito Penal possui "dupla finalidade preventiva": a prevenção de delitos e a prevenção das penas informais. Busca-se prevenir, portanto, para além da repetição do ilícito criminal, que pena seja injusta. O Direito Penal, nesse sentido, não possui como único objetivo a contenção da criminalidade, mas igualmente busca impedir que sejam aplicadas penas "arbitrárias ou desproporcionais" (FERRAJOLI, 2010, p. 331-332).

Nos termos de Martín, o Direito Penal age de modo a limitar o poder punitivo estatal. Por esta razão, considerando que o Estado exerce o monopólio sobre a força estatal e sobre a jurisdição normativa criminal, o autor declara a necessidade de haver um sistema normativo cujo conteúdo limite a intervenção estatal em matéria penal (MARTÍN, 2007, p. 153).

Conforme apresenta Ferrajoli, o garantismo é o fundamento do Direito Penal, uma vez que se pauta na garantia dos direitos fundamentais, ainda que a despeito do desejo punitivo de uma maioria. Busca-se evitar, dentre outros aspectos, que o Estado possua um alcance exacerbados de suas instituições punitivas, violando, destarte, direitos e garantias fundamentais (FERRAJOLI, 2010, p. 335-336).

Tendo como base os pressupostos sinteticamente apresentados, destaca-se, na sequência, a abordagem de Roxin sobre o fundamento de um sistema jurídico-penal que englobe o Direito Penal e a Política Criminal. Compõe a lógica do instituto, assim sendo, a aproximação teórica do Direito Penal com a política criminal (ROXIN, 2000, p. 1-3).

Por esta lente, nos termos de Roxin, política criminal deve estar compreendida com base em um sistema jurídico-penal, de tal modo que as decisões político-criminais devam estar fundamentadas nos princípios deste sistema. O Direito Penal, destarte, pode também ser compreendido como o meio pelo qual os objetivos das políticas criminais alcancem vigência no âmbito jurídico (ROXIN, 2000, p. 82).

Por consequência, os instrumentos atrelados ao poder punitivo devem estar limitados por meio do Direito Penal, o qual deve estar pautado em princípios de proteção dos direitos humanos quando aplicado aos programas de intervenção estatal (PRADO, 2013, p. 92). Diante dos aspectos apresentados, adota-se o entendimento de que as políticas criminais não devem ignorar o direito à proteção de dados pessoais, com vistas a assegurar a tutela dos

direitos fundamentais dos indivíduos e a viabilizar a conformidade dessas políticas de intervenção com o sistema jurídico-penal.

Em um contexto de aumento da importância e da produção de dados, a conclusão deste tópico gravita em torno do pressuposto de que o direito à proteção de dados pessoais se impõe como um imperativo a ser observado no curso das atividades de persecução penal. Na medida em que dados sensíveis são amplamente produzidos, coletados, armazenados e transacionados, estes se tornam cada vez mais úteis na investigação criminal. No entanto, como visto, os limites e as possibilidades de intervenção no direito à proteção de dados pessoais devem estar claramente previstos na legislação.

2.3 AS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PARA FINS DE PERSECUÇÃO PENAL COMO UM RISCO

Com a finalidade de adentrar neste tópico, é necessário levar em consideração alguns pressupostos preliminares. Inicialmente, os crimes transnacionais constituem uma ameaça que ultrapassa os limites territoriais de um Estado, razão pela qual demandam ação conjunta a nível de cooperação internacional. Na sequência, em um contexto de aprofundamento da importância dos dados na sociedade contemporânea, já delineada anteriormente, as autoridades de segurança pública passam a utilizar e a compartilhar progressivamente dados e informações pessoais.

Nesse sentido, com o objetivo de conter os crimes transnacionais, notadamente o cibercrime, o intercâmbio de dados entre autoridades competentes de países distintos passa a se tornar um imperativo. Todavia, se, por um lado, os crimes transnacionais constituem um risco, o compartilhamento de dados e informações pessoais entre Estados também pode ser classificado como um risco na sociedade contemporânea.

Tendo como ponto de partida o objetivo de compreender a maneira pela qual o compartilhamento de informações entre Estados para fins de persecução penal compõe um risco, cumpre retomar a formulação de Ulrich Beck sobre a Sociedade de Risco. O marco analítico está na impossibilidade de se prever precisamente as situações de perigo, de modo que as ameaças – e a expectativa de haver ameaças – difundem um sentimento de insegurança no âmbito social (BECK, 2002, p. 237).

De acordo com os pressupostos da Sociedade de Risco de Beck, os “riscos” são ameaças futuras, derivadas dos avanços técnico-econômicos, que produzem inseguranças na

sociedade (BECK, 2002, p. 237).[66] Assim sendo, a produção social da riqueza e o desenvolvimento tecnológico são acompanhados pela multiplicação de riscos e, portanto, de inseguranças (BECK, 2002, p. 21-22).[67] Conforme já apresentado, o desenvolvimento tecnológico permitiu que os indivíduos controlassem riscos oferecidos pela natureza, mas, ao mesmo tempo, produziu novos riscos inerentes ao processo tecnológico (BARBOSA, 2012, p. 20).

Segundo Beck, o ponto central da percepção dos indivíduos sobre o risco está em uma antecipação de eventual ameaça futura. Destarte, na sociedade de risco, a previsão de ameaças futuras conduz a ação dos indivíduos para se evitar ou mitigar os problemas e as crises que ainda estão por vir – ou que se espera que virão. O risco passa a constituir, portanto, uma força mobilizadora da ação individual e coletiva em prol de maior segurança (BECK, 2002, p. 40).

Os avanços tecnológicos produzem riscos imprevisíveis. Novos perigos se desdobram das inovações técnicas e científicas, dos quais os indivíduos não necessariamente possuem controle, de modo que as decisões são tomadas em um cenário de incertezas e de insegurança (BECK, 2015, p. 20). Com tal avanço, os perigos e ameaças ultrapassam as fronteiras físicas, na medida em que suas causas e consequências não estão limitadas a um espaço geográfico restrito, e os riscos se tornam desafios globais (BECK, 2015, p. 94).[68] Trata-se da sociedade de risco mundial, na medida em que as decisões humanas possuem a capacidade de afetar uma coletividade indistintamente (BARBOSA, 2012, p. 29).

Conforme já salientado, o desenvolvimento tecnológico contribuiu para novos usos aos dados informáticos. Uma vez que os dados passaram a ser mais facilmente coletados, armazenados e processados, novas utilidades se tornaram populares e progressivamente mais relevantes para entidades públicas e privadas. Ao mesmo tempo, com a digitalização das atividades humanas e ampliação da conectividade, produz-se cada vez mais dados e informações de conteúdo sensível (VIOLA, HERINGER; CARVALHO, 2021, p. 2). Por essa

---

[66] Mario Viola, Leonardo Heringer e Celina Carvalho identificam que a circulação transfronteiriça de dados é um elemento importante para o desenvolvimento econômico: "A tendência, portanto, é a circulação transfronteiriça de dados. Em muitos aspectos, os fluxos internacionais de dados podem ser considerados parte do tecido que sustenta a economia global" (VIOLA; HERINGER; CARVALHO, 2021, p. 2).

[67] Segundo Niklas Luhmann, os riscos podem ser compreendidos como consequências possíveis, podendo ou não ser conhecidas pela sociedade, que derivam de uma decisão racional dos indivíduos (LUHMANN, 1996, p. 123-172).

[68] Segundo Beck, os riscos globais possuem 3 características: deslocalização, imprevisibilidade e incompensabilidade. Há deslocalização na medida em que as causas e consequências de um fato se propagam em escala global em períodos curtos de tempo. Verifica-se a imprevisibilidade em razão de que os riscos são hipotéticos e podem se basear em ameaças de difícil imprevisibilidade, com efeitos potencialmente incalculáveis. Por fim, são incompensáveis uma vez que não é possível anular todos os efeitos nocivos produzidos pelos riscos (BECK, 2015, p. 94).

razão, o compartilhamento de dados entre Estados para fins de persecução criminal, ao envolver objetos cujo conteúdo é importante para os titulares, passa a representar um perigo potencial – um risco – ao direito à privacidade dos indivíduos.

De acordo com Alexandra Maria Rodrigues Araújo, o conceito de transferência internacional de dados diz respeito ao compartilhamento de informações a destinatários específicos. Nos termos da autora, "a informação necessita de estar deliberadamente disponível para destinatários no país terceiro. Desta forma, [...] exclui, também, as situações de mero trânsito dos dados pelo território de um Estado terceiro" (RODRIGUES ARAÚJO, 2017, p. 210).

Em relatório publicado pelo Instituto de Tecnologia e Sociedade do Rio, Mario Viola, Leonardo Heringer e Celina Carvalho constataram que, no mundo globalizado e marcado pelo alto fluxo de dados, as relações entre territórios distintos se tornam cada vez mais complexas. Diante da complexidade das relações envolvendo Estados distintos, as relações entre os Estados em busca de objetivos comuns exigem cooperação internacional e o compartilhamento de informações paulatinamente mais constantes. O relatório menciona, a título de exemplo, que o Estado brasileiro endereçou pedidos de cooperação jurídica em matéria penal a 52 países distintos no curso da Operação Lava Jato (VIOLA, HERINGER; CARVALHO, 2021, p. 1).

Uma vez considerado o enorme volume de dados e informações coletadas e processadas atualmente, as instituições de segurança pública e de persecução penal passam a fazer uso ativo de instrumentos de acesso, coleta e compartilhamento de informações por meios eletrônicos. Nesse contexto, as ofensas criminais que produzem impactos extraterritoriais exigem o fortalecimento dos mecanismos de cooperação internacional em matéria criminal, ao mesmo tempo em que se mantenha a proteção dos direitos humanos e a prevalência do Estado de Direito (CARRERA; STEFAN, 2020, p. 3).[69]

Dessa forma, assinala-se trecho do "*Internet & Jurisdiction and ECLAC Regional Status Report 2020*" da Comissão Econômica para a América Latina e o Carible (CELAC):

> No curso de uma investigação multi-jurisdicional, as agências de aplicação da lei precisam ter acesso a informações que estão localizados em outros países, talvez porque as ações em questão cruzaram jurisdições. Por exemplo, uma empresa pode transferir fundos para uma conta offshore pertencente a um funcionário corrupto; ou supostos criminosos pode fazer uso de servidores na nuvem para armazenar dados

[69] No mesmo sentido: E-evidence connected to crime acts perpetrated in the interconnected society is often cross-jurisdictional, because often the data is stored outside the sphere of influence of the investigating authority in the country where investigation has been launched, or by providers of electronic communication services and platforms whose main seat is located outside the investigating country, resulting in the fact that investigating authorities are not able to use their domestic investigative tools (JERMAN-BLAŽIČ; KLOBUČAR, 2019, p. 272).

> em territórios estrangeiros. Evidências produzidas em uma investigação podem ser relevantes para outra, e, em alguns casos, a investigação de um caso de corrupção estrangeira pode afetar a segurança da investigação em outro país (CELAC, 2020, p. 59).[70]

Embora a transferência internacional de dados constitua uma ferramenta importante para a persecução penal, a nível internacional as autoridades competentes possuem suas capacidades de investigação limitada. Nas hipóteses em que os provedores estejam localizados em países estrangeiros, as atividades de investigação criminal de um Estado passam a encontrar como freio as fronteiras e a soberania dos demais Estados (JERMAN-BLAŽIČ; KLOBUČAR, 2019, p. 272). Evidências digitais, por exemplo, podem estar divididas entre diferentes jurisdições e, igualmente, podem ser facilmente transferidas para outro território, transitando constantemente entre servidores localizados em Estados distintos (CELAC, 2020, p. 59). Sob este prisma se insere a necessidade de haver mecanismos de cooperação internacional em consonância com critérios de proteção de dados.

O direito à proteção de dados pessoais está previsto em documentos internacionais, seja a nível mundial ou a nível regional. É necessário identificar instrumentos que versam sobre a transferência internacional de dados, com ênfase à aplicação penal. A Resolução 68/167 da Assembleia Geral das Nações Unidas, de 2013, intitulada "O direito à privacidade na era digital", reconhece que o desenvolvimento tecnológico ampliou o acesso às tecnologias da informação e da comunicação, permitindo que governos, empresas privadas e indivíduos tomem ações de vigilância, interceptação e coleta de dados (ONU, 2013, p. 2-3).

Ademais, a Resolução incentiva os Estados a:

> a) Respeitar e proteger o direito à privacidade, incluindo o contexto das comunicações digitais; b) adotar medidas para colocar fim a violações a esses direitos e para criar as condições de prevenção dessas violações, incluindo assegurar que a legislação nacional esteja em conformidade com as obrigações internacionais de direitos humanos; c) revisar seus procedimentos, práticas e legislações relacionadas à vigilância e à interceptação de comunicações, à coleta de dados, incluindo vigilância em massa [...]; d) estabelecer ou manter mecanismos domésticos de supervisão independentes e efetivos, capazes de assegurar a transparência, quando apropriado, e a *accountability* da vigilância estatal das comunicações, a interceptação destas e a coleta de dados pessoais (ONU, 2013, p. 2-3).[71]

---

[70] Tradução livre. Na versão original: In the course of a multi-jurisdiction investigation, law enforcement agencies need to have access to information that may be located in another country, perhaps because the actions concerned have crossed jurisdictions. For example, a company might wire funds to an offshore account belonging to a corrupt official; or alleged criminals may use cloud Internet services that store data overseas. Evidence produced in one investigation can be relevant to another, and in some cases the investigation of a foreign corruption case can impact the security of an investigation in another country (CELAC, 2020, p. 59).

[71] Na versão original: Calls upon all States: (a) To respect and protect the right to privacy, including in the context of digital communication; (b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law; (c) To review their procedures, practices and legislation

Menciona-se, adicionalmente, o Relatório da Comissão de Direito internacional das Assembleia Geral das Nações Unidas, de 2006, que propõe, no Anexo D, a inclusão da temática de proteção de dados pessoais em fluxos transfronteiriços de informação. A Comissão reconhece que o desenvolvimento tecnológico propiciou a circulação de informações pela via eletrônica de maneira quase que instantânea entre os Estados (COMISSÃO DE DIREITO INTERNACIONAL, 2006, p. 217-229).

Nos termos do relatório, a Comissão observa com preocupação o compartilhamento de dados pessoais por atores distintos (COMISSÃO DE DIREITO INTERNACIONAL, 2006, p. 217-229).[72] Adiante, o relatório identifica 11 princípios centrais identificáveis nos documentos internacionais e na legislação interna dos Estados em matéria de proteção de dados:

> a) coleta e processamento de dados justo e legal; b) precisão; c) especificação e limitação da finalidade; d) proporcionalidade; e) transparência; f) participação do indivíduo e o direito ao acesso; g) não-discriminação; h) responsabilidade; i) supervisão e sanções legais; j) equivalência de dados no caso de fluxo transfronteiriço de dados pessoais; k) princípio da derrogabilidade distintos (COMISSÃO DE DIREITO INTERNACIONAL, 2006, p. 221).[73]

Ressalta-se o item "j", que trata da equivalência de dados nas situações de fluxo transfronteiriço de dados pessoais. Segundo a Comissão, este aspecto poderia levantar disputas entre os Estados em razão de questionar as situações em que a transferência de dados

---

regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law; (d) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data (ONU, 2013, p. 2-3).

[72] O relatório da Comissão menciona a Declaração Montreux sobre a proteção de dados no contexto de mundo globalizado, manifestada por ocasião da *Twenty-seventh International Conference of Data Protection and Privacy Commissioners*. A declaração destaca a importância da cooperação internacional para garantir a conformidade com as normas de proteção de dados no contexto da globalização: "Nous sommes convenus d'attacher une importance particulière à la protection des libertés et des droits fondamentaux des personnes, notamment de leur vie privée, dans l'utilisation des fichier et traitement des données à caractère personnel. Nous appelons à créer ou consolider les règles assurant cette protection. Nous encourageons la coopération internationale entre les autorités indépendantes chargées dans chaque pays de contrôler le respect de ces règles" (DATA PROTECTION AND PRIVACY COMMISSIONERS, 2006).

[73] Na versão original: The international binding and non-binding instruments, as well as the national legislation adopted by States, and judicial decisions reveal a number of core principles, including: (a) lawful and fair data collection and processing; (b) accuracy; (c) purpose specification and limitation; (d) proportionality; (e) transparency; (f) individual participation and in particular the right to access; (g) non-discrimination; (h) responsibility; (i) supervision and legal sanction; (j) data equivalency in the case of transborder flow of personal data; and (k) the principle o derrogability (COMISSÃO DE DIREITO INTERNACIONAL, 2006, p. 221). O princípio da derrogabilidade permite que sejam permitidas exceções nas hipóteses em que seja necessário para a proteção da segurança nacional, da ordem pública, da saúde ou da moralidade pública, ou para proteger o direito de terceiros (COMISSÃO DE DIREITO INTERNACIONAL 2006, p. 224).

poderia ser feita quando uma das partes não garante (ou não consegue garantir) os níveis adequados de proteção (COMISSÃO DE DIREITO INTERNACIONAL, 2006, p. 225).

O "*Privacy Framework*" da Organização para Cooperação e Desenvolvimento Econômico (OCDE), de 2013, estabelece princípios de aplicação do direito à privacidade nas esferas doméstica e internacional. Destaca-se, em consonância com o requisito de equivalência apresentada pela Comissão de Direito Internacional, o item 17 do relatório da OCDE: um Estado membro não deve restringir fluxos transfronteiriços de dados pessoais com outros países que observem as diretrizes dispostas pela OCDE ou que já possua garantias suficientes em matéria de proteção de dados, incluindo mecanismos efetivos de fiscalização. Ao contrário, as restrições ao fluxo de dados pessoais entre países devem ser proporcionais aos riscos de cada cenário, de modo que seja necessário levar em consideração o conteúdo dos dados (se há natureza de dados sensíveis), a finalidade a ser atribuída o contexto em que se insere o processamento dos dados (OCDE, 2013).

O compartilhamento de dados entre Estados e a possibilidade de acesso transfronteiriço se tornaram demandas relevantes para fins de investigação criminal, como já delineado. Contudo, o Estado brasileiro tem encontrado dificuldades na obtenção do acesso a dados de cidadãos europeus ou de estrangeiros residentes na União Europeia, quando relacionado a atividades de segurança pública, controle migratório ou persecução criminal (ARAS, 2020, p. 26).[74]

A LGPD, como já abordado neste capítulo, excluiu o tratamento de dados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (BRASIL, 2018), de modo que a aplicação do direito à proteção de dados nessas matérias deva ser regulada por um futuro diploma normativo. O sistema protetivo europeu, por sua vez, possui dois principais instrumentos que são complementares: o Regulamento Geral de Proteção de Dados e a Diretiva n.º 2016/680, aplicável para fins de segurança pública e investigação criminal (VIOLA, HERINGER; CARVALHO, 2021, p. 2).

Tais instrumentos normativos se tornam notáveis na medida em que, conforme descreve Pessoa, a LGPD e o GDPR, possuem aplicabilidade mesmo para além das fronteiras nacionais (PESSOA, 2020, p. 77). De acordo com o autor:

> De maneira semelhante ao RGPD, a LGPD possui aspectos extraterritoriais, pois aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de

[74] Aras menciona, como exemplo, a exclusão da possibilidade de transferência de dados pessoais no acordo específico promulgado pelo Decreto n. 10.364/2020 entre o Brasil e o Serviço Europeu de Polícia (ARAS, 2020, p. 26).

> tratamento seja realizada no território nacional; ou que a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou que os dados pessoais objeto do tratamento tenham sido coletados no território nacional, o que pode, eventualmente, ocasionar um conflito positivo de normas de direito privado internacional, à medida em que, em determinado tratamento de dados, tanto o RGPD quanto a LGPD podem ser aplicáveis (PESSOA, 2020, p. 77).

É possível identificar alguns fatores explicativos para a aplicação extraterritorial da legislação protetiva de dados pessoais pela União Europeia. Inicialmente, a preocupação das instituições europeias com a tutela dos direitos dos cidadãos europeus diante do atual cenário de conectividade global. Ao mesmo tempo, pesquisa da Comissão Europeia verificou que parcela expressiva da população europeia reconheceram a importância de se manter o mesmo nível de proteção também em escala transnacional (GNOATTON, 2021, p. 34-35).[75]

Segundo consta no artigo 45 do GDPR, a transferência de dados pessoais de um país membro da União Europeia para um Estado terceiro dependerá de a Comissão Europeia ter reconhecido que esse Estado possui um nível adequado de proteção aos dados. Exige-se do país receptor a) o Estado de Direito, com respeito aos direitos humanos; b) a existência de um de uma autoridade supervisora independente responsável por assegurar a conformidade das normas de proteção de dados; e c) comprometimento do Estado com obrigações internacionais relativas à proteção de dados (UNIÃO EUROPEIA, 2016-A). Conforme esclarece o *European Data Protection Board*, entende-se por "nível adequado de proteção" um sistema que estabelece garantias equivalentes àquelas constantes no regime europeu (EUROPEAN DATA PROTECTION BOARD, 2021, p. 8-16).

A LGPD brasileira prevê, de maneira similar ao GDPR, regras com a finalidade de assegurar a proteção na transferência internacional de dados. A legislação brasileira estabelece três regimes de salvaguardas para transferência internacionais de dados, quais sejam: "(i) a declaração de existência de grau de proteção de dados pessoais adequado ao previsto na LGPD; (ii) a existência de garantias de cumprimento dos preceitos da LGPD; (iii) derrogações específicas no regime da LGPD [...] (DOMINGOS; SILVA; OLIVEIRA, 2020, p. 145).

A definição do que constitui um grau de proteção adequado, nos termos do item "i" (e em consonância com o inciso I do artigo 33 da LGPD) é função da Autoridade Nacional de

[75] Ademais, segundo Gnoatton: Cumulativamente às previsões do Regulamento que impactam entes externos à União Europeia, é do interesse desta fomentar globalmente políticas de proteção de dados pessoais, por meio de instâncias multilaterais (Nações Unidas, G20 e APEC) e medidas de cooperação internacional com parceiros internacionais importantes, visando à efetiva aplicação dos direitos previstos no Regulamento.81 Inclusive, o interesse em estabelecer medidas de cooperação internacional em matéria de proteção de dados, seja por meio de regras internacionais, de assistência mútua ou da promoção de debates, atividades e intercâmbio de documentos, legislações e práticas, encontra-se positivado no Art. 50 do GDPR (GNOATTON, 2021, p. 36).

Proteção de Dados. O ordenamento jurídico brasileiro não exige que os Estados destinatários das informações possuam legislação específica sobre o tema, mas deve ser possível verificar que a essência do direito à proteção de dados esteja presente neste país (DOMINGOS; SILVA; OLIVEIRA, 2020, p. 145).[76]

Em relação às derrogações específicas, é relevante destacar os incisos III, V e VI do artigo 33 da LGPD. De acordo com os dispositivos, a transferência internacional de dados pessoais será permitida quando for necessária para a cooperação jurídica internacional entre autoridades públicas responsáveis pela investigação e persecução (inciso III), nas hipóteses em que a autoridade nacional autorizar (inciso V) e quando a transferência estiver associada a compromisso assumido em acordo de cooperação internacional (BRASIL, 2018).[77]

Embora a LGPD mencione a possibilidade de transferência de dados quando necessária para a cooperação jurídica internacional voltada às atividades de investigação e persecução, deverá haver legislação futura para regular especificamente a proteção de dados no contexto da segurança pública e do Direito Penal. No paradigma jurídico da União Europeia, a já mencionada Diretiva n.º 2016/680, que dispõe especificamente sobre o "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", é lançada em conjunto com o GDPR (UNIÃO EUROPEIA, 2016-B) e institui o novo marco jurídico da União Europeia sobre a proteção de dados no domínio da investigação criminal (MARTÍNEZ, 2020, p. 169).[78]

A intenção apresentada nas considerações iniciais da Diretiva indica o interesse de facilitar a circulação de dados e a transferência para países terceiros (UNIÃO EUROPEIA, 2016-A), em consonância com os princípios delineados pelo *Privacy Framework* da OCDE (2013). A chave interpretativa observada a partir dos documentos mencionados diz respeito à intenção de facilitar a troca de informações pessoais entre autoridades competentes para a

[76] A LGPD determina que um rol não exaustivo de critérios a serem avaliados pela autoridade competente para averiguar se há nível de proteção adequado. Dessa forma, são elementos presentes na legislação brasileira: a existência de normas protetivas o país de destino, a própria natureza dos dados transacionados, a observância dos princípios de proteção de dados pessoais, a adoção de medidas de segurança com previsão em regulamento, a existência de garantias judiciais e institucionais de proteção aos dados pessoais, bem como outras circunstâncias específicas ao caso (BRASIL, 2018).

[77] Nos termos legais: art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: [...] III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional [...]; V - quando a autoridade nacional autorizar a transferência; VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional [...] (BRASIL, 2018).

[78] De acordo com os pontos motivadores da Diretiva n.º 2016/680, a livre circulação de dados pessoais entre as autoridades competentes e a transferência para países terceiros e organizações internacionais "deverão ser facilitadas, assegurando simultaneamente um elevado nível de proteção de dados pessoais" (UNIÃO EUROPEIA, 2016-A).

persecução penal, ao mesmo tempo em que seja mantido um regime adequado de proteção de dados pessoais entre as partes.[79]

A Diretiva n.º 2016/680, ao estabelecer um regime especial para a proteção de dados pessoais quando aplicada à persecução penal, oferece critérios e regras mais flexíveis a nível regional para a temática. A justificativa para tanto é a conformação de normas mais adequadas à consecução do interesse público de investigação criminal (MARTÍNEZ, 2020, p. 170). No âmbito da União Europeia há esforço para a harmonização das normas de proteção de dados para fins de cooperação judiciária internacional. No sistema da integração, portanto, já existem mecanismos que promovem a confiança entre os Estados envolvidos na transferência de dados e na permissão de acesso transfronteiriço a dados (MARTÍNEZ, 2020, p. 177).

Em relação aos Estados que não integram o bloco comunitário europeu – e que, portanto, não estão vinculados ao regime protetivo da União Europeia –, é necessário fomentar a confiança por meio da garantia sobre o respeito à proteção de dados pessoais (MARTÍNEZ, 2020, p. 178). Nesse sentido, nos termos da Diretiva, são estabelecidas condições para a transferência de dados pessoais para um Estado que não é membro da União Europeia: a) a transferência deve ser necessária para a realização de atividade de persecução penal; b) os dados pessoais devem ser transferidos para uma autoridade competente a desempenhar as funções de persecução penal;[80] c) que o Estado terceiro envolvido esteja apto segundo decisão de adequação da Comissão Europeia, ou na falta desta, que tenham sido apresentadas garantias adequadas à proteção de dados pessoais ou, ainda, no caso de derrogação (UNIÃO EUROPEIA, 2016-A).

---

[79] Sobre esta interpretação, a consideração n.º 7 da Diretiva n.º 2016/680 é esclarecedora: É crucial assegurar um nível elevado e coerente de proteção dos dados pessoais das pessoas singulares e facilitar o intercâmbio de dados pessoais entre as autoridades competentes dos Estados-Membros, a fim de assegurar a eficácia da cooperação judiciária em matéria penal e da cooperação policial. Para tal, o nível de proteção dos direitos e liberdades individuais 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 — incluindo a salvaguarda e a prevenção de ameaças à segurança pública — deverá ser equivalente em todos os Estados-Membros (UNIÃO EUROPEIA, 2016-A).

[80] Com a finalidade de esclarecer o termo autoridade competente, Rosa Ana Morán Martínez explica: Pero el concepto da autoridad judicial, incluyendo al Ministerio Fiscal, es un concepto definido en el derecho europeo. Efectivamente el TJUE ha establecido que el concepto de autoridad judicial es un concepto autónomo del derecho europeo que comprende no solo a Jueces y Tribunales sino a otros órganos, como el Ministerio Fiscal, que participan con un grado suficiente de independencia en las tareas de la Administración de Justicia. Así lo afirma en las Sentencias de los Asuntos Poltorak C-452/16 y Kovalkovas C-453, de 10 de noviembre de 2016. En estas sentencias el Tribunal aclara que para que una autoridad entre dentro del concepto europeo de autoridad judicial no es suficiente con que se trate de un órgano que participe en la Administración de Justicia sino que además tiene que tener un grado suficiente de autonomía que lo vincule de alguna forma al poder judicial que, conforme al principio de separación de poderes, que determinan el Estado de Derecho, se distingue del poder ejecutivo, en el que están incluidos otras autoridades administrativas o los servicios de policía (MARTÍNEZ, 2020, p. 182).

O item (c) faz referência a 3 possibilidades que um Estado não membro da União Europeia obtenha o reconhecido de que seu sistema de proteção de dados é adequado ao intercâmbio de dados pessoais para as finalidades da Diretiva n.º 2016/680. São elas: a) transferências de dados com fundamento em decisão de adequação da Comissão Europeia; b) transferência de dados com fundamento na apresentação de garantias adequadas; c) derrogações aplicáveis a situações específicas, quais sejam para a proteção de interesses vitais do titular dos dados ou de outrem, para a tutela dos legítimos interesses do titular, para a prevenção de ameaça imediata e grave contra a segurança pública de um Estado e para atender as finalidades de persecução penal definidas na Diretiva (UNIÃO EUROPEIA, 2016-A).

Nesta pesquisa, dá-se ênfase à hipótese das decisões de adequação enquanto mecanismo para reconhecimento de nível adequado de proteção de dados mais apropriado para as finalidades de cooperação jurídica internacional em matéria penal, conforme será abordado no item 3.2.

As exigências apresentadas pela integração europeia perante Estados terceiros buscam assegurar pelo menos três objetivos: a) garantir um bom nível de cumprimento das normas relativas à proteção de dados; b) possibilitar aos afetados que possam exercer seus direitos de forma rápida, efetiva e com poucos custos; e c) garantir que esteja em atuação estrutura independente que "obrigue reparações e imponha sanções" no caso de desrespeito às normas de proteção de dados (SILVA, 2013, p. 192).

Sobre a decisão de adequação e a necessidade de reconhecimento da presença de nível adequado de proteção de dados pessoais, é importante destacar a contribuição dos casos Schrems I e II. A disputa foi levada ao Tribunal de Justiça da União Europeia após a recusa do *Data Protection Comissioner* em investigar a reclamação de Maximilian Schrems sobre o fato de que a companhia *Facebook Ireland Inc.*, filial da *Facebook Inc*., sediada nos EUA, transferia dados pessoais de seus usuários aos Estados Unidos da América (EUA). Schrems apresentou pedido para que a *Facebook Ireland* fosse proibida de transferir seus dados pessoais para os EUA, alegando que o direito em vigor no ordenamento jurídico estadunidense não assegurava proteção suficiente aos dados pessoais (UNIÃO EUROPEIA, 2015). O pedido está inserido no cenário de questionamentos da eficácia das decisões de adequação da Comissão Europeia, diante dos escândalos do caso Snowden relativos à vigilância eletrônica justificada para fins de inteligência e segurança nacional (RODRIGUES ARAÚJO, 2017, p. 214). Estava em questão, portanto, o reconhecimento da adequação de um sistema jurídico como suficiente à proteção de dados pessoais.

Ainda com fundamento na Diretiva 95/46/CE, a Comissão poderia decidir sobre a adequação do nível de proteção de dados pessoais de um Estado não membro da União Europeia. Com a finalidade de garantir os níveis apropriados de proteção e de reduzir as incertezas entre as partes, EUA e União Europeia firmaram o acordo *Safe Harbor* em 2000, posteriormente aprovado pela Decisão 2000/50/EC.[81] No entanto, devido à divulgação de informações por parte de Edward Snowden, em 2013, as garantias ofertadas pelo acordo *Safe Harbor* passaram a ser questionadas. Por essa razão, em 2015, o Tribunal de Justiça da União Europeia, no Caso C-362/14, reconheceu que o acordo não é suficiente para assegurar o nível adequado de proteção e, portanto, decidiu por invalidar a decisão 2000/520 e inviabilizar a continuidade do acordo *Safe Harbor* com os EUA (UNIÃO EUROPEIA, 2015).

De acordo com Rodrigues Araújo, o Tribunal concluiu que um regime jurídico que permita às autoridades públicas de determinado Estado o acesso generalizado às informações pessoais de cidadãos europeus "deve ser considerada lesiva do conteúdo essencial do direito fundamental ao respeito da vida privada [...]" (RODRIGUES ARAÚJO, 2017, p. 223).

Em 2016, a Comissão Europeia, por meio da Decisão n.º 2016/1250, substituiu o acordo *Safe Harbor* para viabilizar juridicamente a transferência de dados com os EUA (UNIÃO EUROPEIA, 2016). Trata-se do *EU-US Privacy Shield*, desenvolvido pelo Colégio dos Comissários para fornecer nova decisão de adequação no âmbito das relações entre União Europeia e EUA (RODRIGUES ARAÚJO, 2017, p. 225).

Schrems, por sua vez, reformulou seu pedido em 2015, alegando que o direito estadunidense exigia da companhia *Facebook Inc.* que os dados pessoais a ela transferidos fossem colocados à disposição das autoridades dos EUA. Sob tal justificada, Schrems argumentava que estes dados pessoais estariam sendo utilizados em programas de vigilância. O Tribunal de Justiça da União Europeia, em 2020, reconheceu que a Decisão de Execução 2016/1250 é inválida (UNIÃO EUROPEIA, 2020).

Dilon Swensen conclui sobre o impacto das decisões:

---

[81] Sobre o acordo *Safe Habor*, trata-se de solução encontrada pela Comissão europeia e pelo Departamento de Comércio dos EUA para resolver as diferenças relativas à proteção de dados. Para tanto, foram estabelecidos os seguintes princípios a serem seguidos pelas organizações estadunidenses, nos termos de Kittichaisaree: The Principles are (a) Notice – Individuals must be informed that their data is being collected and about how it will be used; (b) Choice – Individuals must have the option to opt out of the collection and forward transfer of the data to third parties; (c) Onward Transfer – Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles; (d) Security – Reasonable efforts must be made to prevent loss of collected information; (e) Data Integrity – Data must be relevant and reliable for the purpose it was collected for; (f) Access – Individuals must be able to access information held about them, and correct or delete it if it is inaccurate; and (g) Enforcement – There must be effective means of enforcing these rules. In short, this mutual recognition mechanism is based on private sector certification of companies' privacy practices, enforced by the US Federal Trade Commission (KITTICHAISAREE, 2017, p. 73).

> Se Schrems I estabeleceu os padrões pelos quais todas as futuras decisões de adequação europeias seriam julgadas, Schrems II serve como um aviso: a equivalência essencial não pode ser alcançada por meio de pequenas revisões em um tratado (SWENSEN, 2020, p. 50).[82]

Segundo Maria Helen Murphy, o Tribunal reafirmou que a validade da decisão de adequação depende de que o país receptor dos dados possua um nível de proteção de dados pessoais suficiente e, ao mesmo tempo, reconheceu que as possibilidades de uso de dados para finalidades de vigilância tendem a tornar a decisão cada vez mais complexa. No mesmo sentido, se o nível de proteção não se mostrar suficiente ao longo do tema, o próprio sistema europeu poderá cancelar a decisão do reconhecimento de adequação (MURPHY, 2022).

De acordo com Rodrigues Araújo:

> O acórdão Schrems, ao esclarecer que o princípio do nível de proteção adequada exige ao país terceiro assegurar, efetivamente, um nível de proteção das liberdades e direitos fundamentais substancialmente equivalente ao conferido dentro da UE, permite uma flexibilidade aos meios a que esse país pode recorrer para assegurar tal nível de proteção. Desta forma, preserva-se uma certa margem de abertura para adaptar as apreciações de adequação às diferentes culturas e tradições jurídicas (RODRIGUES ARAÚJO, 2017, p. 223).

Nos termos de João Marques, a decisão do Tribunal reforça a ideia de "portabilidade" global dos direitos fundamentais reconhecidos pela União Europeia aos seus cidadãos. Conforme destaca Marques, as transferências de dados pessoais ainda fazem parte de um regime incerto, uma vez considerada a volatidade das decisões de reconhecimento de adequação do nível de proteção de dados e a ausência de instrumento jurídico global sobre o tema (MARQUES, 2016, p. 69-70).

Observa-se, portanto, que há um desafio em termos de adequação da legislação interna brasileira aos parâmetros internacionais, notadamente aqueles estipulados no âmbito da União Europeia pela Diretiva n.º 680/2016. A harmonização do ordenamento jurídico brasileiro com o sistema europeu de proteção de dados pode ser considerada como um elemento essencial para a participação nos fluxos internacionais de dados em matéria de investigação criminal (VIOLA; HERINGER; CARVALHO, 2021, p. 9-10). E, dessa forma, a garantia de adequação pode ser compreendida como mecanismo de redução dos riscos inerentes às transferências internacionais de dados pessoais.

Sobre esse aspecto, Viola, Heringer e Carvalho assinalam:

> O regramento sobre transferência internacional de dados pessoais previsto na LGPD Penal deve ser enxergado, portanto, como um meio de viabilizar a integração do Brasil aos fluxos de transferências internacionais, além de ser uma garantia de

[82] Tradução livre do original: If Schrems I set the standard by which all future European adequacy decisions would be judged, Schrems II serves as a warning: essential equivalence cannot be met by minor revisions to a treaty (SWENSEN, 2022, p. 50).

> respeito aos direitos fundamentais dos cidadãos brasileiros e dos estrangeiros que vivem no país. O indivíduo não deve ser instrumentalizado em nome de atender interesses coletivos, por mais relevantes que estes sejam. Entende-se, portanto, que há ferramentas que podem auxiliar na harmonização entre o dever legítimo das autoridades com os direitos fundamentais dos indivíduos e o alcance global da Internet - sem desconsiderar as dificuldades de garantir a efetividade dessa (VIOLA; HERINGER; CARVALHO, 2021, p. 10).

Conforme já delineado, o livre fluxo de dados pessoais com países membros da União Europeia depende do reconhecimento de nível adequado de proteção de dados. Este requisito traduz o objetivo de reduzir riscos vinculados ao compartilhamento de dados entre Estados para fins de investigação criminal, bem como para medidas que permitam o acesso transfronteiriço a dados localizados em territórios estrangeiros. Trata-se de medida para promover, portanto, uma reserva de segurança que tutele o direito à privacidade e à proteção de dados pessoais intercambiados ou acessados.

3. O RECONHECIMENTO MÚTUO DE NÍVEL ADEQUADO DE PROTEÇÃO DE DADOS PESSOAIS ENTRE BRASIL E UNIÃO EUROPEIA

O terceiro capítulo desta dissertação tem como objetivo discutir a necessidade de haver instrumento que assegure o reconhecimento mútuo de nível adequado de proteção de dados pessoais entre a União Europeia e o Brasil, com a finalidade de concretizar a possibilidade de acesso transfronteiriço a dados informáticos armazenados, nos termos previstos pela Convenção de Budapeste. Leva-se em consideração, para tanto, o interesse recíproco de se adotar medidas de cooperação internacional para fins de persecução da criminalidade cibernética transnacional.

Com a finalidade de atender ao objetivo proposto deste capítulo, retoma-se o exame da Diretiva n.º 2016/680 da União Europeia, acrescida da Convenção de Budapeste, de 2001, enquanto fontes primárias, de modo a esclarecer quais são os requisitos para o acesso transfronteiriço de dados, no âmbito do compartilhamento de dados pessoais com Estado não membro da integração europeia. Ademais, avalia-se também as decisões de adequação da União Europeia para a Argentina (2003) e o Uruguai (2012), dada a relevância destes país à integração regional brasileira, bem como para o Canadá (2001), Andorra (2010), Israel (2011) e Japão (2019), todos esses sendo partes da Convenção de Budapeste e não membros da União Europeia.

Assim sendo, divide-se este capítulo em 3 momentos: a) inicialmente, será analisada a Convenção de Budapeste, com ênfase nos institutos de cooperação internacional em matéria penal; b) na sequência, examina-se as supramencionadas decisões de adequação da União Europeia associadas ao reconhecimento mútuo de nível de proteção de dados pessoais, com foco a sua aplicação para fins penais; c) por fim, busca-se discutir a necessidade de reconhecimento mútuo para a concretização da possibilidade de acesso transfronteiriço a dados informáticos armazenados.

3. 1 A CONVENÇÃO DE BUDAPESTE.

A Convenção de Budapeste, de 2001, é o principal instrumento internacional voltado especificamente ao fortalecimento da cooperação jurídica internacional para o enfrentamento da criminalidade cibernética. Para os fins aos quais se propõe esta pesquisa, é necessário avaliar os mecanismos de cooperação previstos na Convenção, notadamente o auxílio mútuo.

No primeiro item deste capítulo, para tanto, aborda-se 3 aspectos: a) a cooperação internacional para o combate ao cibercrime, de maneira geral; b) o instituto de auxílio mútuo,

enquanto possibilidade inserida dentro do rol de instrumentos de cooperação jurídica internacional; c) os mecanismos de auxílio mútuo previstos na Convenção de Budapeste, com ênfase à possibilidade de acesso transfronteiriço a dados informáticos armazenados.

3.1.1 A cooperação internacional para enfrentamento do cibercrime.

A partir dos capítulos anteriores, observou-se que a criminalidade cibernética possui caráter transnacional, na medida em que não se limita às fronteiras territoriais de apenas um Estado. A partir desta premissa, entende-se que a política criminal direcionada ao enfrentamento dos crimes cibernéticos deve ter como um de seus princípios ordenadores a cooperação internacional.

Na persecução de um crime cuja conduta, o resultado ou as evidências produzidas podem alcançar mais de uma jurisdição, a realização de diligências para além da jurisdição de determinado Estado pode ser necessária. Nesta hipótese, a interação entre os Estados para solucionar as consequências da multiplicidade de jurisdições interessadas é fundamental para concretização da tutela penal. Para tanto, "é essencial que existam instrumentos que viabilizem a cooperação jurisdicional internacional" (TIBURCIO; DOLINGER; 2010, p. 833).[83]

Dessa forma, segundo Paulo Abrão Pires Júnior, a efetividade na realização da justiça, em um contexto em que cada vez mais os Estados e as populações se conectam entre si, depende de atuação colaborativa e proativa entre as entidades estatais.[84] À medida que as

[83] De acordo com Robert Zimmermann: "La répression des crimes et des délits est l'un des attributs caractéristiques de la souveraineté étatique. On pourrait même dire que la justice pénale est le dernier bastion où l'État peut prétendre être encore pleinement souverain. Son action est libre de toute entrave lorsque sa compétence répressive est acquise, que les personnes poursuivies se trouvent sur son territoire et les moyens de preuve à sa disposition. Son action n'est pas libre lorsque la personne recherchée ou les moyens de preuves à sa disposition. Son action n'est pas libre lorsque la personne recherchée ou les moyens de preuve se trouvent sur le territoire d'un autre État; la poursuite pénale se heurte alors à la souveraineté étrangère. Pour surmonter cet obstacle, les États se prêtent une assistance mutuelle, selon les règles qu'ils définissent. Cette coopération est accordée en application des traités. À défaut de traité, elle est octroyée au regard du droit interne de l'État à qui la demande est adressée, aux conditions qu'il prévoit. En l'absence de traité, aucun principe general du droit international n'oblige un État d'aider un autre à la répression du crime" (ZIMMERMANN, 2009).

[84]Vermeulen, De Bondt e Ryckman argumentam que é possível verificar a tendência de que a cooperação internacional em matéria penal estaria se processando cada vez mais de forma horizontalizada. Isto é, a tomada de decisões e as medidas de cooperação empreendidas ocorreriam em níveis descentralizados, sem que seja necessária a participação direta de autoridade central (VERMEULEN; DE BONDT; RYCKMAN, 2012, p. 185-195). É relevante apontar, contudo, que se trata de perspectiva diversa à noção de horizontalidade da sociedade internacional, lastreada na premissa de que inexiste um poder soberano superior aos Estados e que estes, portanto, relacionam-se juridicamente como iguais uns com os outros. Nesse sentido: Isso significa, basicamente, que apesar das diferenças de natureza econômica, social, política ou de qualquer outro gênero, os Estados, exatamente por serem soberanos e juridicamente iguais, podem produzir direito internacional e destinar a norma a eles próprios. Portanto, à luz do direito internacional, a igualdade entre os membros da sociedade internacional significa que a soberania deve ser entendida como a capacidade de se relacionar entre pares. Ela é, assim, o

relações jurídicas ultrapassam as fronteiras de um Estado soberano, torna-se mais necessário "cooperar e pedir a cooperação de outros Estados para que se satisfaça as pretensões por justiça do indivíduo e da sociedade" (JÚNIOR, 2012, p. 17-21)

Inicialmente, é necessário definir os termos relativos à cooperação internacional em matéria penal. Segundo Karl Härter, o Direito Penal Transnacional é o "sistema que busca conter atividades nocivas que ultrapassam ou que ameaçam ultrapassar fronteiras" estatais. Trata-se, portanto, dos regimes jurídicos que englobam a jurisdição de mais de um Estado para fins de aplicação de medidas judiciais ou administrativas destinadas à contenção de um ilícito transfronteiriço (HÄRTER, 2019, p. 2-3). A cooperação internacional está inserida no conceito amplo de Direito Penal Transnacional, nos termos de Härter, ou no de Direito Penal Internacional (SILVA, 2013, p. 56-59).[85]

Marco Bruno Miranda Clementino destaca dois fundamentos que são complementares no âmbito da cooperação jurídica internacional. Em primeiro lugar, verifica-se que o fundamento reside no interesse de promoção da justiça, com vistas à redução de controvérsias na sociedade e ao respeito ao processo. Na sequência, por outra perspectiva, o fundamento decorre da própria razão de ser do Direito Penal Internacional, baseada no pressuposto de que alguns crimes ultrapassam as fronteiras estatais e, por esse motivo, demandam mecanismos adaptados às suas particularidades (CLEMENTINO, 2013, p. 26-27).

Härter compreende 2 estímulos opostos que circundam o Direito Penal Transnacional: por um lado, há o impulso de contenção dos crimes transfronteiriços por meio da cooperação internacional em matéria penal; por outro, a coordenação entre Estados soberanos, a manutenção da integridade territorial e os direitos humanos se apresentam como freios à persecução penal a nível internacional (HÄRTER, 2019, p. 2-3).

A partir de perspectiva procedimental, a cooperação internacional em matéria penal, de acordo com Denise Neves Abade, é compreendida como o "conjunto de medidas e mecanismos pelos quais os órgãos competentes dos Estados solicitam a prestam auxílio

---

elemento que permite conferir a uma norma o seu selo jurídico, a sua autoridade e a sua legitimidade (CALDEIRA BRANDT, p. 35-38).

[85] Segundo Antonio Cassese, o direito internacional penal é: [...] a body of international rules designed both to proscribe international crimes and to impose upon States the obligation to prosecute and punish at least some of those crimes. It also regulates international proceedings for prosecuting and trying persons accused of such crimes. The first limb of this body makes up substantive (CASSESE, 2003, p. 15). Cassese esclarece que as tradições jurídicas francesas, germânicas, italianas e espanholas fazem a distinção terminológica de direito penal internacional (*criminal international law* ou *droit penal international*), fazendo referência especificamente ao campo jurídico ligado ao papel das cortes nacionais no que tange a criminalidade internacional, incluindo os mecanismos de cooperação internacional para o enfrentamento de crimes (CASSESE, 2003, p. 15).

recíproco para realizar, em seu território, atos pré-processuais ou processuais que interessem à jurisdição estrangeira na esfera criminal" (ABADE, 2013, p. 22). Assim sendo, trata-se do:

> [...] Conjunto de atividades processuais (cuja projeção não se esgota na simples forma), regulares (normais), concretas e de diverso nível, cumpridas por órgãos jurisdicionais (competentes) em matéria penal, pertencentes a distintos Estados soberanos que convergem em nível internacional (funcional e necessariamente), na realização de um mesmo fim, que não é senão o desenvolvimento (preparação e consecução) de um processo (principal) da mesma natureza (penal), dentro de um estrito marco de garantias, conforme o diverso grau e projeção intrínseco do auxílio requerido (CERVINI; TÁVARES, 2000, p. 51).

Observando o fenômeno da cooperação internacional em matéria penal a partir de outro ângulo, menciona-se a contribuição de Gerhard Mueller:

> A assistência judicial internacional, também referida como como a cooperação judicial internacional, é definida como [...] a ajuda prestada por uma nação a outra em auxílio a um procedimento judicial ou quase-judicial em curso no país receptor. [...] A assistência judicial internacional é construída para neutralizar a frustração da política criminal com limitações territoriais de jurisdição criminal (MUELLER, 1965, p. 414).[86]

Para Nádia de Araújo, a cooperação jurídica internacional significa, em sentido amplo:

> [...] o intercâmbio internacional para o cumprimento extraterritorial de medidas demandadas pelo Poder Judiciário de outro Estado. Isso porque o Poder Judiciário sofre uma limitação territorial de sua jurisdição – atributo por excelência da soberania do Estado, e precisa pedir ao Poder Judiciário de outro Estado que o auxilie nos casos em que suas necessidades transbordam de suas fronteiras para as daquele (ARAÚJO, 2012, p. 33-34).

Em consonância com Clementino, pressupõe-se, adiante, que a cooperação jurídica internacional se materializa a partir de algum intercâmbio entre Estados igualmente soberanos, que se relacionam segundo uma lógica de coordenação. Para o autor, a cooperação tem como premissas fundamentais o respeito à soberania de cada Estado, bem como o "reconhecimento da juridicidade da atuação do Estado que a requer" (CLEMENTINO, 2013, p. 22). Nesse sentido, a cooperação jurídica internacional é frequentemente objeto de tratados internacionais, que visam a estabelecer regras uniformes voltadas à temática entre os Estados e organizações internacionais envolvidos. A uniformização das regras é fundamental para garantir maior velocidade e maior abrangência às medidas executados no curso da cooperação (ARAÚJO, 2012, p. 35).[87]

---

[86] Tradução livre da versão original: "International judicial assistance, also referred to as international judicial cooperation, is defined as '[...] aid rendered by one nation to another in support of judicial or quasi-judicial proceedings in the recipient country´s tribunals. [...] International judicial assistance in criminal matters is designed to counteract frustration of criminal policy by territorial limitations of criminal jurisdiction (MUELLER, 1965, p. 414).

[87] De acordo com Clementino: [...] é possível afirmar que a cooperação jurídica internacional em matéria penal: i) é jurídica, porque atende à necessidade de um processo penal, ainda que este não tenha sido instaurado e

É possível argumentar que nenhum Estado pode ser obrigado, com fundamentação em princípios de Direito Internacional, a se empenhar em mecanismos de cooperação jurídica internacional em matéria penal. Trata-se de perspectiva clássica sobre o interesse e o dever de cooperar de um Estado. Contudo, diante da criminalidade transnacional e do aumento da interdependência dos Estados no âmbito da persecução penal, ganha força a perspectiva de que os sujeitos de Direito Internacional possuem a obrigação de cooperar para a promoção da justiça (ZIMMERMANN *apud* CLEMENTINO, 2013, p. 27-28).

Sobre este aspecto, Antonio Cassese, em obra publicada em 2003, observando da prática dos Estados, verifica que não há no direito internacional consuetudinário a presença de normas que obriguem os Estados a exercer suas funções jurisdicionais em matéria de persecução criminal. Todavia, o autor já vislumbrava a possibilidade de haver norma costumeira internacional em relação ao crime de terrorismo, devendo os Estados promover o processamento criminal e o julgamento dos indivíduos ou, caso contrário, extraditá-los a outro Estado interessado (CASSESE, 2003, p. 361-362).[88]

Para além da discussão sobre obrigatoriedade da cooperação jurídica internacional em matéria penal, em atenção à contribuição de Karl Loewenstein, Abade destaca que os Estados cooperam entre si por conta de motivos pragmáticos. Por este ponto de vista, considera-se que a consecução do interesse nacional – entre os quais está inserida a contenção da criminalidade transnacional – exige a cooperação internacional (LOEWENSTEIN *apud* ABADE, 2013, p. 25). A cooperação, nesse caso, depende da decisão soberana de cada um dos Estados envolvidos (AMBOS, 2007).

Diante de tais parâmetros, segundo Abade: "a cooperação ocorrerá se houver a) tratado internacional assim determinado ou b) vontade ad hoc do Estado com base nos conceitos de reciprocidade e do tradicional *comitas gentium*", que pode ser compreendo como a cortesia internacional pautada na prática dos Estado (ABADE, 2013, p. 28).

---

mesmo após sua conclusão; ii) internacional, porque implica uma medida extraterritorial, a ser efetivada no território de outro Estado, exigindo articulação de soberanias; iii) é penal, porque tem por objeto a persecução do crime com elementos de estraneidade (CLEMENTINO, 2013, p. 26).

[88] É relevante destacar o papel da Organização das Nações Unidas no fomento e na institucionalização da cooperação internacional, considerada em sentido amplo. Conforme explica Abade, a *soft law* desenvolvida no âmbito da ONU evidencia a importância atribuída à cooperação internacional, com ênfase à Resolução 2625 de 1970, sobre as relações amistosas e cooperação entre Estados, em conformidade com os princípios da Carta da ONU (ABADE, 2013, p. 31). A Declaração de Princípios estabelece: States have the duty to co-operate with one another, irrespective of the differences in their political, economic and social systems, in the various spheres of international relations, in order to maintain international peace and security and to promote international economic stability and progress, the general welfare of nations and international co-operation free from discrimination based on such differences (ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS, 1970).

A importância da cooperação internacional no ordenamento jurídico brasileiro está presente já nos artigos iniciais da Constituição Federal. O artigo 4º, inciso IX, da Carta de 1988, estabelece a cooperação entre os povos para o progresso da humanidade como um dos princípios regentes do Brasil em suas relações internacionais (BRASIL, 1988). Embora a ênfase na cooperação internacional esteja presente no texto constitucional, a perspectiva adotada pelo Brasil é voluntarista, de modo que a concretização da cooperação deve estar fundamentada em acordo prévio entre as partes ou em promessa de reciprocidade (ABADE, 2013, p. 32).

Fundamental para a exigência de cooperação internacional, conforme visto até então, a natureza transnacional dos crimes cibernéticos é elemento importante que deve ser aprofundado. Os crimes cibernéticos podem ser praticados em determinada localidade, no entanto, os efeitos da conduta podem ser materializados em espaços diversos. Ao mesmo tempo, "vestígios" da conduta criminosa, como dados de tráfego, podem estar armazenados em servidores localizados em outras jurisdições. Cita-se, a título exemplificativo, a hipótese de um vírus de computador, possuindo a capacidade de comprometer a disponibilidade de dados inseridos em um sistema informático, pode contaminar diversos sistemas espalhados em múltiplas localidades (DELGADO, 2007, p. 30).

Os crimes cibernéticos, portanto, podem facilmente ultrapassar as tradicionais fronteiras físicas dos Estados. Santos destaca que mais de 50% dos crimes cometidos na internet envolve algum elemento transnacional (SANTOS, 2018, p. 168). Ademais, conforme já brevemente mencionado, quase metade dos crimes cibernéticos praticados no Brasil são originados de condutas praticadas fora do território nacional (EUROPOL *apud* OCDE, 2020, p. 108).

No mesmo sentido:

> À medida que a maior parte da informação mundial está agora armazenada digitalmente, é difícil imaginar uma investigação criminal que não envolva evidências digitais. Atualmente, evidências criminais não são apenas digitais, mas também desafiam as noções tradicionais de geografia e de jurisdição territorial. Devido à ubiquidade da computação em nuvem, onde o armazenamento local no equipamento do usuário final deu lugar ao armazenamento remeto, os dados que antes eram armazenados localmente e acessíveis sob procedimentos domésticos agora estão frequentemente nas mãos de empresas privadas e armazenados em jurisdições fora do Estado investigador (ABRAHA, 2021, p. 121).[89]

[89] Tradução livre da versão original: As most of the world's information is now stored digitally, it is hard to imagine a criminal investigation that does not involve digital evidence. Criminal evidence today is not only digital but also defies traditional notions of geography and territorial jurisdiction. Due to the ubiquity of cloud computing, where local storage in end-user equipment has given way to remote storage, data that was once stored locally and accessible under domestic procedures is now often in the hands of private companies and stored in jurisdictions outside the investigating country (ABRAHA, 2021, p. 121).

Considerando o expressivo caráter transnacional dos crimes cibernéticos, torna-se relevante examinar a iniciativa da Convenção de Budapeste, de 2001, sobre cibercrime. Neste tópico, com o objetivo de examinar a previsão normativa dos crimes cibernéticos, ressalta-se o esforço da Convenção de Budapeste.

Desde a década de 1980, consoante constatação de Jonathan Clough, grupos de trabalhos de organizações internacionais como a ONU, a OCDE, o Conselho da Europa, o G8 e a Interpol adicionaram aos seus estudos a preocupação com a criminalidade cibernética e o seu alcance global. Defendia-se, para tanto, que seria necessário haver algum nível de harmonização legislativa entre os Estados para se promover de maneira mais efetiva a persecução penal. Para o autor, tal harmonização é relevante justamente para incrementar e facilitar as trocas de informações entre instituições públicas e privadas, bem como para viabilizar a cooperação internacional em matéria penal (CLOUGH, 2010, p. 21-24).

A Convenção sobre o Cibercrime do Conselho da Europa, de 2001, adotada em Budapeste, foi aberta à assinatura – e, posteriormente, à adesão – tanto aos Estados-membros da referida organização, como para Canadá, Japão, África do Sul e Estados Unidos, os quais também integraram as discussões para elaboração da Convenção (ALVES, 2020, p. 24). O tratado foi aberto a assinatura em 23 de novembro de 2001 e entrou em vigor em 01 de julho de 2004, após a 5ª ratificação (sendo pelo menos 3 de membros do Conselho da Europa). Em 05 de fevereiro de 2023, a Convenção contava com 68 partes, além de 15 outros Estados que apenas assinaram ou que foram convidados a aceder (CONSELHO DA EUROPA, 2022).

Nos termos do relatório explicativo da Convenção, os objetivos principais do instrumento são:

> (1) Harmonizar os elementos do direito penal substantivo doméstico relacionados às ofensas e previsões conexas na área do cibercrime, (2) fornecendo ao direito penal processual doméstico os poderes necessários para investigação e a persecução dessas ofensas, assim como de outras cometidas por meio de um sistema de computador, ou de evidências em forma eletrônica, (3) estruturando um regime rápido e efetivo de cooperação internacional (CONSELHO DA EUROPA, 2001-B).[90]

Segundo a nota à imprensa nº 309 de 2019, publicado pelo Ministério de Relações Exteriores, o Brasil foi convidado pelo Comitê de Ministros do Conselho da Europa para aderir à Convenção de Budapeste. O processo de adesão teve início em julho de 2019, quando o governo brasileiro expressou a vontade de aderir ao mecanismo (BRASIL, 2019). O Senado

[90] Tradução livre da versão original: 16. The Convention aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation (CONSELHO DA EUROPA, 2001-B).

Federal aprovou em 15 de abril de 2021 a adesão do Brasil à Convenção (BRASIL, 2021). Em novembro de 2022, o Brasil procedeu o depósito do instrumento formal de adesão à Convenção junto ao Conselho da Europa (BRASIL, 2022).

Conforme Damásio de Jesus e José Antônio Milagre apontam, uma das finalidades da Convenção de Budapeste é estabelecer diretrizes às políticas nacionais e, a partir destas, sugerir formas de harmonização das legislações domésticas de cada Estados, visando o aprimoramento o enfrentamento aos crimes cibernéticos (JESUS; MILAGRE, 2016, p .55).

Esse aspecto se torna relevante, de acordo com Delgado, na medida em que as condutas definidas nominalmente como "crimes informáticos" não representam um conjunto homogêneo de fatos. Dessa forma, as legislações internas dos Estados não contemplam as mesmas condutas quando se referem especificamente aos crimes praticados pela via informática, e tampouco apresentam terminologias similares para a denominação destes. Há, por consequência, diferenças em relação à tipificação adotada (DELGADO, 2007, p. 22). Segundo argumentou Castro, o fato de o Brasil não ser signatário da Convenção de Budapeste, até o momento em que escreveu, é determinante para que se verifique um "fraco arcabouço de proteção contra os crimes cibernéticos" no ordenamento jurídico doméstico (CASTRO, 2018, p. 121).

Roberto Chacon de Albuquerque aduz que algumas condutas são de relativo consenso a nível internacional, tais quais o estelionato praticado pela via informática, a violação de informações sigilosas, as condutas que atentam contra a segurança de sistema informático ou que produzem danos contra o sistema informático, mas outras ainda são objeto de dissenso no campo da tipificação, como a espionagem informática ou a utilização não autorizada de sistemas informáticos (ALBUQUERQUE, 2006, p. 30). Diante da complexidade de se definir todo o rol de condutas qualificadas como cibercriminosas, a Convenção de Budapeste apresentou importante avanço no esforço de tipificação e de harmonização normativa.

De acordo com David Alexandre Ribeirinho Alves, a Convenção é uma referência importante para fins de harmonização mesmo para Estados que não são formalmente partes do instrumento. O autor menciona, para fins de exemplificação, países como Argentina, [91] Botsuana, Egito, Filipinas, Nigéria e Paquistão. Atualmente, cerca de metade dos Estados membros da Organização das Nações Unidas desenvolveram legislações com inspiração nas soluções de tipificação apresentadas pela Convenção (ALVES, 2020, p. 24).

[91] É relevante ressaltar que, atualmente, a Argentina faze parte da Convenção de Budapeste.

A seção 1 do Capítulo 2 da Convenção de Budapeste apresenta proposta de tipificação penal dos crimes cibernéticos em categoria. São elas, na ordem prevista pela Convenção: a) o título 1 apresenta as infrações contra a confidencialidade, integridade e disponibilidade de sistemas e da dos informáticos; b) o título 2 trata das infrações relacionadas a computadores; c) o título 3 diz respeito às infrações relacionadas ao conteúdo; e d) o título 4 apresenta tipificações às infrações relacionadas a violações de direito autoral e direitos conexos. Em cada título há disposição informando que as partes deverão adotar as medidas legislativas necessárias para consolidar a tipificação penal de acordo com as modalidades sugeridas pela Convenção, levando em consideração o seu ordenamento jurídico interno (CONSELHO DA EUROPA, 2001-A).

O título 1 indica as seguintes modalidades de infração penal: (a) acesso ilegítimo; (b) interceptação ilegítima; (c) interferência em dados; (d) interferência em sistemas; e (e) uso abusivo de dispositivos. O título 2 apresenta os tipos penais de (a) falsidade informática e (b) burla informática. No título 3, constam como tipos penais as infrações relacionadas à pornografia infantil. Por fim, no título 4 estão mencionadas as infrações relacionadas à violação do direito e autor e dos direitos conexos, de maneira ampla. (CONSELHO DA EUROPA, 2001-B).

Com a finalidade de concluir esta seção, destacam-se duas conclusões preliminares sobre os crimes cibernéticos: em primeiro lugar, a importância atribuída aos dados e informações armazenados em sistemas informacionais e bancos de dados – a nível de coleta, armazenamento, processamento e transferência – em sua relação com os crimes cibernético. Em segundo lugar, a natureza transnacional dos crimes cibernéticos propiciada pela alta conectividade em escala global e pela difusão dos meios tecnológico-informacionais.

Para Sieber, os dados informacionais correspondem ao principal objeto dos crimes cibernéticos. Ao mesmo tempo, são figuras caracterizadas por uma rápida mobilidade, de modo que um enorme volume de dados possa percorrer grandes distância em pouco tempo. Neste movimento, os dados frequentemente ultrapassam as fronteiras físicas dos Estados (SIEBER, 1998, p. 32).

A rápida velocidade do movimento de dados computacionais em redes globais faz com que seja necessário que o enfrentamento dos crimes cibernéticos tenha soluções internacionais, pautadas na cooperação internacional. A falta de diálogo entre os Estados sobre a matéria poderia produzir, na terminologia adotada por Sieber, “paraísos para crimes cibernéticos” e maiores restrições ao fluxo de dados e informações. Respostas empreendidas unilateralmente por um Estado não seriam capazes acompanhar a alta velocidade de

informações produzidas no ciberespaço. Por conseguinte, a contenção dos crimes cibernéticos não possuiria o alcance ou os meios necessários para atender de maneira eficaz a sua finalidade (SIEBER, 1998, p. 33).

Sobre esse aspecto, Sieber acrescenta:

> Portanto, o caráter internacional das redes de computadores exige a cooperação internacional de polícias e de autoridades judiciárias. A condição para essa cooperação internacional é a de que a polícia e as outras autoridades competentes disponham de poderes adequados ou similares previstos pela legislação nacional. Dentro dos acordos de cooperação policial e de assistência mútua, Estados podem apenas garantir medidas que sejam admissíveis dentro da legislação nacional. Dessa forma, é do interesse internacional que os sistemas jurídicos de todos os Estados contenham não apenas previsões legais harmonizadas, mas também disposições adequadas de processo criminal, especialmente no que tange os poderes coercitivos (SIEBER, 1998, p. 132-133).[92]

Embora a cooperação internacional seja importante, conforme já delineado, questiona-se a possibilidade de se alcançar um nível amplo de consenso entre os Estados. Segundo Clough, a regulação de aspectos criminais, assim como dos usos da internet e das novas tecnologias, é matéria em que não há amplo consenso em escala internacional. No entanto, a Convenção de Budapeste deve ser compreendida como um avanço importante para fins de harmonização legislativa na esfera do enfrentamento dos crimes cibernéticos (CLOUGH, 2010, p. 21-24).[93]

A Convenção de Budapeste, objeto central para esta pesquisa, elenca como possibilidades de cooperação a extradição e o auxílio mútuo. O instrumento prevê, dentre as possibilidades de cooperação internacional a nível de assistência jurídica mútua (capítulo III, seção 2, títulos 1 e 2), a conservação e divulgação de dados informáticos; o auxílio mútuo para acesso a dados informáticos armazenados; o acesso transfronteiriço a dados armazenados em computador, mediante consentimento ou quando se trate de dados acessíveis ao público; auxílio mútuo para recolha, em tempo real, de dados de tráfego; auxílio mútuo para a interceptação de dados de conteúdo (CONSELHO DA EUROPA, 2001-A).

---

[92] Tradução livre. Na versão original: Thus, the international character of computer networks calls for international co-operation of police and law-enforcement authorities. The precondition for such an international co-operation is that police and other law enforcement authorities dispose of adequate and similar powers on the basis of national law. Under all agreements on police co-operation and mutual assistance, states can only provide measures which are admissible under their national law. Thus, there is an international interest that the legal systems of all countries contain not only harmonized provisions in the field of substantive law, but also adequate criminal procedural law provisions, especially in the field of coercive powers (SIEBER, 1998, p. 132-133).

[93] Sobre o assunto, Clough esclarece: While some level of consensus may be achieved in respect of offences against the person and property, crimes against the state and crimes against morality are more problematic. Some countries may even see opportunities to establish themselves as ‘data havens’, providing maximum privacy and minimal regulation of content hosted there. For others, particularly in the developing world, cybercrime may simply not be a priority (CLOUGH, 2010, p. 21-22).

Objetiva-se avaliar o mecanismo de acesso transfronteiriço a dados armazenados em computador, classificado na Convenção como modalidade de auxílio mútuo, levando em consideração, ademais, a maneira como este seria recepcionado no ordenamento jurídico brasileiro. Para tanto, faz-se necessário avaliar, preliminarmente, o enquadramento jurídico do auxílio mútuo no Brasil.

3.1.2 O instituto de auxílio mútuo na cooperação internacional em matéria penal.

O instituto do auxílio mútuo representa uma possibilidade de cooperação internacional em matéria penal. Passa-se a abordar, neste capítulo, a forma pela qual este instrumento está inserido no ordenamento jurídico brasileiro, com vistas a esclarecer, posteriormente, as perspectivas para a eventual coordenação com outros Estados a fim de concluir objetivos comuns, sobretudo a partir das iniciativas da Convenção de Budapeste.

Abade utiliza a seguinte classificação das medidas de cooperação jurídica internacional: a) realizada pela via diplomática; b) pela via da autoridade central; e c) pela via do contato direto. A primeira é realizada por meio dos canais permanentes de comunicação entre os Estados, ainda que estes não sejam propriamente especializados na cooperação jurídica. A segunda, adiante, é baseada em órgão previsto em tratado internacional com competência específica para empreender os procedimentos de cooperação jurídica. A terceira, por fim, é realizada por meio do contato direto entre os órgãos interessados, de modo que não haja intermediação dos agentes diplomáticos ou da autoridade central designada (ABADE, 2013, p. 35-37).

Segundo Viviane Ceolin Dallasta Del Grossi, a cooperação jurídica internacional deve ser considerada como um "gênero", do qual são espécies a extradição, a assistência jurídica mútua, a homologação de sentença estrangeira, a transferência de presos e transferência de processos penais (GROSSI, 2014, p. 28). No Manual de Cooperação Jurídica Internacional e Recuperação de Ativos, de 2012, Paulo Abrão Pires Júnior elenca como instrumentos tradicionais de cooperação jurídica internacional as cartas rogatórias, a homologação de sentença estrangeira, os pedidos de extradição e a transferência de pessoas condenadas (JÚNIOR, 2012, p. 17).[94]

Para Nádia de Araújo, os modelos tradicionais de cooperação jurídica internacional são efetivados por meio de cartas rogatórias, da transferência de presos para cumprimento de

[94] No Brasil, o Superior Tribunal de Justiça, desde a Emenda Constitucional n.º 45/04, possui competência originária para o processamento das cartas rogatórias e dos pedidos de homologação de sentença estrangeira realizados por Estados estrangeiros. Em regra, no campo da cooperação jurídica internacional ativa, o Ministério da Justiça é o órgão responsável pelo envio da carta rogatória (ARAÚJO, 2012, p. 38).

pena, bem como do reconhecimento e da execução de sentenças estrangeiras. Na sequência, também se inserem como medidas de cooperação as ações de natureza administrativa ou a representação judicial do Estado estrangeiro, as quais compõem o denominado auxílio direto (ARAÚJO, 2012, p. 38-40).

No domínio penal, a cooperação internacional tradicionalmente era promovida por meio da extradição. No entanto, levando em consideração a expansão da criminalidade transfronteiriça e das novas formas de comissão de crimes, novas medidas passam a ser de interesse das instituições de persecução penal (ARAÚJO, 2012, p. 39).[95]

O Código Modelo de Cooperação Interjurisdicional para Ibero-América, acrescido de sua exposição de motivos, representa contribuição importante para se compreender os instrumentos de cooperação internacional de maneira clara. O artigo 1º do Código, ao definir o seu âmbito de aplicação, dispõe sobre a cooperação entre Tribunais e órgãos administrativos de estados diversos, com a finalidade de assegurar a efetividade da prestação jurisdicional transnacional (CÓDIGO, 2009, p. 445).

O referido Código, no artigo 19, estabelece como modalidades de cooperação interjurisdicional em matéria penal as seguintes: a) citação, intimação e notificação judicial; b) realização de provas e obtenção de informações; c) investigação conjunta; d) comparecimento temporário de pessoas; e) transferência de processo e de execução penal; f) eficácia e execução de decisão penal estrangeira; g) extradição; e h) medida judicial de urgência (CÓDIGO, 2009, p. 449).

Em relação aos procedimentos de cooperação interjurisdicional, o Código também propõe sistematização. Dessa forma, determina, no capítulo IV, os procedimentos de: a) auxílio mútuo; b) carta rogatória; c) ação e incidente de impugnação de eficácia de decisão estrangeira; d) procedimento de execução de decisão estrangeiro; e) procedimento de medida judicial de urgência; e f) procedimentos de extradição (CÓDIGO, 2009, p. 452-456).

Diante dos novos desafios da criminalidade transnacional contemporânea, com o objetivo de se obter respostas mais rápidas, ganha relevância o auxílio direto, também

[95] Observando o cenário da União Europeia para cooperação internacional em matéria penal, Vermeulen, De Bondt e Ryckman recomendam que os isntrumetnos sejam empreendidos por meio de canais descentralizados. Para os autores: There are two main reasons for this position. Firstly, decentralistion allows for political and interstate dimensions to be cut out of cooperation as much as possible, and no detours in cooperation through funnels and buffers hinder cooperation. This fits the spirit behind the introduction of mutual recognition, being that in the European legal sphere a climate of trust exists between all member states. Secondly, apart from the depolitisation of cooperation, horizontalisation carries several other advantages: direct communication between the authorities involved, has a significant influence on the speediness and ease of cooperation. In contrast, communication via central authorities can be complex and cumbersome (VERMEULEN; DE BONDT; RYCKMAN, 2012, p. 185).

denominado assistência direta.[96] Segundo Nádia de Araújo, trata-se da "cooperação efetuada entre autoridades centrais de países-parte de convenções internacionais com previsão para essa modalidade de cooperação [...]" (ARAÚJO, 2012, p. 45-46).[97]

O Código Modelo de Cooperação Interjurisdicional para Ibero-América esclarece que o auxílio mútuo compreende os procedimentos relacionados à "cooperação entre órgãos administrativos de Estados diversos, no intercâmbio de atos ou diligências que objetivem prestação jurisdicional perante o Estado requerente", ou mesmo que não tenham natureza jurisdicional no Estado requerido (CÓDIGO, 2009, p. 452-453). Grossi, em análise do Código, identifica que as medidas de investigação conjunta, comparecimento temporário de pessoas, citação, intimação e notificação judicial e extrajudicial estão compostas no rol de modalidades que não reclamam medida jurisdicional do Estado requerido. A eficácia e execução de sentença de decisão estrangeira, a medida de urgência, a extradição, a transferência de processo e a execução penal, todavia, são caracterizadas como instrumentos que reclamam medida jurisdicional (GROSSI, 2014, p. 24).

Conforme esclarecido por Grossi, o auxílio mútuo – ou auxílio direto[98] – é definido como a medida de "cooperação prestada pela autoridade nacional apta a atender demanda externa, no uso de suas atribuições legais, como se um procedimento nacional fosse, embora

---

[96] Denise Neves Abade verificou a presença do mecanismo de auxílio mútuo em tratados bilaterais e multilaterais: Esse novo veículo é previsto em vários tratados bilaterais de cooperação jurídica internacional em matéria penal, como também em diversos tratados multilaterais que têm por objeto de temas de cooperação jurídica internacional em matéria penal, entre eles o Protocolo de Assistência Jurídica Mútua em Assuntos Penais, a Convenção Interamericana sobre Assistência Mútua em Matéria Penal, a Convenção Interamericana sobre o Cumprimento de Sentenças Penais no Exterior, a Convenção Interamericana contra a Corrupção (com reserva ao § 1º, inciso c, do art. XI), a Convenção Interamericana contra o Terrorismo, a Convenção das Nações Unidas contra a Corrupção, e a Convenção das Nações Unidas contra o Crime Organizado Transnacional (Convenção de Palermo) (ABADE, 2016, p. 13).

[97] O auxílio direto está inserido no campo da cooperação jurídica internacional direta. Segundo Clementino: A cooperação também é classificada quanto ao canal utilizado, subdividindo-se em: i) direta (ou informal); ii) indireta (ou formal). Quanto à primeira, assim se designa a cooperação que se procede diretamente entre as autoridades públicas envolvidas, sem a necessidade do concurso de instâncias formais, como a via diplomática ou mesmo o Poder Judiciário. A cooperação informal comumente tem lugar nas hipóteses em que já existe um canal institucional aberto entre os dois órgãos envolvidos, o que normalmente ocorre entre órgãos como a Interpol e o Grupo de Egmont (que congrega as unidades de inteligência financeira). Por óbvio, a cooperação somente será viável nesse caso se não houver medidas submetidas à reserva de jurisdição ou a algum procedimento formal previsto no direito interno do Estado requerido para assegurar sua validade. É chamada indireta (ou formal), por outro lado, a cooperação realizada em observância aos padrões institucionalmente estabelecidos, como forma de assegurar a validade da providência a ser viabilizada. Esta modalidade tende a ser a predominante quando se se tratar de diligência mais restritiva de direitos, caso em que normalmente são estabelecidos, nas ordens jurídicas estatais, procedimentos mais rigorosos para a respectiva realização (CLEMENTINO, 2013, p. 33).

[98] Sobre a precisão terminológica, Grossi esclarece: no Código Modelo para Iberoamérica, o auxílio direto foi chamado de auxílio mútuo (arts. 32 a 36) e sua natureza jurídica será voluntária (não contenciosa), ao não reclamar jurisdição ou delibação no Estado requerido, conforme considerações da própria exposição de motivos do Código. Entre tribunais será um procedimento judicial de jurisdição voluntária. Nos demais casos, um procedimento administrativo, de acordo com a legislação administrativa do Estado requerido. Trata-se do auxílio mútuo judicial e do auxílio mútuo administrativo (art. 34) (GROSSI, 2014, p. 36).

oriundo de solicitação do Estado estrangeiro encaminhada por intermédio de autoridade central brasileira" (GROSSI, 2014, p. 35).

No pedido de auxílio direto, segundo Paulo Abrão Pires Júnior, leva-se ao conhecimento do juiz de primeira instância diretamente, sem que seja necessário o juízo prévio de delibação do Superior Tribunal de Justiça. A tramitação deste instrumento ocorre por meio da Autoridade Central brasileira, a qual deverá ser determinada nos tratados internacionais de interesse (JÚNIOR, 2012, p. 18).[99]

Nesse sentido, as autoridades centrais de um país, frequentemente inseridas no domínio do Poder Executivo, fornecem o acesso das informações requeridas pelas autoridades centrais de outros Estados. Isto é, por um lado, a própria autoridade central poderá atender diretamente o pedido formulado por sua contraparte na jurisdição estrangeira (VERGUEIRO, 2012, p. 62-64). Por outro, nas hipóteses em que tais informações estejam protegidas por sigilo ou em que seja necessário o cumprimento de diligência que exija formalidade específica do Poder Judiciário, a autoridade central deverá encaminhar o requerimento ao Ministério Público Federal, que tomará as medidas cabíveis a nível judicial (ABADE, 2016, p. 14).

Sobre a maior rapidez dos procedimentos de auxílio direto, Nádia de Araújo ressalta a possibilidade de dispensa da intervenção judicial:

> Nessa nova modalidade, procura-se agilizar os procedimentos de cooperação tradicional, em vista da morosidade a eles associada. Há países, inclusive, que permitem toda a cooperação entre autoridades administrativas. No caso do Brasil, embora o pedido possa ser transmitido diretamente à Autoridade Central brasileira, sempre haverá necessidade da ordem judicial para seu cumprimento. A intervenção judicial pode ser dispensada quando a situação não seja de molde a exigi-la, como por exemplo, se o requerimento for de informações disponíveis sem a necessidade de intervenção judicial (ARAÚJO, 2012, p. 46).

De acordo com Nádia de Araújo, tratando-se de cooperação jurídica internacional em matéria penal, o instituto do auxílio direto tem sido utilizado nas hipóteses em que já há previsão em acordo internacional. A autora, nesse sentido, menciona o Agravo Regimental 3162, no qual o Superior Tribunal de Justiça reconheceu não haver necessidade de juízo de delibação do tribunal em razão de que não havia decisão prévia na origem, de modo que o

[99] Em relação à importância da temática, Paulo Abrão Pires Júnior reforça o aumento da incidência dos pedidos de cooperação internacional na primeira década de 2000: Considerando-se as estatísticas produzidas pelo Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI), verifica-se que de 2004 a 2010, houve incremento de mais de 40% no número de pedidos de cooperação anuais tramitados no Ministério da Justiça. Saiu-se de um patamar de algo em torno de 2800 pedidos em 2004 para mais de 4000 em 2010. Nos primeiros oito meses de 2011, número próximo a 2700 pedidos já foram tramitados, evidenciando a tendência continuamente crescente da cooperação (JÚNIOR 2012, p. 18). Segundo dados do Ministério da Justiça e Segurança Pública, nos últimos dez anos, houve aumento do número de pedidos para fins de cooperação jurídica internacional em matéria penal e civil, com exceção dos anos de 2015 e 2020. Em 2021, a pesquisa contabilizou 6396 novos pedidos, um aumento em relação aos 5579 novos pedidos de 2020, mas ainda inferior aos 7012 novos pedidos de 2019 (BRASIL, 2021).

cumprimento da medida poderia ser realizado por meio do auxílio direto (ARAÚJO, 2012, p. 45-46).

Nesse sentido:

> O Auxílio Direto diferencia-se das demais hipóteses Cooperação Jurídica Internacional tradicionais, por trazer ao interior do Estado Requerido a responsabilidade pela análise do mérito do pedido do Estado Requerente, criando no interior do sistema jurídico requerido um título judicial (ou jurídico lato sensu), que será produzido observando as regras deste sistema, e não dando efetividade a uma decisão produzida no estrangeiro, segundo o ordenamento do Estado Requerente, e que, deste modo, possui maior chance de causar incompatibilidades com a ordem pública do Estado Requerido (VERGUEIRO, 2012, p. 62).

Adiante, no auxílio direto, a força executória do pedido de uma autoridade central não se encontra em uma determinação judicial, mas está fundamentada nos tratados internacionais que vinculam os Estados envolvidos na cooperação jurídica internacional (VERGUEIRO, 2012, p. 64).[100] Este instrumento se singulariza, portanto, em razão de o Estado estrangeiro se apresentar na figura de "administrador, porquanto não encaminha um pedido judicial de assistência, mas sim uma solicitação para que a autoridade de outro Estado tome as providências e as medidas requeridas no âmbito nacional" (GROSSI, 2014, p. 39).[101]

Abade identifica 5 características inerentes ao auxílio direto: a) trata-se de demanda com origem em outro Estado, direcionada às competências do Poder Executivo brasileiro em suas relações internacionais; b) o requerimento emitido pelo Estado estrangeiro é examinado

---

[100] Segundo Grossi: Os pedidos de auxílio direto são, em regra, alicerçados em tratados ou acordos bilaterais (os chamados Mutual Legal Assistance Treaties ou MLATs). Inexistindo ajuste expresso entre os dois Estados, a assistência poderá ser realizada baseando-se na garantia de reciprocidade do requerente. É possível cooperar nos mais diversos temas, como tributário, trabalhista e previdenciário. No entanto, os tratados mais frequentes no cenário internacional versam sobre matéria penal e civil stricto sensu (GROSSI, 2012, p. 39-40).

[101] Com base em análise do cenário de cooperação jurídica em matéria penal no âmbito da integração europeia, Vermeulen, De Bondt e Ryckman argumentam que os atuais mecanismos sugerem maior ênfase nas soluções baseadas no reconhecimento mútuo. Isto é, o regime lastreado nos termos de Tratado de Lisboa estrutura um modelo no qual as requisições de um Estado para outro ascendem ao status jurídico de uma ordem judicial. Os autores evidenciam, entre outras, as características neste sistema: a) a redução da necessidade de consentimento por parte do Estado "requisitado" e o menor parâmetro de necessidade para se justificar a motivação do Estado "requisitante"; b) limitações no que concerne à possibilidade de rejeição da requisição de cooperação; e c) o requerimento para que prazos sejam respeitados (VERMEULEN; DE BONDT; RYCKMAN, 2012, p. 205). No esforço de tradução, optou-se pelo uso de aspas nos termos "requisitado" e "requisitante", tendo em vista que, no modelo apresentado, não se trata propriamente de requisição, mas de eventual ordem. Para os autores: A first characteristic of enhanced stringency is the reduced need for consent of the executing member state. The appropriate term here is indeed 'executing' state: in the mutual recognition instruments, the issuing member states issue an order instead of a request and the requested state becomes the executing state, implying that its consent is not necessary: when an order comes, the state needs to execute. This was different in the traditional cooperation acquis prior to mutual recognition in the sense that in the those, the terminology is 'requesting' and 'requested' member state, indicating that the consent of the requested member is not implied (VERMEULEN; DE BONDT; RYCKMAN, 2012, p. 206). De maneira similar, Viviane Del Grossi explica: O espírito teórico que impulsiona atualmente a cooperação jurídica na União Europeia é a substituição progressiva de um sistema de assistência jurídica, no sentido em que tradicionalmente tem sido entendida (com base em convenções e em tratados bilaterais entre os países), por um conjunto de normas suportado sobre o princípio do reconhecimento mútuo das decisões judiciais (GROSSI, 2014, p. 131).

em relação ao seu mérito nas hipóteses em que exigir alguma prestação judicial para além do exercício da autoridade central; c) é mecanismo nacional, com início em um pedido de Estado estrangeiro; d) o Poder Executivo exerce o papel, enquanto autoridade central, de decidir pelo encaminhamento do pedido de cooperação aos órgãos internos; e e) o tratado internacional que versa sobre o auxílio direto entre o Brasil e o Estado estrangeiro possui a qualidade de *lex specialis*, uma vez que contém previsão sobre mecanismo específico para o pedido de assistência jurídica internacional (ABADE, 2016, p. 13-15).

No cenário jurídico brasileiro, conforme apuração de Grossi, a maior parte dos tratados de assistência jurídica na esfera criminal determinam como autoridade central o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI), órgão vinculado à Secretaria Nacional de Justiça, do Ministério da Justiça (GROSSI, 2014, p. 44-45).[102] No entanto, alguns tratados apresentam exceções: o Tratado de Auxílio Mútuo em Matéria Penal entre o Governo da República Portuguesa e o Governo da República Federativa do Brasil, de 1991, e o Tratado de Assistência Mútua em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo do Canadá estabelecem a Procuradoria-Geral da República como Autoridade Central (BRASIL, 2012-B).

Verificou-se que o auxílio mútuo é caracterizado por um contato direto entre as autoridades competentes no âmbito da cooperação jurídica internacional, com o objetivo de promover o diálogo entre as instituições interessadas de maneira mais ágil. A Convenção de Budapeste, como será visto no próximo item, prevê modalidades específicas para a cooperação jurídica em matéria penal com a finalidade de enfrentar a criminalidade cibernética.

3.1.3 O auxílio mútuo previsto na Convenção de Budapeste.

Divide-se este subitem em 2 momentos principais. Em primeiro lugar, apresenta-se os mecanismos de cooperação jurídica internacional previstos na Convenção de Budapeste. Na sequência, aprofunda-se no exame do instrumento de acesso transfronteiriço a dados informáticos armazenados, o qual encontra centralidade no objeto desta pesquisa.

Conforme já mencionado previamente, embora a modalidade de acesso transfronteiriço possa ser classificada como medida unilateral a ser adotada por um Estado,

[102] Grossi menciona as quatro principais áreas de atuação do DRCI: 1) Autoridade central brasileira para cooperação jurídica internacional em matérias penal e civil e recuperação de ativos; 2) Articulação institucional voltada para o combate à lavagem de dinheiro e à corrupção; 3) Implementação e Gerenciamento dos Laboratórios de Tecnologia em Combate à Lavagem de Dinheiro (LAB-LD); e 4) Representação do país nos foros nacionais e internacionais relacionados à cooperação jurídica internacional e combate à lavagem de dinheiro (GROSSI, 2014, p. 44-45).

diante de sua posição topográfica no texto da Convenção, opta-se por abordar tal tema neste subitem.

3.1.3.1 A Convenção de Budapeste e a cooperação internacional em matéria penal.

Conforme exposto, a cooperação internacional em matéria penal é uma solução que se impõe para a contenção da criminalidade cibernética, dado o seu forte caráter transnacional. A Convenção de Budapeste, de 2001, é, atualmente, marco jurídico fundamental na promoção da coordenação e da harmonização legislativa dos Estados em prol de uma política criminal mais assertiva no enfrentamento da criminalidade cibernética. Neste item, serão descritos os mecanismos de auxílio mútuo previstos na Convenção, especificamente a possibilidade de acesso transfronteiriço a dados informáticos armazenados.

O relatório explicativo da Convenção de Budapeste reconhece que dados armazenados em computadores são voláteis. Informações podem ser excluídas de forma rápida por programas automáticos, de modo a comprometer evidências e, por consequência, as investigações criminais. Nesse sentido, considerando que uma autoridade responsável pela persecução penal pode demandar dados armazenados em servidores localizados em jurisdições distintas da sua, a Convenção sinaliza a necessidade de fornecer meios para que esses dados sejam conservados e fornecidos, dentro dos limites jurídicos de cada Estado. Nesta estrutura são inseridos os mecanismos de cooperação internacional em matéria penal (CONSELHO DA EUROPA, p. 44-45, 2001-B).

A importância da Convenção na promoção de medidas de cooperação internacional está estritamente ligada ao esforço de harmonização legislativo. Jonathan Clough reafirma a importância de haver algum grau de harmonização entre os Estados para a formação de um modelo efetivo de contenção dos crimes cibernéticos. A título exemplificativo, o autor menciona a hipótese em que, mesmo quando a vítima e o criminoso estão inseridos na mesma jurisdição, as evidências da ofensa podem ter, em algum momento, passado por outras jurisdições, ou mesmo estar armazenadas em jurisdições distintas (CLOUGH, 2014, p. 700).

Para Clough, a harmonização legislativa é fundamental para garantir a efetiva cooperação entre as autoridades responsáveis pela persecução penal, ao mesmo tempo em que também busca reduzir espaços que podem, eventualmente, assumir a qualidade de "porto seguro" para criminosos cibernéticos (CLOUGH, 2014, p. 701). Nesse ponto, a harmonização normativa ultrapassa aspectos de direito material, como a tipificação, e alcança também a coordenação para fins de cooperação internacional em matéria penal.

Clough ressalta a importância da implementação das possibilidades de cooperação previstas na Convenção de Budapeste:

> Se implementadas, uma das mudanças mais significativas a resultarem da Convenção seria o processamento expedito de pedidos urgentes de assistência mútua. Atualmente, mecanismos de assistência mútua são notadamente lentos, e podem durar meses enquanto passam por canais burocráticas baseados em formas tradicionais. A Convenção prevê que as partes, em caso de "circunstâncias urgentes", façam pedidos e comunicações de assistência mútua usando "meios rápidos de comunicação, incluindo fax ou e-mail". Esses meios somente podem ser utilizados na medida em que sejam fornecidos níveis adequados de segurança e autenticação. A parte requerida deve aceitar e responder ao requerimento utilizando meios rápidos de comunicação, de modo que a confirmação formal somente seja necessária em caso de pedido da parte requerida (CLOUGH, 2014, p. 706).[103]

A Convenção prevê como medidas de cooperação, de forma geral, a extradição (art. 24) e o auxílio mútuo (art. 25 e seguintes), ambos concentrados no terceiro capítulo (CONSELHO DA EUROPA, 2001-A). De acordo com Delgado, a Convenção desenvolveu um sistema mais bem detalhado para as modalidades de auxílio mútuo, enquanto apenas reproduziu soluções tradicionais e já consolidadas para a extradição (DELGADO, 2007, p. 177). Esta dissertação tem como foco a análise do mecanismo de acesso transfronteiriço a dados informáticos armazenados, previsto no artigo 32 da Convenção e inserido no rol de instrumentos de auxílio mútuo.

O auxílio mútuo, em Budapeste, é concebido como gênero dos quais são espécies os seguintes mecanismos de cooperação internacional em matéria penal: a) conservação expedita de dados informáticos armazenados (artigo 29); b) divulgação expedita dos dados de tráfego conservados (artigo 30); c) auxílio mútuo relativamente ao acesso a dados informáticos armazenados (artigo 31); d) acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público (artigo 32); e) auxílio mútuo relativamente à recolha de dados de tráfego em tempo real (artigo 33); f) auxílio mútuo em matéria de intercepção de dados e conteúdo (artigo 34). Os mecanismos mencionados estão divididos a nível de auxílio mútuo em matéria de medidas provisórias (itens "a" e "b") e em matéria de poderes de investigação (itens "c", "d", "e" e "f"), diferenciados topograficamente pelos títulos 1 e 2 do capítulo 3 (CONSELHO DA EUROPA, 2001-A).

---

[103] Tradução livre. Na versão original: If implemented, one of the most significant changes to result from the Convention would be the expedited processing of urgent mutual assistance requests. Current mutual assistance mechanisms are notoriously slow and may take months as they pass through bureaucratic channels using traditional means. The Convention makes provision for parties, in 'urgent circumstances', to make mutual assistance requests and communications using 'expedited means of communication, including fax or e-mail'. Such means need only be utilised to the extent that they provide appropriate levels of security and authentication. The requested party must accept and respond to the request using expedited means of communication, with formal confirmation only necessary if at the request of the requested party (CLOUGH, 2014, p. 706).

Para além dos mecanismos acima elencados, a Convenção também prevê a organização da Rede 24/7 (artigo 35), com a finalidade de estabelecer ponto de contato para coordenação entre as partes, o qual deverá estar disponível a todo momento. Trata-se de iniciativa com a finalidade de "assegurar a prestação de assistência imediata a investigações ou procedimentos respeitantes a infrações penais relacionadas com dados e sistemas informáticos, ou a fim de recolher provas, sob a forma eletrônica, de uma infração penal" (CONSELHO DA EUROPA, 2001-A).

Delgado explica que a Convenção de Budapeste procurou adaptar medidas tradicionais executadas na investigação criminal para o cenário cibernético e, ao mesmo tempo, incluiu novas medidas propriamente destinadas a "atender às exigências das investigações no contexto da criminalidade informática", como a conservação expedita de dados informáticos armazenados e a divulgação expedita de dados de tráfego preservados (DELGADO, 2007, p. 182). Sobre tal esforço, destaca o autor:

> Note-se que os redatores da Convenção de Budapeste trataram de adaptar determinados aspectos de algumas medidas tradicionais de obtenção de elementos probatórios relativos a infrações penais, à realidade do moderno contexto tecnológico. Assim, com base na tradicional medida de busca e apreensão de bens (objetos tangíveis), criou-se a medida de "busca ou acesso, apreensão ou obtenção, e divulgação de dados informáticos armazenados" (objetos intangíveis). Por outro lado, a tradicional medida de interceptação de telecomunicações deu origem à "interceptação de dados de conteúdo" e à "coleta em tempo real de dados de tráfego" (DELGADO, 2007, p. 182).

Conforme os dispositivos da Convenção, por meio da modalidade de conservação expedita de dados informáticos armazenados (artigo 29), uma das partes pode efetuar pedido a outra para que esta obtenha rapidamente a conservação de dados armazenados por meio de sistema informático, em conformidade com as disposições de seu direito interno (CONSELHO DA EUROPA, 2001-A). O relatório explicativo aponta a centralidade deste mecanismo, uma vez que dados de interesse das instituições de persecução penal podem ser alterados ou excluídos de maneira rápida por indivíduos ou mesmo por programas automatizados, de modo a prejudicar a identificação do sujeito ou de provas do crime. Não se trata propriamente da posse dos dados por parte da autoridade requerida, mas da garantia de que dados armazenados em sua jurisdição serão preservados (CONSELHO DA EUROPA, 2001-B, p. 50-51).[104] Segundo Delgado, a preservação de dados é uma medida a ser executada

[104] Segundo o relatório explicativo da Convenção, a modalidade de conservação expedita de dados informáticos armazenados é menos intrusiva e, ao mesmo tempo, pode ser realizada de maneira mais rápida nas práticas rotineiras de cooperação jurídica internacional. Dessa forma: This procedure has the advantage of being both rapid and protective of the privacy of the person whom the data concerns, as it will not be disclosed to or examined by any government official until the criteria for full disclosure pursuant to normal mutual assistance regimes have been fulfilled. […] Preservation as foreseen by the drafters, however, is not particularly intrusive,

de maneira célere, a título de medida provisória, com a finalidade de preservar dados necessários à investigação criminal (DELGADO, 2007, p. 186).

Na sequência, a possibilidade de divulgação expedida dos dados de tráfego[105] conservados (artigo 30) amplia o mecanismo previsto no artigo 29. Por meio daquele, caso a parte requerida venha a identificar que um fornecedor de serviços localizado em outro Estado teve participação na transmissão dos dados de interesse da parte requerente, deverá divulgar "rapidamente à Parte requerente uma quantidade suficiente de dados relativos ao tráfego que permita identificar esse fornecedor de serviços e a via através da qual a comunicação foi transmitida" (CONSELHO DA EUROPA, 2001-A).[106]

Por meio do auxílio mútuo relativo ao acesso a dados informáticos armazenados, previsto no artigo 31 da Convenção, a parte poderá pedir a outra que investigue e divulgue dados armazenados em sistemas informáticos localizados em seu território. (CONSELHO DA EUROPA, 2001-A). Trata-se de mecanismo de cooperação jurídica que deve estar em consonância com outros tratados e legislações domésticas aplicáveis ao caso prático (CONSELHO DA EUROPA, 2001-B, p. 52).[107]

---

since the custodian merely maintains possession of data lawfully in its possession, and the data is not disclosed to or examined by officials of the requested Party until after execution of a formal mutual assistance request seeking disclosure of the data (CONSELHO DA EUROPA, 2001-B, p. 50-51). No mesmo sentido, Delgado destaca: de fato, a realização da preservação de dados não provoca, necessariamente, o levantamento do sigilo dos dados. Não se exige das autoridades competentes da Parte requerida o acesso ao conteúdo dos dados, objeto de um pedido de preservação. A Parte requerida apenas estará obrigada a exigir do provedor de serviços ou de outra pessoa responsável pelo armazenamento e/ou manutenção dos dados informáticos localizados em seu respectivo território, que estes permaneçam íntegros durante o período de tempo necessário (DELGADO, 2007, p. 186-187).

[105] Nos termos da Convenção e do seu Relatório Explicativo, dados de tráfego são: 28. For the purposes of this Convention traffic data as defined in article 1, under subparagraph d., is a category of computer data that is subject to a specific legal regime. This data is generated by computers in the chain of communication in order to route a communication from its origin to its destination. It is therefore auxiliary to the communication itself (CONSELHO DA EUROPA, 2001-A; CONSELHO DA EUROPA, 2001-B, p. 6). Ademais, os dados de tráfego são relevantes para as investigações criminais na medida em que permitem o rastreamento das fontes (CONSELHO DA EUROPA, 2001-B, p. 6).

[106] Para Delgado, "o conjunto desses dados de tráfego relativos a uma comunicação informática poderá revelar importantes elementos de prova, que sejam úteis no contexto de uma determinada investigação ou procedimento penal, uma vez que, através dos dados de tráfego relativos a uma comunicação informática é possível determinar a origem, o destino e a trajetória completa da comunicação, com a identificação do número da linha telefônica (em se tratando de acesso através de linha discada) ou da "linha de assinante digital" (DSL – Digital Subscriber Line, em se tratando de acesso "banda larga"), o endereço do protocolo IP atribuído pelo provedor de serviços, também a data e o horário do início (log-in) e do fim (log-off) do estabelecimento da conexão com o servidor, o tipo de serviço utilizado (e-mail, World Wide Web, chat etc.), a quantidade de bytes transmitidos etc." (DELGADO, 2007, p. 201).

[107] Delgado explica que a opção pelo termo "acessar" na denominação desta modalidade de cooperação tem como finalidade melhor refletir os padrões na área da informática, de modo a expressar a ideia de procurar "certa coisa ou pessoa". Para o autor: Por outro lado, o uso do termo "acessar" – que reflete com maior exatidão a terminologia adotada na área da informática – amplia as possibilidades de uma "busca" no sentido tradicional. De fato, o "acesso" aos dados informáticos poderá realizar-se on-line, por meio da utilização de um outro sistema informático, sem a necessidade de se empreender uma "busca" in situ do próprio sistema informático no qual encontrem-se armazenados os dados visados. Por exemplo, naqueles casos em que os dados informáticos

A possibilidade de acesso transfronteiriço a dados informáticos armazenados (artigo 32) permite que uma das partes tenha acesso a dados acessíveis ao público, de fonte aberta, independentemente de onde estiverem localizados. De igual modo, permite que a parte, por meio de um sistema informático localizado em seu território, tenha acesso a dados armazenados no território de outra parte, desde que em conformidade com o "consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados" (CONSELHO DA EUROPA, 2001-A).

O artigo 33 da Convenção dispõe sobre o auxílio mútuo para fins de recolha de dados de tráfego em tempo real. Tal mecanismo resguarda às partes a possibilidade de recolha de dados de tráfego ligados a comunicações transmitidas em seu território pela via informática, em conformidade com as disposições do ordenamento jurídico interno de cada uma das partes (CONSELHO DA EUROPA, 2001-A). Segundo o relatório explicativo da Convenção, justifica-se a inclusão deste mecanismo para fornecer a possibilidade de um Estado ser capaz de rastrear a fonte de determinada comunicação por meio dos dados de tráfegos por ela produzidos. Neste caso, o relatório explicativo assinala a importância da recolha em tempo real, na medida em que dados em tráfego são, recorrentemente, deletados automaticamente pelos provedores de serviço (CONSELHO DA EUROPA, 2001-B, p. 54).

Por fim, inclui-se na Convenção a previsão sobre o auxílio mútuo para fins de interceptação de dados de conteúdo[108] (artigo 34). Esta possibilidade prevê que as partes, levando em consideração a legislação interna e os acordos internacionais aos quais estão vinculadas, recolham ou registrem dados relacionados ao conteúdo de comunicações específicas realizadas pela via informática (CONSELHO DA EUROPA, 2001-A). O relatório explicativo da Convenção reconhece que tal medida de interceptação de dados possui maior grau de intrusão. Por este motivo, reforçou-se que esta modalidade depende do ordenamento jurídico interno das partes envolvidas na cooperação, bem como dos tratados internacionais relacionados (CONSELHO DA EUROPA, 2001-B, p. 54).

Os mecanismos dispostos nos previamente mencionados artigos 33 e 34 da Convenção de Budapeste buscam adaptar as modalidades tradicionais de "interceptação de telecomunicações" para o âmbito das relações informáticas. Ao mesmo tempo, reforça-se que

---

encontrem-se armazenados em um mailbox (caixa de correio eletrônico) em um sistema informático acessível através da Internet, ou mesmo nos casos em que os dados encontrem-se armazenados em um outro computador que esteja conectado ao primeiro, fazendo parte de uma mesma rede de área local (LAN – Local Area Network). (DELGADO, 2007, p. 191-192).

[108] O termo dados de conteúdo faz referência "ao conteúdo informativo da comunicação, isto é, o significado ou o teor da comunicação; ou melhor, a mensagem ou informação transmitida pela comunicação" (DELGADO, 2007, p. 211).

a Convenção não permite a realização da coleta indiscriminada de dados de tráfego, com a finalidade de evitar as *fishing expeditions*, por meio das quais são acessados um enorme volume de dados de maneira aleatória (DELGADO, 2007, p. 204-207).

Embora a Convenção de Budapeste estimule as partes a cooperarem de maneira ampla e com agilidade, não há obrigação expressa para que uma das partes forneça informações espontaneamente a outra. De maneira geral, a Convenção não vincula os Estados a uma obrigação de promover medidas de auxílio mútuo, de modo que qualquer uma das partes pode recusar o pedido de outra, dentro das hipóteses previstas na Convenção.[109] Justifica-se esse fato em razão de a Convenção reconhecer que a instrumentalização da cooperação internacional pela via do auxílio mútuo depende da legislação doméstica de cada Estado e dos tratados internacionais aos quais eles estão vinculados. Assim, à medida que as possibilidades de auxílio mútuo se tornam mais "intrusivas" na jurisdição dos Estados membros, a Convenção sujeita a execução dessas medidas a acordos entre as partes e à legislação doméstica de cada Estado (CLOUGH, 2014, p. 714-716).

A Convenção, nesse sentido, atua de maneira complementar para "suplementar outros acordos multilaterais ou bilaterais entre Estados, ou pode ser utilizada quando não houver nenhum acordo firmado". Quando aplicada subsidiariamente a outro instrumento jurídico internacional, todavia, este acordo deve estar em consonância com a Convenção, de modo que não possa entrar em conflito com os princípios desta (CLOUGH, 2014, p. 714).

Em 12 de maio de 2022, o Conselho da Europa abriu o *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* para assinatura dos Estados partes da Convenção. O protocolo busca ampliar a abordagem da Convenção sobre as medidas de cooperação jurídica internacional, especificando procedimentos a serem adotados para reforçar a cooperação entre provedores e entidades localizadas em outras partes e entre autoridades de Estados distintos para a disponibilização de dados armazenados, bem como procedimentos relativos à assistência mútua emergencial (CONSELHO DA EUROPA, 2022-C).

O segundo protocolo adicional também apresenta condições e salvaguardas a serem observadas no curso da cooperação jurídica internacional. O artigo 14 reforça a necessidade de proteção de dados pessoais no âmbito da aplicação da Convenção. Dessa forma, as partes

[109] Nos termos do artigo 27 da Convenção de Budapeste, nesse sentido, um pedido para cooperação em sede de auxílio mútuo poderá ser recusado pela parte requerida: a) se o pedido respeitar as infrações consideradas pela Parte requerida como infrações políticas ou com ela conexas; ou b) se a Parte considerar que o cumprimento do pedido pode atentar contra a sua soberania, segurança, ordem pública ou qualquer outro interesse essencial do seu país (CONSELHO DA EUROPA, 2001-A).

devem adotar as medidas de proteção e de salvaguarda previstas neste dispositivo quando estiverem processando dados recebidos de outra parte. No entanto, caso ambas as partes requerente e requerida estejam vinculadas a tratado internacional que estabeleça um regime abrangente[110] de proteção de dados pessoais e que seja aplicável às hipóteses de prevenção, detecção, investigação e persecução de ofensas criminais, os termos do tratado específico devem prevalecer em relação ao Segundo Protocolo Adicional. Adiante, as partes também podem optar pela aplicação de outro acordo que as vincule mutuamente em matéria de proteção de dados pessoais em detrimento do Segundo Protocolo Adicional (CONSELHO DA EUROPA, 2022-B, p. 41-42).

O objetivo destes dispositivos é assegurar que as partes tenham algum grau de flexibilidade na escolha do regime de proteção de dados pessoais a ser aplicado às transferências internacionais de dados previstas no âmbito da Convenção de Budapeste e de seus protocolos adicionais (CONSELHO DA EUROPA, 2022-B, p. 41-42).[111]

Ainda sobre a proteção de dados pessoais, o Segundo Protocolo Adicional determina que as partes, com vistas a devidamente assegurar nível adequado de proteção de dados pessoais, devem incluir a garantia da segurança da informação contra incidentes de segurança, como o acesso, a divulgação, a alteração ou a destruição de dados realizados sem autorização válida (CONSELHO DA EUROPA, 2022-C, p. 15).

---

[110] O relatório explicativo do Segundo Protocolo Adicional esclarece a terminologia "tratado abrangente" em matéria de proteção de dados pessoais: In this context, a framework would generally be considered as being "comprehensive" where it comprehensively covers the data protection aspects of the data transfers. Two examples of agreements under paragraph 1.b are the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) as amended by Protocol CETS No. 223, and the Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses. The terms of such agreements shall apply in lieu of paragraphs 2 to 15 for the measures falling within the scope of such agreements. With respect to the Parties to Convention ETS No. 108 as amended by Protocol CETS No. 223, this means that Article 14, paragraph 1, of that treaty, as further explained in paragraphs 105 to 107 of its explanatory report, is applicable. In terms of timing, paragraphs 2 to 15 of this article will be superseded only if the Parties are mutually bound by the agreement at the time of receipt of personal data under this Protocol. This applies for as long as the agreement provides that data transferred pursuant to it continues to be processed under the terms of that agreement (CONSELHO DA EUROPA, 2022-B, p. 42).

[111] Article 14 – Protection of personal data 1 Scope a Except as otherwise provided in paragraphs 1.b and c, each Party shall process the personal data that it receives under this Protocol in accordance with paragraphs 2 to 15 of this article. b If, at the time of receipt of personal data under this Protocol, both the transferring Party and the receiving Party are mutually bound by an international agreement establishing a comprehensive framework between those Parties for the protection of personal data, which is applicable to the transfer of personal data for the purpose of the prevention, detection, investigation and prosecution of criminal offences, and which provides that the processing of personal data under that agreement complies with the requirements of the data protection legislation of the Parties concerned, the terms of such agreement shall apply, for the measures falling within the scope of such agreement, to personal data received under this Protocol in lieu of paragraphs 2 to 15, unless otherwise agreed between the Parties concerned. c If the transferring Party and the receiving Party are not mutually bound under an agreement described in paragraph 1.b, they may mutually determine that the transfer of personal data under this Protocol may take place on the basis of other agreements or arrangements between the Parties concerned in lieu of paragraphs 2 to 15 (CONSELHO DA EUROPA, 2022-C).

Ressalta-se, ademais, o reconhecimento do Conselho da Europa concernente à necessidade de proteção aos direitos humanos no curso dos procedimentos previstos na Convenção de Budapeste:

> Além disso, exige-se das partes contratantes que adotem as medidas legislativas para permitir que suas autoridades nacionais interceptem dados de tráfico e de conteúdo. Também obriga que as partes contratantes, quando da implementação da Convenção, prevejam uma proteção adequada aos direitos humanos e às liberdades, incluindo os direitos garantidos pela ECHR, como o direito à proteção de dados (CONSELHO DA EUROPA, 2018, p. 280).[112]

Observa-se, assim sendo, que as modalidades de auxílio mútuo previstas na Convenção de Budapeste buscam aprimorar o cenário de cooperação jurídica internacional para o enfrentamento do cibercrime, seja por meio do estabelecimento de novas possiblidades de cooperação entre os Estados-partes, seja por meio atualização de medidas já tradicionais para o contexto cibernético.

Como visto, por fim, a Convenção não se apresenta como um mecanismo definitivo para a cooperação. Isto é, busca-se a harmonização dos termos de Budapeste com o ordenamento jurídico doméstico dos Estados e com outros acordos internacionais, bilaterais ou multilaterais, com a finalidade de complementar as possibilidades de cooperação jurídica internacional em matéria penal.

3.1.3.2 A modalidade de acesso transfronteiriço a dados informáticos armazenados.

Topograficamente, a Convenção de Budapeste insere a modalidade de acesso transfronteiriço a dados informáticos armazenados no título 2, da seção 2, do capítulo III, referente à cooperação jurídica internacional. No entanto, terminologicamente, este mecanismo, de maneira distinta das demais modalidades constantes neste título, não apresenta a identificação "auxílio mútuo" em seu dispositivo correspondente. Embora o acesso transfronteiriço a dados informáticos armazenados possa depender de coordenação entre os Estados para a sua concretização, a previsão normativa dispõe que sua execução possa ocorrer de maneira unilateral, sem autorização de outra Parte.

As medidas procedimentais estabelecidas pela Convenção estão delimitadas ao Estado onde a investigação criminal ocorre. Nesse sentido, o instrumento busca privilegiar o recurso à cooperação jurídica internacional entre as partes, com exceção das hipóteses

[112] Tradução livre da versão original: Furthermore, it requires Contracting Parties to adopt legislative measures to enable their national authorities to intercept traffic and content data. It also obliges the Contracting Parties, when implementing the convention, to foresee adequate protection of human rights and liberties, including the rights guaranteed under the ECHR, such as the right to data protection. Contracting parties are not required to also join Convention 108 in order to join the Budapest Convention on Cybercrime (CONSELHO DA EUROPA, 2018, p. 280).

dispostas no artigo 32 da Convenção, sobre acesso transfronteiriço a dados informáticos armazenados ou de acordo supranacional diverso (ALVES, 2020, p. 27-28).

Uma vez identificadas quais são as modalidades de auxílio mútuo previstas na Convenção de Budapeste, é necessário aprofundar o exame na hipótese de acesso transfronteiriço a dados informáticos armazenados, prevista nos termos do artigo 32, a qual integra o objeto central deste capítulo. Quando da elaboração da Convenção, debateu-se sobre a possibilidade de acesso unilateral a dados informáticos armazenado em computadores localizados na jurisdição de Estado distinto. Naquele momento, a conclusão parcial descrita no relatório explicativo indicava que ainda não era possível formalizar tratado internacional abrangente sobre o tema (CONSELHO DA EUROPA, 2001-B, p. 53).

A comissão elaboradora entendeu, naquele momento, que ainda não havia ampla experiência em casos concretos voltados ao acesso transfronteiriço a dados informáticos armazenados. Diante dessas circunstâncias, haveria dificuldades para a formulação de normas gerais que regulamentem a matéria a nível de tratado internacional. Por consequência, decidiu-se por não apresentar regras específicas para esta modalidade até que houvesse tempo suficiente para novas discussões (CONSELHO DA EUROPA, 2001-B, p. 53). Sobre tema, Alves destaca:

> É, por isso, a título excecional que se elenca no artigo 32.º da CBCc as situações em que é admissível o acesso transfronteiriço (unilateral) a dados informáticos armazenados em sistema informático sito no estrangeiro, sem necessidade de autorização nem notificação do Estado visado. A previsão de apenas duas formas de acesso transfronteiriço reforça esta ideia de excecionalidade, na medida em que, após longo debate, os "redatores [da Convenção] decidiram que apenas seriam definidas, ao abrigo do Artigo 32.º da Convenção, as situações nas quais, por unanimidade, a acção unilateral se mostrasse aceitável», uma vez que, à data, não existia ainda «uma experiência objectiva relativamente a este tipo de situações, ao que se acrescenta o facto de se considerar que a resolução adequada está, frequentemente, ligada à conjuntura do caso concreto, pelo que se torna difícil estipular regras gerais" (CONSELHO DA EUROPA apud ALVES, 2020, p. 28).

Trata-se de tema complexo na medida em que o acesso transnacional a dados realizado de maneira unilateral toca princípios sensíveis de Direito Internacional, tal qual a soberania dos Estados, e envolve também os direitos fundamentais dos indivíduos, como a privacidade e a proteção de dados pessoais (CONSELHO DA EUROPA, 2012, p. 6). Desde a década de 1990 o assunto já era objeto de preocupações no âmbito do Conselho da Europa, conforme é possível observar pela Recomendação de número R (95) 13 do Comitê de Ministros do Conselho da Europa:

> VII. Cooperação internacional. 17. O poder de estender uma procura a outros sistemas de computadores deve também ser aplicável quando o sistema esteja localizado em jurisdições estrangeiros, desde que seja necessária uma ação imediata. Para evitar possíveis violações da soberania estatal ou do direito internacional, deve

> ser estabelecida uma base legal não ambígua para tal extensão da busca e apreensão. Portanto, há uma necessidade urgente de se negociar acordos internacionais sobre como, quando e em que extensão tal busca e apreensão deva ser permitida (CONSELHO DA EUROPA, 1995).[113]

Reforça-se que o artigo 32 estabelece duas condições por meio das quais o acesso transfronteiriço se torna possível. Na primeira, quando os dados armazenados estão disponíveis publicamente e, na segunda, quando o Estado-parte obteve a permissão com o consentimento legal e voluntário da pessoa com a autoridade para divulgar os dados de interesse (CONSELHO DA EUROPA, 2001-B, p. 53).

Segundo Pedro Verdelho, a possibilidade de acesso transfronteiriço a dados publicamente abertos é comumente aceita entre os Estados. No entanto, o acesso transfronteiriço mediante consentimento de pessoa legalmente autorizada é objeto de maiores controvérsias (VERDELHO, 2019, p. 138).

Na hipótese de acesso transfronteiriço a dados armazenados com acesso publicamente disponível, estão incluídos os dados cujo acesso não dependa de pré-requisitos especiais. Trata-se de medida que é realiza sem a ativação de instrumento de cooperação jurídica internacional, embora tenha inevitáveis caráter e aplicação transnacionais. Nesta hipótese, a Convenção prevê apenas o acesso aos dados informáticos, embora seja possível interpretar que tais dados também podem ser coletados e armazenados pelo Estado-parte (ALVES, 2020, p. 29-31).[114]

No entanto, mesmo quando se trata do acesso a dados disponíveis ao acesso público, a aplicação de ferramentas para a execução de pesquisas sistemáticas, por meio de instrumentos de "recolha e/ou tratamento automatizado de dados" pode implicar em uma ameaça à privacidade dos titulares destes dados (ALVES, 2020, p. 29-31). Nesse sentido,

---

[113] Tradução livre da versão original: VII. International co-operation. 17. The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted (CONSELHO DA EUROPA, 1995).

[114] Alves menciona, a título exemplificativo, o uso desta modalidade pelas autoridades responsáveis pela persecução penal: De facto, os órgãos de investigação operam frequentemente pesquisas com recurso a motores de busca ou perfis de redes sociais (desde que o usuário não tenha limitado o acesso às informações publicadas) como forma de obter informações básicas sobre suspeitos que, mesmo não servindo, muitas vezes, de prova, revelam-se fundamentais na determinação do rumo da investigação. A título de exemplo, o atentado terrorista ocorrido na maratona de Boston, de 15 de abril de 2013, que vitimou mais de 250 pessoas, três das quais não sobreviveram, demonstrou que, numa fase preliminar da investigação, as informações recolhidas de fontes publicamente acessíveis, nomeadamente, em redes sociais podem ser determinantes. Neste caso, a identificação da conta de Twitter de Dzhokhar Tsarnaev, suspeito de, conjuntamente com o irmão Tamerlan, ter perpetrado o ataque contra as multidões que assistiam à maratona, permitiu à investigação traçar o seu perfil, capturando-o dias depois, a 19 de abril (ALVES, 2020, p. 30).

ainda que em relação aos dados publicados no mundo virtual, há necessidade de observância do direito à privacidade e à proteção de dados pessoais (KOOPS, 2013, p. 655).

Adiante, aborda-se a possibilidade de acesso transfronteiriço a dados informáticos armazenados mediante consentimento de pessoa legalmente autorizada. Em primeiro lugar, ressalva-se que o consentimento, nesta hipótese, deve ser lícito e voluntário (VERDELHO, 2019, p. 139). Sobre este aspecto, os termos que definem a pessoa com autoridade para divulgar os dados dependem da legislação aplicável e da própria natureza desta pessoa autorizada. Sobre o tema, o relatório explicativo da Convenção busca esclarecer:

> Quem é a pessoa que é "legalmente autorizada" a divulgar dados pode variar dependendo das circunstâncias, da natureza da pessoa e da legislação aplicável. Por exemplo, o e-mail de uma pessoa pode estar armazenado em outro Estado por um provedor de serviços, ou a pessoa pode ter intencionalmente armazenado seus dados em outro país. Essas pessoas podem recuperar os dados e, uma vez que possuam a autoridade legal, podem voluntariamente divulgar seus dados para os agentes da lei ou podem permitir que esses agentes tenham acesso aos dados, conforme previsto no artigo (CONSELHO DA EUROPA, 2001-B, p. 53).[115]

A pessoa legalmente autorizada a divulgar dados, destarte, poderá ser o próprio titular dos dados, de modo a coincidir com o réu ou com a vítima de determinado processo criminal. Existem possibilidades, todavia, em que terceiros podem ter legitimidade para oferecer o consentimento relativo ao acesso a dados informáticos, tais quais fornecedores de serviços de internet, como operadores de internet, de armazenamento em nuvem ou de serviços de *e-mail* (ALVES, 2020, p. 31-33).

De acordo com Delgado, nem sempre a pessoa autorizada a permitir o acesso aos dados armazenados em sistema informático será detentora do direito de divulgá-los. Menciona-se, a título exemplificativo, a hipótese do administrador de sistema informático que, embora autorizado a acessar os dados armazenados em um sistema, não necessariamente possuíra autorização jurídica para divulgá-los (DELGADO, 2007, p. 199).

Neste caso, acrescenta-se ao exemplo a política de privacidade da *Google*:

> Não compartilhamos informações pessoais com empresas, organizações ou indivíduos externos ao Google, exceto nos casos descritos abaixo. [...] Por motivos legais: Compartilharemos informações pessoais fora do Google se acreditarmos, de boa-fé, que o acesso, o uso, a conservação ou a divulgação das informações sejam razoavelmente necessários para: cumprir qualquer legislação, regulação, processo legal ou solicitação governamental aplicável. Compartilhamos informações sobre o número e o tipo de solicitações que recebemos dos governos em nosso Transparency Report; cumprir Termos de Serviço aplicáveis, inclusive investigação de possíveis

[115] Tradução livre da versão original: Who is a person that is "lawfully authorised" to disclose data may vary depending on the circumstances, the nature of the person and the applicable law concerned. For example, a person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article (CONSELHO DA EUROPA, 2001-B, p. 53).

> violações; detectar, impedir ou lidar de alguma forma com fraudes, problemas técnicos ou de segurança; proteger de prejuízos aos direitos, à propriedade ou à segurança do Google, dos nossos usuários ou do público, conforme solicitado ou permitido por lei (GOOGLE, 2022).

Verifica-se, desta maneira, que os meios de acesso transfronteiriço a dados informáticos produzem também um contato entre o Estado e entidades privadas detentoras de dados. Por essa razão, nota-se que o acesso a dados localizados na jurisdição de outro Estado por parte da autoridade responsável pela persecução penal de um Estado produz efeitos tanto em relação aos indivíduos quanto em relação a entidades terceiras relacionadas.

O Relatório *Transborder access and jurisdiction: What are the options?*, do Conselho da Europa, destaca a dificuldade que autoridades de persecução penal enfrentam para garantir a proteção dos direitos fundamentais dos indivíduos cujos dados estão sendo acessados em outras jurisdições. O relatório entende que o acesso transfronteiriço a dados informáticos armazenados deve levar em consideração a tutela dos direitos humanos, sendo necessário desenvolver condições e salvaguardas para a aplicação esta modalidade (CONSELHO DA EUROPA, 2012, p. 12).

No entanto, há divergências entre os Estados sobre quais garantias protetivas devem ser aplicadas no que tange à medida de acesso transfronteiriço a dados armazenados. Isto é, nos termos do Relatório mencionado, "as pessoas de um Estado particular normalmente esperam, no mínimo, as proteções a eles garantidas pelo seu Estado; elas não esperam ser investigadas de acordo com os padrões de um Estado no qual elas não vivem [...]" (CONSELHO DA EUROPA, 2012, p. 12).[116]

Sob tal prisma, o Relatório demonstra a preocupação com o uso das medidas de acesso transfronteiriço por parte de Estados não comprometidos com a proteção de direitos fundamentais, tais quais o direito à privacidade e à proteção de dados (CONSELHO DA EUROPA, 2012, p. 13). Diante destes pressupostos, a execução de política criminal baseada no acesso transfronteiriço pode se configurar como um novo risco aos indivíduos.

Sobre esta preocupação, destaca-se que:

> Soluções para a proteção dos indivíduos e de terceiros ou para operações de aplicação da lei precisam superar as dificuldades práticas da expansão de regras para acesso transfronteiriço. Os Estados participantes devem concordar com um nível mínimo de condições e salvaguardas a serem aplicadas quando uma agência de aplicação da lei alcançar outro Estado para obter informações eletrônicas. Estados devem desenvolver e concordar com procedimentos para coordenar o acesso transfronteiriço e as comunicações entre eles nesse tipo de atividade. Deverão ser considerados a legislação doméstica e os procedimentos do Estado onde os dados ou

[116] Tradução livre da versão original: The people in a particular State normally expect, at a minimum, the protections afforded to them by this State; they do not expect to be searched according to the standards of a State they do not live in and may never have been in (CONSELHO DA EUROPA, 2012, p. 12).

> o indivíduo está localizado, incluindo regulamentações de proteção de dados. Para que um Estado concorde com o acesso transfronteiriço, ele deve estar satisfeito que o acesso deverá ser compatível com as leis e com as políticas-chave, as quais alcançam desde as proteções constitucionais para indivíduos e o direito penal substantivo relacionado a computadores e a redes para proteção da propriedade privada. Os Estados também devem decidir por mecanismos de aplicação da lei que impeçam o uso indevido do acesso transfronteiriço (CONSELHO DA EUROPA, 2012, p. 16).[117]

Dessa forma, observa-se que, embora a possibilidade de acesso transfronteiriço a dados informáticos armazenados, prevista na Convenção de Budapeste, não exija um pedido prévio de auxílio mútuo, esta possibilidade demanda a coordenação entre os Estados, com a finalidade de que haja consenso sobre os níveis adequados de proteção aos direitos fundamentais, tais quais o direito à proteção de dados pessoais. Ressalta-se, nesse sentido, a Diretiva n.º 2016/680 da União Europeia, que contém condições específicas sobre a transferência internacional de dados em matéria de persecução penal.

A política criminal direcionada ao enfrentamento do cibercrime transnacional, ainda que materializada pela via do acesso transfronteiriço a dados informáticos armazenados, levando em consideração também o Segundo Protocolo Adicional à Convenção de Budapeste, passa a depender também de um regime acordado de proteção de dados pessoais entre os Estados envolvidas.

3. 2 AS DECISÕES DE ADEQUAÇÃO DA UNIÃO EUROPEIA E A SUA POSSÍVEL APLICAÇÃO PARA FINS PENAIS.

Conforme já se indicou no item 2.3 desta dissertação, é relevante retomar a importância das decisões de adequação da Comissão Europeia enquanto mecanismo de reconhecimento por parte da União Europeia de que há nível adequado de proteção de dados pessoais no país parceiro para fins de cooperação internacional.

No relatório *Cross-border data access in criminal proceedings and the future of digital justice*, Sergio Carrera, Marco Stefan e Valsamis Mitsilegas indicam que a União Europeia leva em consideração os seus padrões protetivos no âmbito da cooperação jurídica

---

[117] Tradução livre da versão original: Solutions to the protection of individuals and other third parties or of law enforcement operations will have to overcome the practical difficulties of expanding rules for transborder access. Participating States will have to agree on the minimum conditions and safeguards that apply when a law enforcement agency reaches into another State to obtain electronic information. States must develop and agree on procedures for coordinating transborder access and communicating with each other on such activities. A significant consideration will be the domestic laws and procedures of the State where the data or subject is located, including data protection regulations. For a State to agree to transborder access, it must be satisfied that the access will comport with laws and key policies ranging from constitutional protections for individuals and the substantive criminal law related to computers and networks to protection of private property. States must also agree to enforcement mechanisms that deter improper use of transborder access (CONSELHO DA EUROPA, 2012, p. 16).

internacional com países externos à integração. Isto é, os procedimentos de cooperação não devem comprometer os padrões jurídicos estabelecidos internamente pela União (CARRERA, STEFAN, MITSILEGAS, 2020, p. 76).

Nos termos do já mencionado artigo 45 da GDPR, a transferência de dados pessoais de um país membro da União Europeia para Estado terceiro depende do reconhecimento de que esse Estado possui níveis adequados de proteção de dados pessoais (UNIÃO EUROPEIA, 2016-A). Especificamente em relação ao domínio penal e ao interesse de investigação criminal, a Diretiva n.º 2016/680 determina critérios específicos para a transferência de dados pessoais a partir de um país da União Europeia para Estado terceiro (UNIÃO EUROPEIA, 2016-B; MARTÍNEZ, 2020, p. 170).

De acordo com os critérios para transferência internacional de dados estabelecidos pela GDPR e pela Diretiva n.º 2016/680, já apresentados no item 2.3 desta pesquisa, é necessário que o Estado terceiro a ter acesso aos dados informáticos de conteúdo pessoal demonstre possuir os níveis adequados de tutela ao direito à proteção de dados. São 3 as possibilidades previstas na GDPR e na Diretiva para o reconhecimento de adequação do sistema de proteção de dados pessoais: a) a decisão de adequação da Comissão Europeia; b) a apresentação de garantias adequadas; c) derrogações em situações específicas (UNIÃO EUROPEIA, 2016-B; MARTÍNEZ, 2020, p. 178).

A hipótese relacionada à decisão de adequação, segundo Alexandra Maria Rodrigues Araújo, está em consonância com o princípio da adequada proteção. Isto é, o fluxo de dados pessoais da União Europeia para Estado terceiro somente será permitido se neste estiver garantido um nível adequado de proteção de dados pessoais (RODRIGUES ARAÚJO, 2015, p. 82-83).

As decisões de adequação, assim, são mecanismos por meio dos quais a União Europeia autoriza a livre transferência de dados pessoais, levando em consideração a tutela da GDPR, sem que seja necessária a autorização específica *ad hoc* (GNOATTON, 2021, p. 48). A decisão reconhece, portanto, que o Estado a receber os dados pessoais de cidadão europeu oferecerá garantias a nível equivalente àquelas previstas pela União Europeia, de modo a reduzir os riscos atinentes à transferência internacional de dados (EUROPEAN DATA PROTECTION BOARD, 2021, p. 8-16).

As decisões de adequação, para além da avaliação do sistema de proteção de dados pessoais, ponderam os já mencionados critérios de existência de Estado de Direito e de respeito aos direitos e liberdades fundamentais (MARTÍNEZ, 2020, p. 186). Ademais, a consideração n.º 68 da Diretiva explica que a Comissão deverá levar em conta as obrigações

do Estado não membro da União Europeia em outros instrumentos internacionais que versem sobre a proteção de dados, especialmente a Convenção nº 108 de 1981 (UNIÃO EUROPEIA, 2016-A). Outro aspecto essencial avaliado pela Comissão é a existência e atuação de autoridade independente responsável pela conformidade da proteção de dados no Estado (MARTÍNEZ, 2020, p. 188-189).

Havendo, destarte, decisão de adequação reconhecendo nível adequado de proteção de dados pessoais em Estado terceiro, poderá haver livre fluxo de dados para tal país. No entanto, nas hipóteses em que a decisão não estiver presente, mas em que haver prova de que as garantias necessárias em matéria de proteção de dados pessoais serão observadas em situação especificada – por meio de tratado internacional, por exemplo –, poderá haver fluxos de dados pessoais, ainda que em nível restrito ao Estado terceiro (RODRIGUES ARAÚJO, 2015, p. 86-88).

Nas hipóteses em que não houver decisão de adequação por parte da Comissão, ainda resta a possibilidade de intercâmbio de dados pessoais por meio de mecanismos internacionais vinculantes entre as partes envolvidas que assegurem juridicamente a proteção aos dados pessoais. No mesmo sentido, também será permitida a transferência se o responsável pelo tratamento de dados do país membro da União Europeia tenha avaliado, no caso concreto, que existem garantias adequadas de proteção (MARTÍNEZ, 2020, p. 189-190).

A avaliação da Comissão, como identifica Rodrigues Araújo, é realizada por meio de exame do sistema jurídico do Estado, o qual pode ser parametrizado de forma completa ou setorizada. (RODRIGUES ARAÚJO, 2017, p. 213). Dessa forma, há a possibilidade de reconhecimento da adequação apenas em relação a determinado setor do país terceiro a ser avaliado, a depender dos critérios levantado quando da decisão (MARQUES, 2020, p. 66).

Em sua dissertação de mestrado, Letícia Mulinari Gnoatton identificou 8 elementos considerados relevantes para a Comissão Europeia na realização da decisão de adequação para reconhecimento de nível adequado de proteção de dados pessoais, quais sejam: a) estrutura; b) funções; c) poderes; d) âmbito de exercício de seus poderes; e) direitos dos titulares; f) membros e integrantes; g) orçamento; e h) cooperação internacional (GNOATTON, 2021, p. 106). Nos termos apresentados por Gnoatton:

> 1. Estrutura. A estrutura do órgão deve garantir sua autonomia, embora não se exija um modelo específico que deva ser adotado. Registre-se que, até o presente momento, não houve concessão de decisão de adequação a um Estado terceiro cujo órgão não possuísse natureza pública; 2. Funções. Suas funções devem ser similares às estabelecidas pelo Regulamento. Em resumo, ele deve assegurar o cumprimento das normas de proteção dados pessoais; 3. Poderes. O órgão deve ter poderes investigativos e coercitivos, exercidos por processos administrativos, com destaque à possibilidade de aplicação de advertências e multas e a determinação de suspensão

> ou proibição do tratamento de dados pessoais pelos responsáveis; 4. Âmbito de exercício de seus poderes. Seus poderes devem ser aplicáveis a todos os responsáveis pelo tratamento de dados pessoais, incluindo órgãos que compõem o Governo; 5. Direitos dos titulares. Deve contar com mecanismos que viabilizem o acesso dos titulares ao exercício de seus direitos; 6. Membros e integrantes. Os processos de nomeação e afastamento de membros do órgão devem ser transparentes, justos e imparciais, garantindo a estabilidade para o exercício do mandato, enquanto o pessoal que integra a Autoridade de Controle deve estar hierarquicamente submetido unicamente a seus próprios membros; 7. Orçamento. Deve ter dotação orçamentária própria; 8. Cooperação internacional. Deve ter competência para cooperar, em matéria de dados pessoais, com Autoridades de Controle dos Estados-Membros (GNOATTON, 2021, p. 106).

A Comissão Europeia é a autoridade competente para formular a decisão de adequação, bem como de monitorar a aplicação do tema no terceiro avaliado ao longo do tempo. Dessa forma, havendo transformações significativas no regime protetivo do Estado terceiro que comprometam o nível adequado de proteção, a Comissão poderá revogar, alterar ou suspender a decisão (MARQUES, 2020, p. 66).

A decisão de adequação, nesse sentido, é instrumento de reconhecimento unilateral da União Europeia que permite o livre fluxo de dados pessoais entre os Estados-membros e o Estado terceiro. Tal medida unilateral, no entanto, conforme observado por Gnoatton, normalmente é acompanhada de reconhecimento recíproco por parte do país terceiro, de modo a autorizar juridicamente, por ambas as partes, o livre trânsito de dados (GNOATTON, 2021, p. 49).

A Comissão Europeia, na consideração n.º 1 de introdução à decisão de adequação ao Japão, destaca:

> O fluxo de dados pessoais com origem em países não pertencentes à União Europeia ou a eles destinado é necessário para se poder aprofundar a cooperação e o comércio internacionais, garantindo, simultaneamente, que o nível de proteção dos dados pessoais conferido na União Europeia não é comprometido (COMISSÃO EUROPEIA, 2019).

Busca-se examinar, na sequência, as decisões de adequação relativas a 6 casos considerados relevantes para esta pesquisa: a) Canadá; b) Argentina; c) Andorra; d) Israel; e) Uruguai; e f) Japão. Dentre as decisões de adequação já proferidas pela Comissão Europeia, elege-se estas 6 por dois motivos, a serem justificados.

Em primeiro lugar, opta-se pela análise do caso de Argentina e do Uruguai em razão da proximidade regional e da maior intensidade na cooperação jurídica internacional com Brasil, notadamente pela via da integração mercosulina. Ademais, seleciona-se também as decisões relativas ao Canadá, Andorra, Israel e Japão, uma vez que tais Estados são igualmente partes da Convenção de Budapeste sobre cibercrime e não são membros da União Europeia.

Pesquisas anteriores já se debruçaram sobre as decisões de adequação da Comissão Europeia, incluindo estudos sobre seus impactos e suas características, avaliando-se eventuais padrões e critérios previamente adotados (RODRIGUES ARAÚJO, 2017; MARQUES, 2020; GNOATTON, 2021). Assim sendo, não se pretende examinar os requisitos formais e materiais por meio dos quais a Comissão profere a decisão de adequação, tampouco o sistema protetivo de dados pessoais dos países elencados. Desta feita, esta investigação busca visualizar eventual aplicabilidade para fins de cooperação internacional em matéria penal das decisões. Busca-se, assim sendo, focalizar a lente investigativa na presença de eventuais menções à aplicação da proteção de dados pessoais para questões de persecução criminal e de segurança pública.

3.2.1 Decisão de adequação ao Canadá (2001).

A decisão de adequação proferida pela Comissão Europeia em relação ao Canadá data de 2001, ainda com base na Diretiva 95/46/EC. A avaliação tem como embasamento o *Canadian Personal Information Protection and Electronic Documents Act*, de 2000, relativo à proteção de dados pessoais em território canadense (COMISSÃO EUROPEIA, 2001).

Não há menção expressa na decisão sobre aspectos relacionados à aplicação do direito à proteção de dados pessoais em matéria de investigação criminal ou para fins de segurança pública em geral. A legislação canadense avaliada tem sua aplicação determinada às organizações privadas que coletam, usam e divulgam informações de caráter pessoal, de modo que a referida norma não se aplique propriamente ao setor público (COMISSÃO EUROPEIA, 2001).

No entanto, a decisão reconhece que a legislação canadense assegura nível adequado de proteção, ainda que exista previsão de exceções justificáveis por interesse público (COMISSÃO EUROPEIA, 2001). A Comissão, contudo, não justifica expressamente a motivação da decisão, nem se aprofunda em quais foram os parâmetros de proteção considerados (MARQUES, 2020, p. 95).

3.2.2 Argentina (2003).

A decisão de adequação em relação ao sistema jurídico argentino foi proferida pela Comissão Europeia em 2003, ainda com base na Diretiva 95/46/EC. A avaliação é realizada com base na Constituição argentina, no *Personal Data Protection Act* n.º 25.326 e no Decreto n.º 1558/2001, complementar à legislação (COMISSÃO EUROPEIA, 2003).

Não há menção expressa na decisão sobre aspectos relacionados à aplicação do direito à proteção de dados pessoais em matéria de investigação criminal ou para fins de segurança pública em geral (COMISSÃO EUROPEIA, 2003).

A Comissão reconheceu que o sistema jurídico argentino possui nível adequado de proteção, ainda que levando em consideração eventuais riscos oriundos das possiblidades de exceção em caso de interesse público (COMISSÃO EUROPEIA, 2003; MARQUES, 2020, p. 97).

3.2.3 Andorra (2010).

A decisão de adequação em relação ao sistema jurídico de Andorra foi proferida pela Comissão Europeia em 2010, ainda com base na Diretiva 95/46/EC. A decisão é realizada em atenção à Constituição do Principado de Andorra, de 1993, na *Llei qualificada de protecció de dades personals*, de 2003, e nos Decretos de 2004, sobre registro público para inscrição de arquivos de dados pessoais, e de 2010, referente à agência responsável pela proteção em Andorra, ambos complementares à legislação (COMISSÃO EUROPEIA, 2010).

Não há menção expressa na decisão sobre aspectos relacionados à aplicação do direito à proteção de dados pessoais em matéria de investigação criminal ou para fins de segurança pública em geral (COMISSÃO EUROPEIA, 2010).

A Comissão reconheceu que o sistema jurídico de Andorra possui nível adequado de proteção, ainda que levando em consideração as possiblidades de exceção em casos de interesse público (COMISSÃO EUROPEIA, 2010; MARQUES, 2020, p. 99-100).

3.2.4 Israel (2011).

A decisão de adequação em relação ao sistema jurídico de Israel foi proferida pela Comissão Europeia em 2011, ainda com base na Diretiva 95/46/EC. Para tanto, a Comissão se embasou nas Leis Básicas de Israel, bem como no *Privacy Protection Act* 5741-1981 (COMISSÃO EUROPEIA, 2011).

Não há menção expressa na decisão sobre aspectos relacionados à aplicação do direito à proteção de dados pessoais em matéria de investigação criminal ou para fins de segurança pública em geral (COMISSÃO EUROPEIA, 2011).

A Comissão reconheceu que o sistema jurídico de Israel possui nível adequado de proteção (COMISSÃO EUROPEIA, 2011; MARQUES, 2020, p. 101-102).

3.2.5 Uruguai (2012).

A decisão de adequação em relação ao sistema jurídico uruguaio foi proferida pela Comissão Europeia em 2012, ainda com base na Diretiva 95/46/EC. A avaliação realizada pela Comissão levou em consideração a Constituição da República Oriental do Uruguai, de 1967, a *Ley n.o 18.331 de protección de datos personales y acción de habeas data*, de 2008, e o Decreto n.º 414/009, de 2009, complementar à legislação de 2008.

Não há menção expressa na decisão sobre aspectos relacionados à aplicação do direito à proteção de dados pessoais em matéria de investigação criminal ou para fins de segurança pública em geral (COMISSÃO EUROPEIA, 2012).

A Comissão reconheceu que o sistema jurídico do Uruguai possui nível adequado de proteção, ainda que levando em consideração as possiblidades de exceção em casos de interesse público (COMISSÃO EUROPEIA, 2012; MARQUES, 2020, p. 101-102).

3.2.6 Japão (2019).

A decisão de adequação proferida pela Comissão Europeia em relação ao Japão data de 2019, período em que o GDPR e a Diretiva n.º 2016/680 já estavam em vigência no ordenamento jurídico da União Europeia. Nesta, há tratamento expresso em relação às questões de investigação criminal ou para fins de segurança pública, diferenciando-se imediatamente das decisões anteriores.

A avaliação da Comissão levou em consideração a Constituição japonesa, de 1946, a Lei relativa à proteção de informações pessoais, a Lei relativa à proteção de informações pessoais na posse de órgãos administrativos, e a Lei relativa à proteção de informações pessoais na posse de serviços administrativos legalmente constituídos (COMISSÃO EUROPEIA, 2019).

O texto constante nesta decisão é mais completo e pormenorizado do que a redação constante nas demais decisões avaliadas. Na decisão de adequação voltada ao sistema jurídico japonês, a Comissão Europeia se debruçou com maior ênfase à aplicação do direito à proteção de dados pessoais em matéria de investigação criminal ou para fins de segurança pública (COMISSÃO EUROPEIA, 2019).

A Comissão dedicou o item 3 da decisão ao “acesso e utilização de dados pessoais transferidos da União Europeia por autoridades públicas no Japão”. Neste tópico, foram ressaltadas as declarações do governo japonês se comprometendo com a tutela adequada ao direito à proteção de dados pessoais (COMISSÃO EUROPEIA, 2019). Observa-se, portanto,

a preocupação com a equivalência das garantais de proteção de dados pessoais adotadas pelo país.

No subitem 3.2, a Comissão se aprofundou na legislação atinente ao tratamento de dados pessoais em matéria penal por parte do governo japonês. A decisão realça que o sistema jurídico japonês possui limitações ao acesso e ao uso de dados pessoais, com previsão de atuação de mecanismos de supervisão e possibilidade de recursos, de modo que esteja presente nível adequado de proteção "contra ingerência ilícita e o risco de abusos" (COMISSÃO EUROPEIA, 2019).

No anexo 2 desta decisão de adequação, consta documento enviado pelo Estado japonês à Comissão Europeia contendo ensaio sobre o quadro jurídico relativo à "recolha e utilização de informações pessoais pelas autoridades públicas japonesas para efeitos de aplicação da lei penal e de segurança nacional". O documento enfatiza os limites e as possibilidades constantes na legislação japonesa em matéria de proteção de dados aplicada ao contexto penal, os quais são apreciados pela Comissão no curso da decisão (COMISSÃO EUROPEIA, 2019).

Gnoatton argumenta que a União Europeia demonstrou maior rigidez no exame do nível de adequação do sistema de proteção de dados vigente no Japão. Nesse sentido, a decisão é mais contundente na análise da legislação estrangeira e de suas lacunas. O parâmetro de partido, todavia, como base comparativa, é o regime protetivo europeu (GNOATTON, 2021, p. 102-103).

A Comissão reconheceu que o sistema jurídico japonês possui nível adequado de proteção de dados pessoais para fins de transferências por parte da União Europeia (COMISSÃO EUROPEIA, 2019). Ressalva-se que esta é a primeira decisão de adequação proferida pela Comissão após a aprovação do GDPR e da Diretiva n.º 2016/680.

Ademais, a decisão de adequação ainda estabeleceu condições adicionais necessárias ao livre fluxo de dados pessoais entre União Europeia e Japão. Tais condições são acrescentadas ao regime já vigente de proteção de dados pessoais no Japão e apresentam maior rigidez (MARQUES, 2020, p. 114).

O Anexo 1 da decisão apresenta "normas complementares ao abrigo da lei relativa à proteção de informações pessoais para o tratamento de dados pessoais transferidos da UE com base numa decisão de adequação". A Comissão reconheceu que o sistema jurídico japonês assegura nível adequado de proteção, mas adotou normas complementares diante de diferenças pontuais entre ambos os sistemas protetivos. Tais normas complementares são vinculantes apenas aos "operadores comerciais responsáveis pela gestão de informações

pessoais que recebam dados pessoais transferidos da UE" (União Europeia) (COMISSÃO EUROPEIA, 2019).

Ressalta-se, assim, o campo de aplicação da decisão de adequação e das normas complementares:

> Conforme se vê, a decisão não se estende a todo o Japão, mas limita-se ao âmbito de aplicação da APPI, cuja proteção cobre as informações pessoais tratadas pelos "operadores comerciais responsáveis pela gestão de informações pessoais" (do inglês *Personal Information Handling Business Operators* - PIHBO), segundo os termos estabelecidos na APPI. Nesse quesito, fica de fora da cobertura da legislação e, portanto, da decisão de adequação, as entidades do setor público, as quais são reguladas de forma apartada por legislação específica, chamadas de Lei relativa à proteção de informações pessoais na posse de órgãos administrativos (APPIHAO) e Lei relativa à proteção de informações pessoais na posse de serviços administrativos legalmente constituídos (APPI-IAA) (MARQUES, 2020, p. 114).

Diante do exame das decisões de adequação verificadas nesta pesquisa, observa-se que o caso japonês destoa em relação aos demais no que concerne à ênfase adotada aos aspectos criminais. O maior rigor verificado coincide temporalmente com a vigência no novo regime jurídicos de proteção de dados pessoais, lastreado no GDPR e na Diretiva n.º 2016/680. Restou verificado, neste caso em específico, a maior preocupação da Comissão com as possibilidades de uso por parte das autoridades públicas japonesas dos dados transferidos, notadamente em matéria criminal e de segurança nacional.

3.3 A NECESSIDADE DE RECONHECIMENTO MÚTUO PARA A CONCRETIZAÇÃO DA POSSIBILIDADE DE ACESSO TRANSFRONTEIRIÇO A DADOS INFORMÁTICOS ARMAZENADOS.

Atualmente, a inserção internacional dos Estados para fins de cooperação exige adaptações ao cenário da era digital. A criminalidade cibernética se apresenta como ameaça diante das vulnerabilidades resultantes deste cenário digitalizado (BOWMAN, 1995, p. 1936). Nesse sentido, novos padrões de segurança pública e de garantia aos direitos fundamentais, levando em consideração a capacidade de manipular e armazenar informações, tornam-se cada vez mais relevantes.

Conforme visto, o desenvolvimento tecnológico, ao mesmo tempo em que permite novas possibilidades aos Estados, também apresenta novos desafios. Em relação às tecnologias da informação e da comunicação, se, por um lado, há crescente preocupação com a criminalidade transnacional, por outro, são desenvolvidas novas formas de vigilância e de policiamento. O incremento tecnológico, dessa forma, contribuiu para possibilitar formas

inéditas de aplicação da política criminal para além das fronteiras estatais, facilitando a interlocução entre Estados distintos (ANDREAS; NADELMANN, 2006, p. 248).

Já se argumentou que os dados armazenados por empresas privadas passam a ter um papel cada vez mais importantes para as atividades de investigação criminal, sejam eles cometidos no mundo virtual ou no *offline*. Nesse sentido, a cooperação internacional por meio do acesso transfronteiriço a dados informáticos e do intercâmbio de informações se configura como um elemento estratégico para as autoridades responsáveis pela persecução penal (CARRERA; STEFAN; MITSILEGAS, 2020, p. 1). O acesso transfronteiriço a dados informáticos armazenados inclui o acesso a provas eletrônicas localizadas em território de jurisdição estrangeira. Salienta-se que o rol de dados a serem acessados pode incluir dados pessoais sensíveis, de modo que a autorização deste recurso deve levar em consideração o direito à proteção de dados dos indivíduos.

No ordenamento jurídico brasileiro, o Marco Civil da Internet permite o acesso direto a dados eletrônicos em servidores localizados fora do território nacional, ainda que em termos amplos (DOMINGOS; SILVA; OLIVEIRA, 2020, p. 145). A referida legislação permite operações de coleta, armazenamento, guarda e tratamento de dados pessoais desde que pelo menos um dos terminais esteja localizado no Brasil. A legislação também permite o acesso nas hipóteses em que pessoa jurídica sediada no exterior oferte serviço ao público brasileiro ou que pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil (BRASIL, 2014).[118] Por esta perspectiva, em síntese, o Marco Civil da Internet reconhece a possibilidade de acesso a dados envolvendo jurisdições distintas.

Dessa forma, a despeito do interesse por parte das forças de persecução penal e, em tese, a possibilidade jurídica de se promover o acesso transfronteiriço a dados, ainda persistem problemas com o atraso e com a dificuldade de se concretizar tais instrumentos. Nesse contexto, de acordo com Jennifer Daskal, alguns Estados, entre eles o Brasil e o Reino Unido, desenvolveram legislação que os permitem, unilateralmente, obrigar provedores de internet atuantes em sua jurisdição a fornecer o acesso a dados e informações armazenados em jurisdições estrangeiras (DASKAL, 2016, p. 473).

---

[118] Conforme dispõe o marco civil da internet: Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros (BRASIL, 2014). Nesse sentido: assim, ainda que a operação da empresa ocorra toda no exterior, e ali sejam tomadas as decisões corporativas e mantidos os servidores que coletam e armazenam os dados necessários para a prestação dos serviços, deverá ser observada a legislação brasileira para os dados coletados no Brasil, inclusive quanto às requisições judiciais descritas no artigo 10 (ABREU E SILVA, 2017, p. 115).

Segundo Melissa Garcia Blagitz de Abreu e Silva, o legislador, no Marco Civil da Internet, foi coerente com o posicionamento de que as empresas que prestam serviços no Brasil devem cumprir a legislação nacional. Para a autora, portanto, as negações dos provedores com a sede operacional em outros países, mas constituído sob a lei brasileira, em fornecer dados às autoridades brasileiras não possuiriam fundamento jurídico, quando avaliadas à luz do ordenamento jurídico brasileiro (ABREU E SILVA, 2017, p. 115-116).

Contudo, diante da referida possibilidade jurídica, travam-se o que Jacqueline de Souza Abreu denomina "*jurisdictional battles for digital evidence*". Isto é, o interesse das autoridades de persecução penal em obter acesso a informações armazenadas em servidores localizados em território estrangeiro é contraposto pela negativa das entidades que armazenam estes dados (ABREU, 2018, p. 233-234).

De acordo com Abreu, o principal argumento para a negativa contra as requisições das autoridades penais brasileiras reside em dois pontos: a) os dados estão armazenados em servidores localizados em território estrangeiro; e b) a entidade localizada em território nacional não possui o controle efetivo sobre o acesso às informações requisitadas (ABREU, 2018, p. 237-238).[119]

Nesse sentido, uma alternativa possível é a formalização de acordos internacionais de assistência jurídica mútua, esclarecendo a coordenação entre Estados em relação às entidades privadas que armazenam os dados de interesse. Estes mecanismos, todavia, são caracterizados como soluções lentas diante das novo contexto informacional em que se inserem os Estados (ABREU, 2018, p. 234).

Abreu e Silva defende a aplicação da regra do controle para fins de acesso transfronteiriço a dados, de modo que "terá jurisdição para requisitar dados diretamente o Estado em que a empresa que controla os dados presta serviços, independente do local físico em que mantidos seus equipamentos e armazenados os documentos" (ABREU E SILVA, 2017, p. 116).

O critério do controle, defendido pela autora, pode ser compreendido pela premissa de que aqueles que possuem o controle efetivo sobre os dados devem fornecê-los, independentemente do local em que estes dados estão fisicamente armazenados (ABREU E

[119] No que tange à cooperação internacional entre Brasil e Estados Unidos, Abreu verificou que: ISPs [provedor de serviço de internet] claim that a U.S. warrant is necessary for the disclosure, because they are bound by U.S. law. Then, they refer to the MLAT. In opposition, law enforcement agents (and many courts) have argued that if the company – subsidiary or not – offers services, that is, makes business in Brazil, then Brazilian law applies. The implication claimed – but disputed – is that Brazilian courts have authority to compel production of data held by these ISPs, without deference to the MLAT (ABREU, 2018, p. 237-238; o termo entre colchetes é de minha autoria).

SILVA, 2017, p. 107). São dois os argumentos apresentados por Abreu e Silva para reforçar a opção pelo critério do controle no contexto do acesso transfronteiriço a dados informáticos armazenados:

> Existem duas razões principais para a adoção do critério controle. A primeira delas é a realidade da prova eletrônica. Dados e documentos eletrônicos são, por essência, móveis. Eles podem ser armazenados em qualquer lugar e também podem ser movimentados para qualquer lugar, a qualquer tempo, em questão de minutos, com um único clique. Eles podem ser movidos para o território de um Estado observador de obrigações internacionais, para Sealand ou para o alto mar. Com frequência, é impossível determinar onde os dados estão fisicamente localizados (servidores que utilizam redes de anonimato como TOR 2 e i2p, por exemplo), ou mesmo autenticar a localização declarada (nem todos os servidores de internet são transparentes quanto ao local de sua operação). A lei não pode ignorar a realizada e o único critério disponível hoje é controle. Em segundo lugar, o critério controle preserva a territorialidade e a soberania dos Estados. Uma empresa não pode ser constituída, manter escritórios ou subsidiárias, ou prestar serviços em um país, dirigidos especificamente a seus residentes, sem se submeter à lei local. Do contrário, empresas não apenas poderiam escolher a jurisdição, como também a lei que as regula, escolhendo aquela que mais lhes favorece, não necessariamente aquela que melhor protege seus consumidores e usuários. Se é inconcebível que uma empresa possa prestar qualquer tipo de serviço físico sem obedecer à lei local, o mesmo é válido para empresas de internet. O modelo de negócios possui peculiaridades, mas não demanda tratamento preferencial (ABREU E SILVA, 2017, p. 116).

Não se propõe, nesta pesquisa, investigar a competência jurisdicional para fazer valer as requisições de acesso a dados informáticos localizados em território estrangeiro. Embora se trate de problemática importante, entende-se que a dificuldade de se determinar a localização própria dos dados informáticos (DASKAL *apud* ABREU, 2018, p. 244)[120] e as constantes inovações tecnológicas exigem investigação a partir de outros critérios metodológicos. A preocupação central está na necessidade de aplicação do direito à proteção de dados a este instrumento de política criminal que transcende as fronteiras físicas dos Estados.

Aduz-se que o acesso a dados pessoais localizados em jurisdições estrangeiras produz riscos aos direitos humanos, notadamente ao direito à privacidade e à liberdade de expressão e de associação. Segundo Daskal, evidenciam-se riscos na medida em que a coleta de dados pode fornecer arcabouço de informações capaz de possibilitar novos meios de

---

[120] Sobre o assunto, Daskal aduz que a mobilidade internacional de dados informáticos não depende necessariamente da ação dos usuários, de modo que possa haver deslocamento em razão de decisões de roteamento técnico. Ademais, o armazenamento de dados normalmente é realizado em mais de um servidor, havendo a possibilidade de cada qual estar localizado em território sob a jurisdição de Estado distinto. Por fim, o processamento de dados não depende da sua localização, de sorte que o seu uso pode ser realizado a partir de outro território (DASKAL *apud* ABREU, 2018, p. 244). De acordo com Abreu: Both the U.S. and Brazilian governments have capitalized precisely on this normative disconnect in the cases explored. In their assertions of authority to compel data, location of the bits is said to be irrelevant. The U.S. government considers that the location of data, in general, does not constrain the scope of applicability of the SCA and, in the specific case, does not constrain the authority to compel production of data stored abroad via a U.S. warrant. Meanwhile, Brazil rejects that the location of data ought to have any relevance in determining the rules that apply to a specific case setting. These assertions are not unreasonable, given the "un-territoriality" of data (ABREU, 2018, p. 245).

intervenções estatais abusivas, facilitando, por exemplo, perseguições políticas ou a instrumentalização de mecanismos de vigilância contra opositores (DASKAL, 2016, p. 481-482).

Daskal reconhece, todavia, que muitos Estados não possuem as garantias à proteção de dados pessoais necessárias para se obter acesso a dados localizados em países integrantes do sistema da União Europeia. A falta de harmonização legislativa entre os Estados interessados na cooperação internacional em matéria de proteção de dados, portanto, torna os procedimentos de acesso a dados localizados em jurisdições estrangeiras mais lentos (DASKAL, 2016, p. 483).

De maneira semelhante, conforme aponta Rui Soares Pereira, observa-se que o acesso transfronteiriço a dados informáticos para fins de persecução penal, especialmente quando praticado de forma unilateral, apresenta riscos aos indivíduos. Todavia, diante das demandas impostas pela criminalidade transnacional contemporânea, o compartilhamento de dados pela via da cooperação internacional oferece soluções mais céleres entre as autoridades responsáveis pela persecução penal (PEREIRA, 2019, p. 270).[121]

É possível argumentar, nesse sentido, que as disputas entre as entidades controladoras dos dados armazenados e as autoridades penais em torno do acesso transfronteiriço a dados informáticos armazenados podem ser solucionadas mediante acordo internacional que reconheça mutuamente, entre outros aspectos, a adequada tutela ao direito à proteção de dados pessoais.

Retomando os princípios da cooperação jurídica internacional, de acordo com Abade, os modelos de cooperação podem ser concretizados sob p paradigma de confiança e de reconhecimento mútuo. Os mecanismos de coordenação entre os Estados partem do pressuposto de que há relativa proximidade entre os sistemas jurídicos em contato. Isto é, o processo de harmonização legislativa para compatibilizar as regras atinentes aos instrumentos de cooperação representaria avanço na interlocução entre os Estados (ABADE, 2013, p. 57-58).

Segundo Fábio Bechara, a preocupação com a tutela dos direitos fundamentais é um dos elementos a ser observado na garantia de segurança e de confiança entre as partes

[121] Observando o ordenamento jurídico português, Rui Soares Pereira apresenta a seguinte conclusão sobre a possibilidade de acesso unilateral a dados informáticos armazenados em servidores localizados em jurisdição estrangeira: Para além dos riscos de os acessos transfronteiriços não contemplarem as garantias de segurança necessárias, tal como já detetado pelo Transborder Group em 2014, cremos que será mais avisado continuar a fazê-lo no quadro dos mecanismos da cooperação judiciária internacional enquanto se aguarda pela elaboração (reclamada pela doutrina) de princípios gerais relevantes em matéria de perseguição criminal transnacional e de standards sobre a forma de lidar com a prova transnacional (PEREIRA, 2019, p. 270).

envolvidas na cooperação jurídica internacional (BECHARA, 2012, p. 51). A simplificação procedimental, como ocorre em uma modalidade de acesso transfronteiriço a dados informáticos, embora ofereça solução mais eficiente para a tutela penal, deve estar em consonância com os direitos humanos.

A construção de confiança mútua entre os agentes envolvidos na cooperação internacional, destarte, é um processo necessário diante da "intensa mutabilidade das relações humanas no tempo e no espaço" (BECHARA, 2012, p. 52). A confiança mútua pode ser desenvolvida a partir da solidariedade entre os Estados, com o estabelecimento de identidades comuns resultantes, entre outros aspectos, de valores compartilhados a serem tutelados (BECHARA, 2012, p. 52-53). Dessa forma:

> A definição dos direitos humanos como valor universal teve por objetivo influenciar os sistemas nacionais à incorporação de determinados valores como padrão ou modelo, cuja equivalência entre o direito interno e o direito internacional independe do aspecto plural que caracteriza a sociedade mundial. Este fundo de valores comuns compreende a dignidade do homem, as liberdades, a ordem do bem-estar, o nível de vida, o nível de benefícios, o acesso aos benefícios, na expressão da Declaração Universal dos Direitos Humanos de 1948 (BECHARA, 2012, p. 52-53).

Verificou-se, portanto, a existência de duas demandas: a primeira, de cooperação internacional em matéria penal diante da fluidez dos dados e informações pessoais em jurisdições distintas, para fins de enfrentamento da criminalidade cibernética; e, a segunda, de haver garantias mútuas relativas à existência de um sistema de proteção de dados pessoais aplicável ao contexto de persecução penal. As duas demandas se impõem no cenário atual em razão de o compartilhamento de dados pessoais e o acesso transfronteiriço implicarem em riscos aos titulares dos dados e a terceiros que de alguma maneira são envolvidos.

A despeito de parte da literatura reconhecer que a possibilidade de acesso transfronteiriço a dados informáticos armazenados já encontra previsão no ordenamento jurídico brasileiro (DOMINGOS; SILVA; OLIVEIRA, 2020, p. 145; DASKAL; 2016, p. 473; ABREU E SILVA, 2017, p. 115-116), nas hipóteses em que o requerimento da autoridade competente brasileira é realizado a pessoa jurídica prestadora de serviço no Brasil, entende-se que o cenário internacional apresenta condicionantes mais rígidas.

Conforme já observado, a Diretiva n.º 2016/680 da União Europeia, conjugada com o GDPR, condiciona o livre fluxo de dados pessoais ao reconhecimento por parte das instituições europeias à necessidade de o país receptor possuir nível adequado de proteção de dados (UNIÃO EUROPEIA, 2016-B). Percebe-se que, formalmente, é necessário haver coordenação bilateral para se promover as transferências internacionais de dados pessoais, incluindo quando para finalidades de persecução penal.

Acrescenta-se a este aspecto, a decisão de adequação proferida pela Comissão Europeia em relação ao Japão, em 2019, examinada no subitem anterior deste capítulo. Nesta, restou evidenciado a preocupação da Comissão com as possibilidades e limitações ao uso dos dados por parte das autoridades públicas japonesas, bem como estabeleceu-se normas complementares sobre o uso de dados a serem transferidos (COMISSÃO EUROPEIA, 2019). Para além da decisão de adequação, restou-se relevante a coordenação entre o Estado japonês e a integração europeia em matéria de proteção de dados pessoais.

De acordo com o relatório *Cross-border data access in criminal proceedings and the future of digital justice*:

> Nenhuma decisão de adequação deve ser adotada caso seja descoberto que esses terceiros países não asseguram um nível adequado de proteção de direitos humanos, nem oferecem salvaguardas apropriadas. Na ausência uma decisão de adequação, transferências de dados pessoais somente podem ocorrer se baseadas nos procedimentos e mecanismos previstos por um instrumento legalmente vinculante (como por exemplo um acordo MLA) que garante as salvaguardas apropriadas para a proteção de dados pessoais (CARRERA, STEFAN, MITSILEGAS, 2020, p. 78).[122]

Adiante, uma vez considerado que tanto a legislação da União Europeia, manifestada pelo *General Data Protection Regulation* e pela Diretiva n.º 2016/680, assim como a Lei Geral de Proteção de Dados Pessoais brasileira, condicionam às transferências internacionais de dados pessoais à existência de nível adequado de proteção no país receptor, entende-se que uma modalidade de cooperação jurídica internacional baseada no compartilhamento de dados, tal qual a prevista na Convenção de Budapeste, dependerá de harmonização normativa em matéria de proteção de dados pessoais.

Adicionalmente, o Segundo Protocolo Adicional à Convenção de Budapeste, de 2022, reconheceu que a coleta de evidências eletrônicas para fins de investigação criminal pode produzir impactos contra os dados pessoais. Por essa razão, nos termos do protocolo, torna-se necessário que as partes possuam sistemas de proteção de dados capazes de atender às obrigações constitucionais e internacionais no que tange à cooperação jurídica internacional (CONSELHO DA EUROPA, 2022-C).

Sobre a aplicabilidade do Segundo Protocolo ao regime europeu, Carrera, Stefan e Mitsilegas argumentam que o fortalecimento dos mecanismos de acesso a dados informáticos armazenados em outros Estados com vistas ao enfrentamento da criminalidade cibernética não

[122] Tradução livre da versão original: No adequacy decisions should be adopted on finding that these third countries do not ensure an adequate level of protection of human rights, nor provide for appropriate safeguards. In the absence of an adequacy decision, transfers of personal data may only take place based on the procedures and mechanisms provided by a legally binding instrument (i.e. an MLA agreement) that provides appropriate safeguards to protect personal data (CARRERA, STEFAN, MITSILEGAS, 2020, p. 78).

pode estar em dissonância com a legislação europeia (CARRERA, STEFAN, MITSILEGAS, 2020, p. 78).

Ademais, o Segundo Protocolo Adicional indicou que o direito à proteção de dados pessoais se tornou ser elemento integrante do modelo de cooperação jurídica internacional de Budapeste. Já no preâmbulo, houve destaque no referido instrumento de que a cooperação internacional em matéria penal é beneficiada pela existência de salvaguardas e de garantias à proteção dos direitos humanos (CONSELHO DA EUROPA, 2022-C).

Diante das condicionantes formais estabelecidas no âmbito da União Europeia e da legislação brasileira, é possível concluir que a concretização da modalidade de acesso transfronteiriço a dados informáticos, prevista na Convenção de Budapeste, depende do reconhecimento mútuo que há nível adequado de proteção de dados entre os dois sistemas jurídicos.

CONCLUSÃO

Em um cenário em que o enfrentamento do cibercrime assume cada vez mais importância na esfera internacional, a proteção de dados pessoais contra abusos potencialmente praticáveis por entidades públicas e privadas se torna uma demanda. Diante dessa constatação, esta pesquisa problematizou como realizar a proteção de dados pessoais para que o acesso transfronteiriço a dados informáticos armazenados no âmbito da União Europeia e do Brasil seja uma possibilidade concreta.

Nesta dissertação, partiu-se do pressuposto de que a criminalidade cibernética representa um risco contemporâneo. Seguindo as premissas da sociedade de risco de Ulrich Beck, considerou-se os crimes cibernéticos como riscos derivados do próprio avanço econômico e tecnológico da humanidade, o qual produziu novas ameaças. A fluidez e o caráter transnacional dos crimes virtuais os qualificam como um desafio à sociedade internacional.

Argumentou-se que a antecipação de ameaças futuras motiva demandas por maiores diligências em prol da segurança. Contudo, conforme abordado no primeiro capítulo, tais providências podem constituir elas próprias novos riscos aos indivíduos. Especificamente em relação aos riscos decorrentes das inovações na tecnologia da informação, menciona-se as novas possibilidades de coleta, armazenamento, tratamento e transferência de dados pessoais por parte de entidades públicas e privadas. Nesse sentido, identificou-se no segundo capítulo que o desenvolvimento das tecnologias da informação e da comunicação ampliou e aprofundou os mecanismos de vigilância potencialmente aplicáveis aos indivíduos.

Observou-se, a partir destas premissas, crescente preocupação com a segurança da informação e com a proteção dos dados pessoais. No segundo capítulo, evidenciou-se que à medida que os dados pessoais são mais produzidos, coletados, armazenados e transacionados entre diferentes atores, cada vez mais eles se constituem informações úteis para investigações criminal, notadamente em relação aos crimes cibernéticos que alcançam escala transfronteiriça.

Levando em consideração que os crimes cibernéticos podem facilmente ultrapassar os limites territoriais de um Estado, identificou-se a demanda internacional de enfrentamento conjunto ao cibercrime. Tornou-se necessário, destarte, o desenvolvimento de soluções pautadas na cooperação jurídica internacional. Nesse contexto, a Convenção de Budapeste de 2001 é o principal instrumento internacional voltado à temática. Contudo, as medidas de cooperação internacional – ou de uma política criminal transnacional –, notadamente o acesso transfronteiriço a dados informáticos armazenados, também podem constituir um risco aos

direitos fundamentais dos indivíduos, entre eles o direito à privacidade e o direito à proteção de dados pessoais.

Salientando-se o relatório de *Cross-border data access in criminal proceedings and the future of digital justice*, de Carrara, Stefan e Mitsilegas, há a preocupação latente de que o fortalecimento de mecanismos de cooperação jurídica internacional para o combate à criminalidade cibernética não configure em si uma ameaça aos direitos fundamentais da população (CARRERA, STEFAN, MITSILEGAS, 2020, p. 76-78). Nesse sentido, o Direito Penal deve se pautar como limite da política criminal transnacional que se manifesta a partir da cooperação jurídica entre os Estados, de modo a assegurar a adequada tutela dos direitos humanos.

Ao longo do segundo capítulo, evidenciou-se a partir da revisão bibliográfica princípios de ordem garantistas necessários para a proteção de dados pessoais para fins penais, os quais também devem ser aplicados no curso da cooperação jurídica internacional em matéria penal. Trata-se dos princípios da proporcionalidade, da legalidade e da finalidade vinculada, os quais devem limitar o exercício da persecução criminal, com vistas a garantir que o Direito Penal os limites dos direitos fundamentais com a finalidade de tutelar os bens jurídicos afetados pelo cibercrime (COMISSÃO DE DIREITO INTERNACIONAL, 2006, P. 224; TOSCHI; LOPES, 2020, p. 102; VIANA; MONTENEGRO; GLEIZER, 2020, p. 3;)

Diante dos riscos ligados à transferência internacional de dados para fins de enfrentamento da criminalidade cibernética, inovações institucionais ganharam relevo na última década. Identificou-se, ao longo da pesquisa, 3 elementos que demonstram a preocupação da União Europeia com a destinação dos dados pessoais de cidadãos europeus transferidos a terceiros países: a) os casos Schrems I e II; b) a *General Data Protection Regulation* e a Diretiva n.º 2016/680; e c) a decisão de adequação relativa ao Japão. A estes 3, acrescenta-se o Segundo Protocolo Adicional à Convenção da Budapeste, no âmbito do Conselho da Europa, que prevê expressamente a necessidade observação ao direito à proteção de dados pessoais entre as partes envolvidas no processo de cooperação jurídica, seja ele previsto em acordo bilateral/multilateral específico ou nos termos da Protocolo Adicional.

Examinou-se no segundo e no terceiro capítulo a Diretiva n.º 2016/680 da União Europeia. O documento, que dispõe especificamente sobre o tratamento de dados pessoais por parte das autoridades públicas para fins de prevenção, investigação, detecção ou repressão de infrações penais ou exceção de sanções penais, estabelece requisitos para que Estados não membros da União Europeia tenham acesso a dados pessoais de cidadãos europeus para as finalidades descritas pela diretiva.

A possibilidade de acesso transfronteiriço a dados armazenados em território estrangeiro, prevista na Convenção de Budapeste, insere-se nos parâmetros da Diretiva, conforme descrito no terceiro capítulo. Ainda que a legislação brasileira permita que o referido acesso seja realizado de maneira unilateral, nas hipóteses em que a pessoa jurídica controladora preste serviços em território nacional, com fundamento em interpretação do Marco Civil da Internet, entende-se que, ao envolver jurisdições e cidadãos de nacionalidade diversa, deve haver coordenação prévia entre os Estados envolvidos. A cooperação internacional em matéria penal, portanto, deve levar em consideração o direito à proteção de dados pessoais para sua concretização.

As decisões de adequação proferidas pela Comissão Europeia, avaliadas no terceiro capítulo, permitem identificar algumas conclusões. Com exceção do caso japonês, nenhuma das decisões anteriores analisadas abordou com profundidade a aplicação do direito à proteção de dados pessoais às investigações criminais. Entende-se que esta maior rigidez coincide com a positivação da GDPR e da Diretiva n.º 2016/680. A partir de então, observou-se maior preocupação da integração europeia com os dados pessoais dos cidadãos europeus em estados terceiros. Especificamente no caso concernente ao Japão, verificou-se na decisão de adequação um aprofundamento da análise da Comissão no que tange os usos dos dados pessoais por parte das autoridades públicas japonesas para fins penais e de segurança pública.

Uma vez destacada a crescente preocupação com a proteção de dados pessoais na esfera da persecução penal, entende-se que a cooperação internacional em matéria penal para o enfrentamento do cibercrime, nos moldes previstos pela Convenção de Budapeste, exige coordenação entre os países no que tange ao regime de tutela de dados. Isto é, uma vez que os instrumentos de auxílio mútuo previstos em Budapeste dependem do fluxo internacional de dados pessoais, notadamente a modalidade de acesso transfronteiriço a dados informáticos armazenados, a existência de restrições à circulação de informações comprometeria celeridade da atuação das autoridades penais.

O reconhecimento da devida tutela do direito à proteção de dados pessoais, assegurada por ambas as partes envolvidas na cooperação jurídica internacional, poderia facilitar as tratativas a nível internacional e favorecer a realização da medida de acesso transfronteiriço a dados informáticos armazenados. Tal possibilidade parte do pressuposto de que as partes possuem, em seus sistemas jurídicos, as garantias necessárias para a proteção dos direitos fundamentais tangenciados pelas atividades de cooperação jurídica internacional em matéria penal.

Esta coordenação se reflete na harmonização legislativa em torno do direito à proteção de dados pessoais aplicado ao contexto criminal. Torna-se fundamental, assim sendo, que o Brasil e a União Europeia, no âmbito da cooperação jurídica para lidar com a criminalidade cibernética, reconheçam mutuamente que ambos os regimes jurídicos possuem nível adequado de proteção de dados pessoais. Havendo este reconhecimento, entende-se que a aplicação de medidas investigativas como o acesso transfronteiriço a dados informáticos armazenados encontraria menos obstáculos em sua concretização, especialmente ao envolver entidades privadas na posição de controladora de dados.

Tal harmonização legislativa, contudo, não deve ser traduzida em mera recepção acrítica de padrões normativos exteriores. Ainda que necessária à cooperação jurídica internacional, segundo os termos propostos nesta dissertação, as garantias de proteção de dados pessoais estabelecidas no sistema jurídico brasileiro devem levar as particularidades históricas e culturais da sociedade brasileira.

Dessa maneira, esta pesquisa conclui que o reconhecimento mútuo de que há entre as partes um nível adequado de proteção de dados pessoais é essencial para concretizar a possibilidade de acesso transfronteiriço a dados informáticos armazenados em servidores localizados em países da União Europeia, segundo o modelo de cooperação previsto na Convenção de Budapeste.

Esta dissertação adotou a perspectiva de que a definição qualitativa do que é nível adequado de proteção, no âmbito das relações entre o Brasil e os Estados membros da União Europeia, depende justamente de critérios estabelecidos pelas próprias partes. Trata-se de definição realizada institucionalmente pela parte. No caso da União Europeia, depende, em grande medida, das decisões de adequação, abordadas no capítulo 3.2. No entanto, conforme se depreendeu da decisão referente ao caso japonês, acordo adicional entre as partes pode vir a se tornar necessário para formalizar o reconhecimento mútuo.

Por essa razão, a título propositivo, para além da decisão de adequação por parte da instituição competente europeia, a elaboração de acordo internacional específico sobre a proteção de dados pessoais no contexto do acesso transfronteiriço de dados para fins de investigação criminal pode materializar de maneira positiva a necessidade de reconhecimento mútuo entre as partes.

Reconhece-se, igualmente, a importância do aprofundamento dos estudos em torno da aplicação do direito à proteção de dados pessoais em matéria de cooperação jurídica internacional para fins de investigação criminal, com o objetivo de esclarecer tal campo

temático e de propor novas soluções de prevenção contra abusos aos direitos humanos e de aprofundamento da coordenação entre Estados.

REFERÊNCIAS

ABADE, Denise Neves. **Direitos fundamentais na cooperação jurídica internacional**: Extradição, assistência jurídica, execução de sentença estrangeira e transferência de presos. Versão digital [ebook]. São Paulo: Saraiva, 2013.

ABADE, Denise Neves. **Análise da coexistência entre carta rogatória e auxílio direto na assistência jurídica internacional**. In: Brasil. Ministério Público Federal. Secretaria de Cooperação Internacional. Temas de Cooperação Internacional. 2ª ed. Brasília: MPF, 2016.

ABRAHA, Halefom H. **Law enforcement access to electronic evidence across borders**: mapping policy approaches and emerging reform initiatives. International Journal of Law and Information Technology, 2021, vol. 29, p. 118–153.

ABREU, Jacqueline de Souza. **Jurisdictional battles for digital evidence, MLAT reform, and the Brazilian experience**. RIL Brasília a. 55 n. 220 out./dez. 2018 p. 233-257.

ABREU E SILVA, Melissa Garcia Blagitz de. **Internet e Jurisdição, Acesso Transfronteiriço a Dados e o Caso Irlanda Microsoft**. Revista Eletrônica de Direito Penal e Política Criminal – UFRGS, vol. 5, n.º 1, 2017. Disponível em: https://seer.ufrgs.br/index.php/redppc/article/view/73172/45842. Acesso em 27/05/2022.

ACCIOLY, Hildebrando; NASCIMENTO E SILVA, Geraldo; CASELLA, Paulo Borba. **Manual de Direito Internacional Público**. 16. ed. São Paulo: Saraiva, 2008.

ALBUQUERQUE, Roberto Chacon de. **A criminalidade informática**. São Paulo: Juarez de Oliveira, 2006.

ALVES, David Alexandre Ribeirinho. **O acesso transfronteiriço a dados informáticos em processo penal**. 2020. Dissertação (Mestrado em direito e Prática Jurídica) – Universidade de Lisboa. Lisboa: 2020.

AMARAL JÚNIOR, Alberto do. **Curso de Direito Internacional Público**. São Paulo: Atlas, 2011.

AMBOS, Kai. **Prosecuting international crimes at the national and international levels**: between justice and realpolitik. In: KALECK, Wolfgang. et al (eds.). International Prosecution of Human Rights Crimes. Part II. Berlin: Springer Verlag, 2007.

AMBOS, Kai. **Treatise on International Criminal Law**. Volume 1: Foundations and General Part. Oxford University Press: 2013.

ANDREAS, Peter; NADELMANN, Ethan. **Policing the globe**: criminalization and crime control in international relations. Oxford University Press: 2006.

ARAÚJO, Nádia. **A importância da cooperação jurídica internacional para a atuação do Estado brasileiro no plano interno e internacional**. In: BRASIL. Secretaria Nacional de Justiça. Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional. Manual de cooperação jurídica internacional e recuperação de ativos: cooperação em matéria

penal. Brasília: Ministério da Justiça, 2012. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/pedido-de-cooperacao-1/manuais-de-atuacao-1/manual-de-atuacao-drci-materia-penal. Acesso em 13/06/2022.

ARAS, Vladimir Barros. **A título de introdução**: segurança pública e investigações criminais na era da proteção de dados. In: ARAS, Vladmir; MENDONÇA, Andrey Borges; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA; Marcos Antônio da Silva [Orgs.]. Proteção de dados pessoais e investigação criminal. Brasília: ANPR, 2020.

ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. **Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations.** 1970. Disponível em: https://undocs.org/en/A/RES/2625(XXV). Acesso em 20/05/2022.

BARBOSA, Karlos Alves. **Sociedade de risco e os crimes de perigo abstrato**. 2012. Dissertação (Mestrado em Direito) – Universidade Federal de Uberlândia. Uberlândia: 2012.

BAUMAN, Zygmunt. **Globalização**: As consequências humanas. Rio de Janeiro: Zahar. 1999.

BAUMAN, Zygmunt. **Medo líquido**. Rio de Janeiro: Zahar. 2008.

BAUMAN, Zygmunt. **Modernidade Líquida**. Rio de Janeiro: Zahar, 2001.

BAUMAN, Zygmunt. **O mal-estar da pós-modernidade**. Rio de Janeiro: Zahar, 1998.

BECHARA, Fábio Ramazzini. **Cooperação Jurídica Internacional em Matéria Penal**: Eficácia da Prova Produzida no Exterior. Tese (Doutorado em Direito) – Universidade de São Paulo. São Paulo: Saraiva, 2009.

BECHARA, Fábio Ramazzini. **Cooperação judicial internacional**: equilíbrio entre eficiência e garantismo. In: In: BRASIL. Secretaria Nacional de Justiça. Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional. Manual de cooperação jurídica internacional e recuperação de ativos: cooperação em matéria penal. Brasília: Ministério da Justiça, 2012. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/pedido-de-cooperacao-1/manuais-de-atuacao-1/manual-de-atuacao-drci-materia-penal. Acesso em 13/06/2022.

BECK, Ulrich. **La sociedade del riesgo**: Hacia una nueva modernidad. Barcelona: Paidós, 2002.

BECK, Ulrich. **Power in the Global Age**: A new global political economy. Malden: Polity Press, 2005.

BECK, Ulrich. **Sociedade de risco mundial**: em busca da segurança perdida. Edições 70, 2015.

BECK, Ulrich. **The Cosmopolitan Vision**. Malden: Polity Press, 2006.

BECK, Ulrich. **World at Risk**. Malden: Polity Press, 2009.

BIONI, Bruno; EILBERG, Daniela Dora; CUNHA, Brenda; SALIBA, Pedro; VERGILI, Gabriela. **Proteção de dados no campo penal e de segurança pública**: nota técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2020.

BOBBIO, Norberto. **A Era dos Direitos**. Rio de Janeiro: Elsevier, 2004.

BOWMAN, M. E. **Is International Law Ready for the Information Age**? Fordham International Law Journal, vol. 19, 5, p. 1935-1946. 1995.

BRADFORD, Anu. **The Brussels Effect**. NorthWestern University Law Review, v. 107, n. 1, p. 1-68, 2012. Disponível em: https://scholarship.law.columbia.edu/faculty_scholarship/271. Acesso em: 17/06/2022.

BRANDÃO, Luiza Couto Chaves. **Fluxo Transnacional de Dados**: estruturas, políticas e o Direito nas vertentes da governança. 2020. Dissertação (Mestrado em Direito). Universidade Federal de Minas Gerais. Belo Horizonte: 2020.

BRASIL. Agência Nacional de Telecomunicações. **Segurança Cibernética**. 2022. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica. Acesso em 12/08/2022.

BRASIL. **Aprovada adesão do Brasil à Convenção sobre o Crime Cibernético**. Agência Senado. 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico. Acesso em 07/03/2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 02/06/2022.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 30/03/2022.

BRASIL. **Estratégia Nacional de Segurança Cibernética**. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em 21/06/2021.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 30/03/2022.

BRASIL. **Lei n.º 8.078, de 11 de setembro de 1990**. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 09/05/2022.

BRASIL. **Lei nº 9504, de 30 de setembro de 1997**. Estabelece normas para as eleições. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L9504.htm. Acesso em 30/03/2022.

BRASIL. **Lei nº 9.983, de 14 de julho de 2000**. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9983.htm. Acesso em 30/03/2022.

BRASIL. **Lei nº 10.695, de 01 de julho de 2003**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/l10.695.htm. Acesso em 03/03/2022.

BRASIL. **Lei nº 11.829, de 25 de novembro de 2008**. Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm. Acesso em: 30/03/2022.

BRASIL. **Lei n.º 12.527, de 18 de novembro de 2011**. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 04/05/2022.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. 2012-A. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 30/03/2022.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 18/05/2022.

BRASIL. **Lei nº. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 04/05/2022.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em 03/03/2022.

BRASIL. **Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública – Adesão do Brasil à Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001**. Nota à imprensa n.º 186. 2022. Disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica-2013-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico-celebrada-em-budapeste-em-23-de-novembro-de-2001. Acesso em 02/12/2022.

BRASIL. **Processo de adesão à Convenção de Budapeste – Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública**. Nota 309. Ministério das Relações Exteriores. 2019. https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2019/processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica. Acesso em 20/06/2021.

BRASIL. Secretaria Nacional de Justiça. Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional. **Manual de cooperação jurídica internacional e recuperação de ativos: cooperação em matéria penal**. Brasília: Ministério da Justiça, 2012-B. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/pedido-de-cooperacao-1/manuais-de-atuacao-1/manual-de-atuacao-drci-materia-penal. Acesso em 13/06/2022.

BRASIL. Secretaria Nacional de Justiça. Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional. **Indicadores DRCI/SENAJUS/MJSP – 2021**. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/cooperacao-internacional/estatisticas/indicadores/indicadores-drci-2021-cooperacao-juridica-intermacional.pdf. Acesso em 13/06/2022.

BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 - Distrito Federal**. Relatora: Min. Rosa Weber. 07 de maio de 2020. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em 13/05/2022.

BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental 722 – Distrito Federal**. Relatora: Min. Cármen Lúcia. 20 de agosto de 2020. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344764619&ext=.pdf. Acesso em 03/05/2022.

BURT, Andrew. **Nowhere to hide**: Data, Cyberspace, and the dangers of the Digital World. Yale Law School: Information Society Project. Nova York: 2020. Disponível em: https://law.yale.edu/sites/default/files/area/center/isp/documents/white_paper_2020_nowhere_to_hide_burt_yls_isp_digital_future.pdf. Acesso em 09/05/2022.

BUZAN, Barry; HANSEN, Lene. **A evolução dos estudos de segurança internacional**. Tradução Flávio Lira. São Paulo: Editora da Unesp, 2012.

BUZAN, Barry; WÆVER, Ole; DE WILDE, Jaap. **Security**: A New Framework for Analysis. Boulder: Lynne Rienner, 1998.

CALABRICH, Bruno Freire de Carvalho. **O conceito de tratamento de dados pessoais e o acórdão Lindqvist, do Tribunal de Justiça da União Europeia**. Revista Tribunal Regional Federal 1ª Região, ano 31, n. 2. Brasília: 2019. Disponível em: https://rtrf1.emnuvens.com.br/trf1/article/view/103/92. Acesso em 09/05/2022.

CANCELIER, Mikhail Vieira de Lorenzi. **Infinito Particular**: Privacidade no século XXI e a manutenção do direito de estar só. 2016. Tese (Doutorado em Direito) – Universidade Federal de Santa Catarina. Florianópolis: 2016.

CARMO, Valter Moura do. **A cooperação judicial entre os países do MERCOSUL**: estudo comparativo com a União Europeia a partir dos casos brasileiro e espanhol. 2021. Tese (Doutorado em Direito) – Universidade Federal de Santa Catarina. Florianópolis: 2021.

CARRERA, Sergio; STEFAN, Marco. **Access to Electronic Data for Criminal Investigations Purposes in the EU**. CEPS Paper in Liberty and Security in Europe, n. 2020-01. 2020. Disponível em: https://www.ceps.eu/wp-content/uploads/2020/02/LSE20120-01_JUD-IT_Electronic-Data-for-Criminal-Investigations-Purposes.pdf. Acesso em 17/05/2022.

CARRERA, Sergio; STEFAN, Marco; MITSILEGAS, Valsamis. **Cross-border data access in criminal proceedings and the future of digital justice**: Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic. Report of CEPS and QMUL Task Force. Centre for European Policy Studies (CEPS): Bruxelas, 2020.

CASIMIRO, Sofia de Vasconcelos. **Novas guerras em novos campos de batalha**: o RGPD Europeu e as gigantes tecnológicas norte-americanas. In: WACHOWICZ, Marcos [org.]. Proteção de Dados Pessoais em perspectiva: LGPD e RGPD na ótica do Direito Comparado. Curitiba: Gedai, UFPR, 2020.

CASSESE, Antonio. **International Criminal Law**. Oxford University Press: 2003.

CASTRO, José Roberto Wanderley. **A tipicidade dos crimes cibernéticos no direito penal brasileiro**: um estudo sobre o impacto da Lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos. 2018. 231f. Tese (doutorado) – Universidade Federal de Pernambuco. Recife, 2018.

CATALA, P. **Ébauche d'une théorie juridique de l'information**. In : Le droit à l'épreuve du numérique. Jus ex Machina, coll. "Droit, Éthique, Société", p. 224-244, Paris, 1998. Disponível em: https://mafr.fr/fr/article/ebauche-dune-theorie-juridique-de-linformation. Acesso em 08/05/2022.

CAVALCANTI, Natália Peppi. **Acesso a dados além das fronteiras**: a cooperação jurídica internacional como solução para o (aparente) conflito de jurisdições. Dissertação (Mestrado em Direito). 2019. Instituto Brasiliense de Direito Público (IDP). Brasília: 2019.

CERVINI, Raúl; TAVARES, Juarez. **Princípios de Cooperação Judicial Penal Internacional no Protocolo do Mercosul**. São Paulo: Revista dos Tribunais, 2000.

CLEMENTINO, Marco Bruno Miranda. **A Cooperação Jurídica Internacional em Matéria Penal-Tributária como instrumento de repressão à criminalidade organizada transnacional**: globalização e novos espaços de juridicidade. 2013. 375f. Tese (Doutorado em Direito). Universidade Federal de Pernambuco, Recife, 2013.

CLOUGH, Jonathan. **A world of difference**: the Budapest Convention on cybercrime and the challenges of harmonisation. 2014. Monash University Law Review, vol. 40, nº.3, p. 698-736. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2615789. Acesso em 13/06/2022.

CLOUGH, Jonathan. **Principles of Cybercrime**. Cambridge University Press: Nova York, 2010.

CÓDIGO de Cooperação Interjurisdicional para Ibero-américa. Revista da SJRJ, Rio de Janeiro, n. 25, 2009, p. 429-456. Disponível em: https://www.jfrj.jus.br/sites/default/files/revista-sjrj/arquivo/22-67-1-pb.pdf. Acesso em 02/06/2022.

COMISSÃO DE DIREITO INTERNACIONAL. **Yearbook of the international law commission**. Report of the Commission to the General Assembly on the work of its fifty-eighth session. Nações Unidas: Nova York e Genebra, 2013. Disponível em: https://legal.un.org/ilc/publications/yearbooks/english/ilc_2006_v2_p2.pdf. Acesso em 17/05/2022.

COMISSÃO ECONÔMICA PARA A AMÉRICA LATINA E O CARIBE (CELAC). **Internet & Jurisdiction and ECLAC Regional Status Report 2020**. Santiago: 2020. Disponível em: https://repositorio.cepal.org/bitstream/handle/11362/46421/1/S1901092_en.pdf. Acesso em 18/05/2022.

COMISSÃO EUROPEIA. **Comunicação n.º COM/2017/07**. Comunicação da Comissão ao Parlamento Europeu e ao Conselho: Intercâmbio e proteção de dados pessoais num mundo globalizado. 2017. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=COM%3A2017%3A7%3AFIN. Acesso em 16/06/2022.

COMISSÃO EUROPEIA. **Decisão 2002/2/EC. C(2001) 4359**. 2001. Disponível em: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32002D0002. Acesso em 05/06/2022.

COMISSÃO EUROPEIA. **Decisão 2003/490/EC. C(2003) 490**. 2003. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003D0490. Acesso em 05/06/2022.

COMISSÃO EUROPEIA. **Decisão 2010/635/EU. C(2010) 7084**. 2010. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010D0625. Acesso em 05/06/2022.

COMISSÃO EUROPEIA. **Decisão 2011/61/EU. c(2011) 332**. 2011. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011D0061. Acesso em 05/06/2022.

COMISSÃO EUROPEIA. **Decisão 2012/484/EU. C(2012) 5704**. 2012. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32012D0484. Acesso em 05/06/2022.

COMISSÃO EUROPEIA. **Decisão 2019/419/EU. C(2019) 304**. 2019. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC. Acesso em: 05/06/2022.

COLOMBO, Matteo. **Regolamento UE sulla Privacy**: principi generali e ruolo del data protection officer. 3. ed. Milão: CreateSpace, 2015.

CONSELHO DA EUROPA. **Chart of signatures and ratifications of Treaty 185**. 2022-A. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185. Acesso em 31/05/2022.

CONSELHO DA EUROPA. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)**. 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108. Acesso em 08/05/2022.

CONSELHO DA EUROPA. **Convention on Cybercrime**. 2001-A. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Acesso em: 20/06/2021.

CONSELHO DA EUROPA. **Explanatory Report to the Convention on Cybercrime**. 2001-B. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b. Acesso em: 20/06/2021.

CONSELHO DA EUROPA. **Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence**. 2022-B. Disponível em: https://rm.coe.int/1680a49c9d. Acesso em 27/06/2022.

CONSELHO DA EUROPA. **Handbook on European data protection law**. Luxembourg: Publications Office of the European Union, 2018. Disponível em: https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf. Acesso em 17/05/2022.

CONSELHO DA EUROPA. **Recommendation n. º R (95) 13 of the Committee of Ministers to member states concerning problems of criminal procedural law connected with information technology**. 1995. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76. Acesso em 27/06/2022.

CONSELHO DA EUROPA. **Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence**. 2022-C. Disponível em: https://rm.coe.int/1680a49dab. Acesso em 27/06/2022.

CONSELHO DA EUROPA. Comitê da Convenção sobre Cibercrime. **Transborder access and jurisdiction**: What are the options? Estrasburgo: 2012. Disponível em: https://rm.coe.int/16802e79e8. Acesso em 16/06/2022.

CRESPO, Marcelo. **Proteção de Dados Pessoais e o Poder Público**: noções essenciais. In: CRAVO, Daniela Copetti; CUNDA, Daniela Zago Gonçalves da; RAMOS, Rafael [orgs]. Lei Geral de Proteção de Dados e o poder público. Porto Alegre: Escola Superior de Gestão e Controle Francisco Juruena; Centro de Estudos de Direito Municipal, 2021.

DASKAL, Jennifer. **Law Enforcement Access to Data Across Borders**: The Evolving Security and Rights Issues. Journal of National Security Law & Policy, vol. 8:473, 2016. Disponível em: https://jnslp.com/wp-content/uploads/2017/10/Law-Enforcement-Access-to-Data-Across-Borders_2.pdf. Acesso em 27/05/2022.

DATA PROTECTION AND PRIVACY COMMISSIONERS. **The protection of personal data and privacy in a globalized world**: a universal right respecting diversities. Montreux Declaration. 28º Conferência Internacional. 2006. Disponível em: https://globalprivacyassembly.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf. Acesso em 17/05/2022.

DELERUE, François. **Cyber Operations and International Law**. Cambridge University Press: 2020.

DELGADO, Vladimir Chaves. **Cooperação internacional em matéria penal na convenção sobre o cibercrime**. Dissertação (Mestrado em Direito). Centro Universitário de Brasília. Brasília: 2007.

DELMAS-MARTY. **Les forces imaginatives du droit**: Le relative et l'universel. Paris: Seuil, 2004.

DELMAS-MARTY, Mireille. **Les forces imaginatives du droit (II)**: Le pluralisme ordonné. Paris: Seuil, 2006.

DÍEZ RIPOLLÉS, José Luis. **De la sociedad del riesgo a la seguridad ciudadana: Un debate desenfocado**. In: MELIÁ, M.C.; DÍEZ, Gómez-Jara. Derecho Penal del Enemigo: El discurso penal de la exclusión. Vol. 1. São Paulo: Livraria dos advogados, 2006.

DIPP, Gilson. **A cooperação jurídica internacional e o Superior Tribunal de Justiça**: comentários à Resolução n.º 9/02. In: BRASIL. Secretaria Nacional de Justiça. Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional. Manual de cooperação jurídica internacional e recuperação de ativos: cooperação em matéria penal. Brasília: Ministério da Justiça, 2012. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/pedido-de-cooperacao-1/manuais-de-atuacao-1/manual-de-atuacao-drci-materia-penal. Acesso em 13/06/2022.

DOMINGOS, Fernanda Teixeira Souza; SILVA, Melissa Garcia Blagitz de Abreu e; OLIVEIRA, Neide M. Cavalcanti Cardoso de. **Transferência internacional de dados pessoais para fins de investigações criminais à luz das Leis de Proteção de Dados Pessoais**. In: ARAS, Vladmir; MENDONÇA, Andrey Borges; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA; Marcos Antônio da Silva [Orgs.]. Proteção de dados pessoais e investigação criminal. Brasília: ANPR, 2020.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJJL], 12(2), 91–108. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em 09/05/2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, Danilo et. al. [orgs.]. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

ESCRITÓRIO DAS NAÇÕES UNIDAS SOBRE DROGAS E CRIME. **Comprehensive Study on Cybercrime**. United Nations: Viena, 2013. Disponível: https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf. Acesso em 14/06/2021.

EUROPEAN DATA PROTECTION BOARD. **Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive**. 2021. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_en. Acesso em 18/05/2022.

EUROPOL. **Internet Organized Crime Threat Assessment (IOCTA)**. European Agency for Law Enforcement Cooperation. 2020. Disponível em: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020. Acesso em 14/06/2021.

FALEIROS JÚNIOR, José Luiz de Moura. **Governança de Dados e o Poder Público**: Perspectivas à luz da Lei Geral de Proteção de Dados Pessoais. In: CRAVO, Daniela Copetti; CUNDA, Daniela Zago Gonçalves da; RAMOS, Rafael [orgs]. Lei Geral de Proteção de Dados e o poder público. Porto Alegre: Escola Superior de Gestão e Controle Francisco Juruena; Centro de Estudos de Direito Municipal, 2021.

FERRAJOLI, Luigi. **Direito e Razão**: teoria do garantismo penal. São Paulo: Revista dos Tribunais, 2010.

FLÔRES, Mariana Rocha de; SILVA, Rosane Leal da. **Desafios e perspectivas da proteção de dados pessoais sensíveis em poder da Administração Pública**: entre o dever público de informar e o direito do cidadão de ser tutelado. Revista de Direito. Viçosa. ISSN 2527-0389. V. 12, n. 02, 2020.

GENDEREN, Rob van den Hoven. **Cybercrime investigation and the protection of personal data and privacy**. Conselho da Europa. 2008. Disponível em: https://rm.coe.int/16802fa3a3. Acesso em 17/05/2022.

GIDDENS, Anthony. **The consequences of modernity**. Stanford: Stanford University, 1990

GNOATTON, Letícia Mulinari. **A conformidade da Autoridade Nacional de Proteção de Dados aos critérios exigidos pela União Europeia para a concessão de decisão de adequação ao Brasil nos termos do Regulamento Geral de Proteção de Dados**. 2021. Dissertação (Mestrado em Direito) – Universidade Federal de Santa Catarina. Florianópolis: 2021.

GRADY, Mark F; PARISI, Francesco [orgs]. **The Law and Economics of Cybersecurity**. Cambridge University Press: 2006.

GREENLEAF, G. **The influence of European data privacy standards outside Europe**: implications for globalization of convention 108. International Data Privacy Law, Oxford University Press, v. 2, n. 2, p. 68–92, 2012.

GOOGLE. **Política de Privacidade**. Disponível em: https://policies.google.com/privacy?hl=pt-BR#infosharing. Acesso em 26/06/2022.

GROSSI, Viviane Ceolin Dallasta Del. **A defesa na cooperação jurídica internacional penal**. 2014. Dissertação (Mestrado em Direito) – USP. Universidade de São Paulo: São Paulo, 2014.

GUBERT, Paulo Soares Campeão. **A eficácia das redes de cooperação jurídica direta no combate à corrupção transnacional e sua concretização pelo sistema processual brasileiro**: notas sobre a Operação Lava-Jato. 2019. Dissertação (Mestrado em Direito) – Universidade Federal do Espírito Santo. Vitória: 2019.

HANSEN, Lene; NISSENBAUM, Helen. **Digital Disaster, Cyber Security, and the Copenhagen School**. International Studies Quarterly, vol. 53, p. 1155–75. 2009.

HÄRTER, Karl. **The Transnationalisation of Criminal Law in the Nineteenth and Twentieth Century**: Political Crime, Police Cooperation, Security Regimes and Normative Orders: an Introduction. In: HÄRTER, Karl; HANNAPPEL, Tina; TYRICHTER, Jean Conrad [orgs.]. The Transnationalisation of Criminal Law in the Nineteenth and Twentieth Century: Political Crime, Police Cooperation, Security Regimes and Normative Orders. Frankfurt am Main: Klostermann, 2019. Disponível em: https://www.academia.edu/39435373/The_Transnationalisation_of_Criminal_Law_in_the_Nineteenth_and_Twentieth_Century_Political_Crime_Police_Cooperation_Security_Regimes_and_Normative_Orders_an_Introduction. Acesso em 07/10/2021.

HUREL, L. M. **Cibersegurança no Brasil**: uma análise da estratégia nacional. Instituto Igarapé: 2021. Disponível em: https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf. Acesso em 10/08/2022.

HUREL, L. M.; LOBATO, L. Cruz. **A Strategy for Cybersecurity Governance in Brazil**: Strategic Note 30. Instituto Igarapé: Rio de Janeiro, 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2019/01/A-Strategy-for-Cybersecurity-Governance-in-Brazil.pdf. Acesso em 14/06/2021.

INTERPOL. **Constitution of the ICPO-INTERPOL**. 1956. Disponível em: https://www.interpol.int/Who-we-are/Legal-framework/Legal-documents. Acesso em 18/05/2022.

JERMAN-BLAŽIČ, Borka; KLOBUČAR, Tomaž. **A New Legal Framework for Cross-Border Data Collection in Crime Investigation amongst Selected European Countries**. International Journal of Cyber Criminology, v. 13, 2, jun. 2019.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

JUNIOR, Ademar Pozzatti. **Cooperação internacional como acesso à justiça nas relações internacionais**: os desafios do direito brasileiro para a implementação de uma cultura cosmopolita. 2015. Tese (Doutorado em Direito) – Universidade Federal de Santa Catarina. Florianópolis: 2015.

JUNIOR, Antonio Coêlho Soares. **O princípio da legalidade penal**: o que se fala e o que se cala. 2002. Dissertação (Mestrado em Direito). Universidade Federal de Santa Catarina. Florianópolis: 2002.

JUNIOR, Francisco de Assis do Rego Monteiro Rocha. **A legalidade penal constitucional filtrada**: uma análise da jurisprudência do Supremo Tribunal Federal. Constituição, Economia e Desenvolvimento: Revista da Academia brasileira de Direito Constitucional, vol. 11, n. 21, p. 167-197, ago-dez, 2019. Curitiba: 2020. Disponível em: https://abdconst.com.br/revista22/Artigo%207%20-%20167-197%20%20Francisco%20Monteiro.pdf. Acesso em 04/05/2022.

JÚNIOR, Paulo Abrão Pires. **O papel da cooperação jurídica internacional**. In: BRASIL. Secretaria Nacional de Justiça. Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional. Manual de cooperação jurídica internacional e recuperação de ativos: cooperação em matéria penal. Brasília: Ministério da Justiça, 2012. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/pedido-de-cooperacao-1/manuais-de-atuacao-1/manual-de-atuacao-drci-materia-penal. Acesso em 13/06/2022.

KOOPS, Bert-Japp. **Police investigations in Internet open sources**: Procedural-law issues. Computer Law & Security Review, v. 29, n.º 6, dez. 2013, pp. 654 a 665. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364913001660. Acesso em 26/06/2022.

KOSKENNIEMI, Martti. **The Politics of International Law**. In: European Journal of Internationa Law. v. 01, n. 01, 1990, p. 04 – 32.

KOSKENNIEMI, Martti. **The Gentle Civilizer of Nations**: The Rise and Fall of International Law 1870–1960. New York: Cambridge University Press, 2001.

KOSKENNIEMI, Martti. **From apology to utopia**: the structure of international legal argument. New York: Cambridge University Press, 2005.

KOSSEFF, Jeff. **Cybersecurity Law**. Hoboken: Wiley, 2020.

KREMLING, Janine; PARKER, Amanda M. Sharp. **Cyberspace, Cybersecurity, and Cybercrime**. Thousand Oaks : SAGE Publications, 2017.

LOBATO, Luísa Cruz; KENKEL, Kai Michael. **Discourses of cyberspace securitization in Brazil and in the United States**. Rev. Bras. Polít. Int. 58, 2: 23-43, 2015.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. **Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa**. Revista de Direito de Viçosa, v. 12, n. 02, 2020. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em 08/05/2022.

LUHMANN, Niklas. **El concepto de riesgo**. Barcelona: Anthropos, 1996.

LUHMANN, Niklas. **Risk**: A Sociological Theory. Nova York: de Gruyter, 1993.

LONG, William RM; SCALI, Géraldine; BLYTHE, Francesa; e RAUL, Alan Charles. **EU Overview**. In: RAUL, Alan Charles (org.). The Privacy, Data Protection and Cybersecurity Law Review. 6ª edição. Law Business Research: 2019.

LYNSKEY, Orla. **The Foundations of EU Data Protection Law**. Oxford University Press, 2015.

MARQUES, Fernanda Mascarenhas. **Regulação do fluxo de dados pessoais entre fronteiras**: Os contornos e limites da Decisão de Adequação de países terceiros. 2020. Dissertação (Mestrado em Direito e Desenvolvimento) – Fundação Getúlio Vargas, Escola de Direito de São Paulo. São Paulo: 2020.

MARQUES, João. "**And [they] built a crooked h[arbour]" – the Schrems ruling and what it means for the future of data transfers between the EU and US**. UNIO – EU Law Journal, vol. 2, n.º 2, jun. 2016, p. 54-70. Disponível em: http://www.unio.cedu.direito.uminho.pt/Uploads/UNIO%20-%202%20Eng/Joao_Marques.pdf. Acesso em 19/05/2022.

MARQUES, Paulo Rubens Carvalho; BARRETO, Paulo Coutinho; NETO, Octávio Celso Gondim Paulo. **O anteprojeto da "LGPD penal", a (in)segurança pública e a (não) persecução penal**. In: ARAS, Vladmir; MENDONÇA, Andrey Borges; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA; Marcos Antônio da Silva [Orgs.]. Proteção de dados pessoais e investigação criminal. Brasília: ANPR, 2020.

MARTÍNEZ, Rosa Ana Morán. **Garantías requeridas en la UE para la transferencia de datos a terceros países en la cooperación judicial penal internacional**. In: ARAS, Vladmir; MENDONÇA, Andrey Borges; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA; Marcos Antônio da Silva [Orgs.]. Proteção de dados pessoais e investigação criminal. Brasília: ANPR, 2020.

MASSENO, Manuel David. **Na borda**: dados pessoais e não pessoais nos dois regulamentos da União Europeia. In: WACHOWICZ, Marcos [org.]. Proteção de Dados Pessoais em perspectiva: LGPD e RGPD na ótica do Direito Comparado. Curitiba: Gedai, UFPR, 2020.

MEDEIROS, Carlos Henrique Pereira de. **Direito Penal na "sociedade mundial de riscos" - Uma aproximação da crise da ciência penal frente às exigências do contemporâneo**. Disponível em: https://www.mpba.mp.br/sites/default/files/biblioteca/criminal/artigos/penal-constitucional/direito_penal_na_sociedade_mundial_de_riscos-_uma_aproximacao_da_crise_da_ciencia_penal_frente_as_exigencias_do_contemporaneo_-_carlos_henrique_pereira_de_medeiros.pdf. 10/05/2022.

MENDES, Laura Schertel; JÚNIOR, Otavio Luiz Rodrigues; FONSECA, Gabriel Campos Soares. **O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais**: rumo a um direito fundamental autônomo. In: DONEDA, Danilo et. al. [orgs.]. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

MOROZOV, Evgeny. **Big Tech**: A ascensão dos dados e a morte da política. Tradução: Claudio Marcondes. São Paulo: Ubu, 2018.

MUELLER, Gerhard. **International Judicial Assistance in Criminal Matters**. In: MUELLER, Gerhard; WISE, Edward (orgs.). International Criminal Law. New Jersey: Rothman Ed., 1965.

MURPHY, Maria Helen. **Assessing the implications of Schrems II for EU-US data flow**. International & Comparative Law Quarterly, vol. 71, Issue 1, jan. 2022, pp. 245 – 262. Disponível em: https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/assessing-the-implications-of-schrems-ii-for-euus-data-flow/71E5412185BA0AE59B9F1AE1CFB6B97B. Acesso em 19/05/2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **The right to privacy in the digital age**. A/RES/68/167. 2013. Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/449/47/PDF/N1344947.pdf?OpenElement. Acesso em 17/05/2022.

ORGANIZAÇÃO PARA A COOPERAÇÃO E O DESENVOLVIMENTO EECONÔMICO. **A Caminho da Era Digital no Brasil**. OECD Publishing: Paris, 2020.

ORGANIZAÇÃO PARA A COOPERAÇÃO E O DESENVOLVIMENTO ECONÔMICO. **Report on the cross-border enforcement of privacy law**. 2006. Disponível em: https://www.oecd.org/digital/ieconomy/37558845.pdf. Acesso em 27/05/2022.

ORGANIZAÇÃO PARA A COOPERAÇÃO E O DESENVOLVIMENTO ECONÔMICO. **The OECD Privacy Framework**. 2013. Disponível em: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em 18/04/2022.

PEREIRA, Rui Soares. **O acesso (unilateral e sem recurso a mecanismos de cooperação judiciária internacional) a dados armazenados em sistemas informáticos localizados no estrangeiro**. Revista de Estudios Europeos, n. extraordinário monográfico, I-2019. 2019. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=7109709. Acesso em 27/05/2022.

PESSOA, João Pedro Seefeldt. **O efeito Orwell na sociedade em rede**: cibersegurança, regime global de vigilância social e direito à privacidade no século XXI. Porto Alegre, RS: Editora Fi, 2020.

PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Saraiva, 2013.

PRADO, Luiz Regis. **Bem jurídico-penal e Constituição**. São Paulo: Revista dos Tribunais, 2013.

RAMOS, André de Carvalho. **Pluralidade das ordens jurídicas: uma nova perspectiva na relação entre o Direito Internacional e o Direito Constitucional**. R. Fac. Dir. Univ. São Paulo v. 106/107 p. 497 - 524 jan./dez. 2011/2012

RODOTÀ, Stefano. **Tecnologie e diritti**. Bologna: Il Mulino, 1995.

RODRIGUES, Luiz Fernando. **A importância do compartilhamento de dados pessoais para fins de investigação criminal e os possíveis reflexos da LGPD**. In: ARAS, Vladmir; MENDONÇA, Andrey Borges; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA; Marcos Antônio da Silva [Orgs.]. Proteção de dados pessoais e investigação criminal. Brasília: ANPR, 2020.

RODRIGUES ARAÚJO, A. M. **As transferências transatlânticas de dados pessoais: o nível de proteção adequado depois de Schrems**. Revista Direitos Humanos e Democracia, [S. l.], v. 5, n. 9, p. 201–236, 2017. DOI: 10.21527/2317-5389.2017.9.201-236. Disponível em: https://www.revistas.unijui.edu.br/index.php/direitoshumanosedemocracia/article/view/6058. Acesso em: 14/09/2022.

RODRIGUES ARAÚJO, A. M. **The Right to Data Protection and the Comissions' Adequacy Decision**. UNIO - EU Law Jounal. Vol. 1, No. 1, 2015, p. 77-93. Disponível em: http://www.unio.cedu.direito.uminho.pt/Uploads/UNIO%201/The%20Right%20to%20Data%20Protection%20and%20the%20Commissions%20Adequacy%20Decision_formatado.pdf. Acesso em 14/09/2022.

ROXIN, Claus. **La evolución de la Política criminal, el Derecho Penal y el Proceso Penal**. Valencia: Tirant lo Blanch, 2000.

ROXIN, Claus. **Política Criminal e Sistema Jurídico-Penal**. Rio de Janeiro: Renovar. 2000.

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

SANTOS, Boaventura de Sousa. **A globalização e as ciências sociais**. São Paulo: Cortez. 2002.

SANTOS, Paulo Ernani Bergamo dos. **Direito internacional e o combate à cibercriminalidade contra crianças**. In: BRASIL. Ministério Público Federal. Crimes cibernéticos. 2ª Câmara de Coordenação e Revisão, Criminal. MPF: Brasília, 2018. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em 14/06/2021.

SETZER, V. W. **Dado, informação, conhecimento e competência**. DataGramaZero, v. 0, n. 0, 1999. Disponível em: http://hdl.handle.net/20.500.11959/brapci/7327. Acesso em: 08/05/2022.

SIEBER, Ulrich. **Legal aspects of computer-related crime in the information society**. European Comission. University of Würzburg, 1998. Disponível em: http://www.oas.org/juridico/english/COMCRIME%20Study.pdf. Acesso em 20/03/2022.

SIERRA, Joana de Souza. **A não responsabilização dos provedores de aplicações de internet por conteúdos gerados por terceiros como ruptura dos sistemas tradicionais de responsabilidade civil**: notice and takedown e marco civil da internet. 2018. Dissertação (Mestrado em Direito) – Universidade Federal de Santa Catarina. Florianópolis: 2018.

SILVA, Alexandre Pereira da. **Direito internacional penal (direito penal internacional?)**: breve ensaio sobre a relevância e transnacionalidade da disciplina. Rev. Fac. Direito UFMG, Belo Horizonte, n. 62, pp. 53 - 83, jan./jun. 2013.

SILVA, Carlos Bruno Ferreira da. **La transferencia de datos entre la Unión Europea y la administración pública brasileña**: análisis de la "protección adecuada" de los datos personales en Brasil conforme a los parámetros de la directiva 95/46/CE. 2013. Tese (Doutorado em Direito). Universidade de Sevilla. Sevilla: 2013.

SMITH, Robert Ellis. **Privacy**: How to protect what's left of it. New York: Anchor Press, 1979.

SWENSEN, Dilon. **Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems**: Where Do We Go From Here?. Maryland Journal of International Law, vol. 36, issue 1. Disponível em: https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1719&context=mjil. Acesso em 19/05/2022.

TIBURCIO, Carmem. DOLINGER, Jacob. **Direito Internacional Privado**. 15ª ed. Rio de Janeiro: Forense, 2010.

TIMMERS, Paul. **The technological Construction of Sovereignty**. In: Werthner, Hannes; Prem, Erich; Lee, Edward A.; Ghezzi, Carlo. Perspectives on Digital Humanism. Springer: Cham, 2020.

TOSCHI, Aline Seabra; LOPES, Herbert Emílio Araújo. **Dados de Troia**. In: ARAS, Vladmir; MENDONÇA, Andrey Borges; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA; Marcos Antônio da Silva [Orgs.]. Proteção de dados pessoais e investigação criminal. Brasília: ANPR, 2020.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em 04/05/2022.

UNIÃO EUROPEIA. Comissão Europeia. **Decisão de Execução (UE) 2016/1250, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Privacy Shield UE-EUA, com fundamento na Diretiva 95/46/CE**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016D1250. Acesso em 02/05/2022.

UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em 09/05/2022.

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, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho**.

2016-B. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016L0680. Acesso em: 16/01/2022.

UNIÃO EUROPEIA. Corte Europeia de Direitos Humanos. **Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15)**. Recorrente: Big Brother Watch e Outros. Recorrido: Reino Unido. Presidente: Juiz Linos-Alexandre Sicilianos. Estrasburgo, França, 13 de setembro de 2018. Disponível em: http://hudoc.echr.coe.int/eng?i=001-186048. Acesso em 10/02/2022.

UNIÃO EUROPEIA. **Tratado sobre o Funcionamento da União Europeia**. 2012. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A12012E%2FTXT. Acesso em 16/06/2022.

UNIÃO EUROPEIA. Tribunal de Justiça. **Acórdão do processo n.º C-362-14**. Maximillian Schrems contra Data Protection Comissioner. 2015. Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=169195&mode=req&pageIndex=1. Acesso em 19/05/2022.

UNIÃO EUROPEIA. Tribunal de Justiça. **Acórdão do processo n.º C-311/18**. Data Protection Commissioner contra Facebook Ireland Ltd e Maximillian Schrems. 2020. Disponível em: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62018CJ0311&qid=1606742479317. Acesso em 19/05/2022.

UNIÃO EUROPEIA. Tribunal de Justiça. **Acórdão do processo n.º C-101/01**. 2003. Disponível em: http://publications.europa.eu/resource/cellar/bcc476ae-43f8-4668-8404-09fad89c202a.0009.02/DOC_1. Acesso em: 03/05/2022.

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)**. 2016-A. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em 07/03/2022.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES. **Understanding Cybercrime**: Phenoma, challenges and legal responde. ITU: 2012. Disponível em: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf. Acesso em 14/06/2021.

VALERIANO, Brandon; MANESS, Ryan. **International relations theory and cyber security**: Threats, conflicts, and ethics in an emergent domain. In: BROWN, Chris; ECKERSLEY; Robyn. The Oxford Handbook of International Political Theory. Oxford University Press: 2018.

VALES, Tiago Pedro. **Brazil´s cyberspace politics**: Combining emerging threats with old intentions. Politikon: IAPSS Political Science Journal, vol. 29, 2016.

VASCONCELOS, Francisco Victor. **A segurança jurídica da computação em nuvem**: responsabilidade jurídica na proteção de dados digitais por parte dos provedores de aplicação

de internet. 2017. Dissertação (Mestrado em Direito) – Universidade Federal de Santa Catarina: Florianópolis: 2017.

VERDELHO, Pedro. **Obtaining digital evidence in the global world**. EU Law Journal, vol. 5, n.º 2, July 2019, p. 136-145.
VERGUEIRO, Luiz Fabricio Thaumaturgo. **Implementação da Cooperação Jurídica Internacional**. 2012. Tese (Doutorado em Direito) – Universidade de São Paulo. São Paulo: 2012.

VERMEULEN, G.; DE BONDT, W.; RYCKMAN, C. [orgs.]. **Rethinking international cooperation in criminal matters in the EU**. IRCP research series, vol. 42. Comissão Europeia, 2012.

VIANA, Eduardo; MONTENEGRO, Lucas; GLEIZER, Orlandino. **A esfera protegida dos dados pessoais e as intervenções informacionais do Estado**: A dogmática constitucional aplicada ao tratamento de dados na Segurança Pública e no Processo Penal – Diretrizes técnicas para subsidiar Policy Paper. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2020.

VIANA, Marco Túlio. **Fundamentos de direito penal informático: do acesso não autorizado a sistemas computacionais**. Rio de Janeiro: Forense, 2003.

VIOLA; Mario. **Transferência de dados entre Europa e Brasil**: Análise da Adequação da Legislação Brasileira. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2019. Disponível em: https://itsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf. Acesso em 17/05/2022.

VIOLA, Mario; HERINGER, Leonardo; CARVALHO, Celina. **O anteprojeto da LGPD Penal e as regras sobre transferência internacional de dados pessoais**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2021. Disponível em: https://itsrio.org/wp-content/uploads/2021/07/Relatorio-Transferencia-de-dados-pessoais.pdf. Acesso em 18/04/2022.

WACHOWICZ, Marcos [org.]. **Proteção de Dados Pessoais em perspectiva**: LGPD e RGPD na ótica do Direito Comparado. Curitiba: Gedai, UFPR, 2020.

WADE, Marianne L. **General Principles of Transnationalised Criminal Justice**? Exploratory Reflections. Utrecht Law Review, vol. 9, 4, set. 2013.

WAEVER, Ole. **Aberystwyth, Paris, Copenhagen New 'Schools' in Security Theory and Their Origins between Core and Periphery**. In: TICKNER, Arlene B.; BLANEY, David L. [orgs.]. Thinking international relations differently. Nova York: Routledge, 2012.

WANG, Qianyun. **A Comparative Study of Cybercrime in Criminal Law**: China, US, England, Singapore and the Council of Europe. Tese (doutorado) – Erasmus University Rotterdam. Rotterdam, 2016.

WARREN, Samuel D; BRANDEIS, Louis D. **The Right to privacy**. Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220. Disponível em:

https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em 25/04/2022.

WERTHNER, Hannes; PREM, Erich; LEE, Edward A.; GHEZZI, Carlo. **Perspectives on Digital Humanism**. Springer: Cham, 2020.

WHITMAN, James Q. **The Two Western Cultures of Privacy**: Dignity versus Liberty. Yale Law School: Public Law & Legal Theory Research Paper Series, Research Paper nº 64. 2003. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=476041. Acesso em 10/05/2022.

WIENER, Norbert. **Cibernética e Sociedade**: o uso humano de seres humanos. Editora Cultrix: São Paulo, 1954.

WOLFRUM, Rüdiger. **International law of cooperation**. In: Encyclopedia of Public International Law. Amsterdam: North-Holand, 1986.

ZIMMERMANN, Robert. **La Coopération Judiciaire Internationale en Matière Pénale**. 3 ed. Berna: Stämpfli, 2009.