O CONGELAMENTO DE DADOS INFORMÁTICOS PARA FINS DE PROVA NO PROCESSO PENAL

COMPUTER DATA PRESERVATION (QUICK FREEZE) FOR EVIDENTIARY PURPOSES IN CRIMINAL PROCEEDINGS

Vladimir Aras[1]
UFBA

Resumo
O autor examina o tema do congelamento de dados para fins probatórios no processo penal e o procedimento para obtê-los validamente no Brasil. Para atingir tal objetivo, a abordagem se vale da revisão bibliográfica sobre os conceitos de dados cadastrais, dados de conexão e dados de conteúdo comunicacional. Em seguida, analisa as definições de preservação e conservação de dados para a persecução criminal, revisitando as fontes normativas pertinentes, especialmente o Marco Civil da Internet e a Convenção do Conselho da Europa sobre Cibercrimes, concluída em

[1] Doutor em Direito pelo Centro Universitário de Brasília (2023), com a tese O Dever de Requerer Cooperação Internacional, é mestre em Direito Público pela Universidade Federal de Pernambuco (2003), com dissertação sobre a Convenção de Budapeste sobre Cibercriminalidade, e graduado em Direito pela Universidade Católica do Salvador (1992). Tem MBA em Gestão Pública pela Fundação Getúlio Vargas (2016). Cursou a Capacitación para Fiscales de América Latina (2007) no Centro de Estudios de Justicia de las Américas (CEJA) e o Regime Global Antitterrorismo na DiploFoundation (2009). Fez capacitação pelo Programa Nacional de Capacitação e Treinamento para o Combate à Corrupção e à Lavagem de Dinheiro (PNLD) do Ministério da Justiça. Cursou o 16 Programa de Treinamento sobre a Convenção das Nações Unidas contra a Corrupção (UNCAC) em 2013, no United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (Unafei), em Tóquio, tendo sido visiting expert do mesmo programa em 2017. É professor assistente de Processo Penal da Universidade Federal da Bahia (UFBA). É professor colaborador do Mestrado Profissional em Direito e do LL.M. em Direito Penal Econômico do IDP.

Budapeste, em 2001. O texto discute os diferentes graus de proteção aos dados pessoais e os requisitos mais ou menos rigorosos para acessá-los no interesse da investigação criminal. Estabelecidas essas premissas, o autor analisa as medidas investigativas de natureza cautelar, cuja finalidade é a preservação imediata de dados informáticos e os requisitos mínimos para obtê-los, mediante a aplicação das fontes jurídicas discutidas. Conclui-se que a legislação brasileira é compatível com a Constituição e parcialmente com o regime convencional, devendo ser interpretada pelos tribunais de modo a permitir a preservação imediata e posterior acesso a provas digitais sobre crimes graves, com as salvaguardas necessárias à privacidade e à proteção de dados pessoais.

Palavras-chave

Guarda de dados. Preservação de dados. Congelamento expedito. Marco Civil da Internet. Convenção de Budapeste. Privacidade. Autorização judicial

Abstract

The author examines data freezing for evidentiary purposes in criminal proceedings and the procedure for validly obtaining them in Brazil. To achieve this objective, a literature review in made on the concepts of subscriber data, traffic data and content data. The author then analyzes the definitions of data preservation and conservation for criminal prosecution, revisiting the relevant normative sources, especially the Civil Rights Act for the Internet and the Council of Europe Convention on Cybercrime, concluded in Budapest in 2001. This article discusses the different degrees of protection for personal data and the more or less stringent requirements for accessing them in a criminal investigation. Having established these premises, the author turns to the examination of the investigative measures of a provisional nature, whose purpose is the immediate preservation of computer data and the requirements to obtain them, through the application of the legal sources discussed. It is concluded that Brazilian legislation is compatible with the Constitution and partially with the treaty regime, and should be interpreted by the courts in such a way as to allow law enforcement agencies' later access to digital evidence on serious crimes, with safeguards for privacy and the protection of personal data.

Keywords

Data retention. Data preservation. Quick freeze. Digital Rights Framework. Budapest Convention. Privacy. Court warrant.

1 INTRODUÇÃO

A investigação de crimes comuns ou de cibercrimes depende cada vez mais do acesso a provas digitais, que têm natureza intangível. Reconhecendo esse problema, a Convenção sobre Cibercriminalidade, de 2001, estende seu alcance probatório aos crimes informáticos próprios, aos crimes informáticos impróprios e também aos crimes não relacionados a sistemas informáticos, mas cuja prova possa ser feita por meios digitais. (COUNCIL OF EUROPE, 2001, p. 21-22).

Aprovado em 2014, as mais do que óbvias inspirações do Marco Civil da Internet (MCI) (BRASIL, 2014) foram a Constituição Federal de 1988 (notadamente o art. 5º, com sua carta de direitos), as convenções internacionais de direitos humanos (mais particularmente o Pacto de São José da Costa Rica, de 1969), as recomendações do Comitê Gestor da Internet no Brasil – conhecidas como "Princípios para a governança e uso da Internet" (CGI, 2009) – e a Diretiva 95/46/CE da União Europeia, de 1995, então vigente (UNIÃO EUROPEIA, 1995) relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (ARAS, 2014). Essa diretiva foi revogada pelo Regulamento Geral de Proteção de Dados, aprovado em 27 de abril de 2016, e conhecido como GDPR. (UNIÃO EUROPEIA, 2016).

Contudo, o marco mais notável do esforço universal para a proteção de dados pessoais já então encontrava-se na Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 1981. atualizada em 2018, dando lugar à chamada Convenção 108+, ainda não em vigor (COUNCIL OF EUROPE, 2018, pp. 16-17). O tratado europeu dos anos 1980 foi o primeiro instrumento internacional vinculativo para a proteção de dados pessoais. Conforme decidiu o Tribunal de Justiça da União Europeia, no caso *Volker*, de 2010, "o

artigo 8º, nº. 1, da Carta estabelece que '[t]odas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito'. Este direito fundamental está indissociavelmente relacionado com o direito ao respeito da vida privada consagrado no artigo 7º desta mesma Carta." (UNIÃO EUROPEIA, 2010). Tal documento já garantia "a todas as pessoas singulares […] o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal" (ARAS, 2014).

Ao entrar em vigor, a Constituição brasileira já previa o direito à privacidade no art. 5º. Em 2022, a Emenda Constitucional nº 115 ali também introduziu o direito à proteção de dados pessoais (BRASIL, 1988). É de se esperar, portanto, que o MCI também tutele esses bens jurídicos, tal como o faz no seu art. 11, determinando que nas operações de tratamento de dados pessoais sejam "obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros." Aqui já se nota a interação entre tal legislação e a Lei Geral de Proteção de Dados (Lei 13.709/2018), que, inexplicavelmente, exclui de seu âmbito de incidência as investigações criminais e o processo penal (BRASIL, 2018), conforme constatam Estellita (2021, p. 608) e Aras (p. 15-17, 2020).

Sem ingressar no dissenso sobre a aplicação ou não da LGPD, neste estudo cuidamos de uma questão processual penal do MCI, atinente à aquisição ou obtenção de dados pessoais de usuários de provedores de acesso e de aplicações de Internet, no contexto de uma investigação criminal. O tema ganhou maior interesse após a decisão monocrática de 2022 do então ministro Ricardo Lewandowski no HC 222.141/PR (BRASIL, 2022). Aparentemente se afastou da melhor compreensão da matéria quanto ao congelamento de dados de tráfego

de Internet *(quick freeze),* sem necessidade de prévia autorização judicial. Posteriormente, nos agravos regimentais interpostos pelo Ministério Público Federal e pelo Ministério Público do Estado do Paraná, o ministro Lewandoswki mandou excluir dos autos "todo material que não se enquadre no conceito de 'registros de conexão' (art. 5º, VI, da Lei 12.965/2014)". Iniciada a votação no plenário virtual em setembro de 2023, o ministro André Mendonca abriu divergência e o julgamento ainda não se definiu. (BRASIL, 2023).[2] O ministro vogal pontuou em seu voto (BRASIL, 2023, p. 12, § 28) que o MCI não teria regulado "a forma de produção probatória [...], deixando de prever a preservação extrajudicial do conteúdo dos dados digitais armazenados" e negou a ordem de habeas corpus porque "o conteúdo dos dados telemáticos foi disponibilizado apenas após decisão judicial", não havendo nexo de causalidade entre o pedido ministerial de preservação e a prova produzida (BRASIL, 2023, p. 14, § 37-38).

O objeto de análise deste artigo é o Marco Civil da Internet e seu entrelaçamento com a Convenção de Budapeste, exclusivamente no âmbito do processo penal. A questão que nos incomoda está em saber se, de acordo com o MCI, as autoridades de persecução criminal podem solicitar a plataformas digitais a *preservação* (isto é, o congelamento) de dados de tráfego e de conteúdo, sem autorização judicial, e se o cenário normativo se alterou após a entrada em vigor no Brasil da Convenção de Budapeste. O pano de fundo teórico do artigo é a tensão

[2] STF: "Após o voto do Ministro Ricardo Lewandowski (Relator), que negava provimento ao agravo regimental, e dos votos divergentes dos Ministros André Mendonça e Edson Fachin, que davam provimento aos agravos regimentais do Ministério Público Federal e do Ministério Público do Estado do Paraná, a fim de denegar a ordem de habeas corpus, com base no art. 192 do RISTF, pediu vista dos autos o Ministro Gilmar Mendes. Segunda Turma, Sessão Virtual de 8.9.2023 a 15.9.2023". (BRASIL, 2023).

entre liberdades públicas, especialmente o direito à privacidade e à proteção de dados pessoais e o dever do Estado de apurar crimes graves, por meio de medidas de persecução criminal, no ambiente digital.

Assim, por meio de levantamento do conjunto normativo legislativo e convencional e da revisão bibliográfica dos conceitos de preservação, conservação e dados pessoais, descrevemos a controvérsia e discutimos o problema central: há ou não necessidade de prévia autorização judicial para a preservação de dados, para posterior acesso pelas autoridades de persecução criminal e seu uso como prova digital em processos penais? Não pretendemos fazer um estudo de caso do HC 222.141/PR, que aqui é tomado apenas como referência para revelar a atualidade do tema e a escassez de precedentes judiciais na matéria, como se nota dos votos tornados públicos, o do relator, ex-ministro Ricardo Lewandowski, e o do ministro André Mendonca, que abriu divergência. Tal discussão é também atual, tendo em vista a entrada em vigor no Brasil da Convenção de Budapeste em 2023 e da necessidade cada vez maior de acesso a provas digitais em processos penais, numa sociedade dependente de dados e os riscos para os direitos digitais e o devido processo. Pode-se projetar que outros casos semelhantes chegarão às cortes superiores brasileiras.

A técnica dedutiva empregada na pesquisa permitirá compreender o contexto de aplicação das normas em questão, que lidam com a contínua digitalização da persecução criminal, um campo que reclama modernização legislativa e o abandono do pensamento analógico na interpretação dos novos fenômenos eletrônicos, numa mudança de paradigmas que tenha foco específico nos desafios da prova digital. (KERR, 2005, p. 280). Ao final, esperamos responder à questão problema de modo coerente com o conjunto normativo, com o respeito às garantias fundamentais da pessoa humana e as necessidades estatais no cumprimento de suas obrigações processuais

positivas, numa perspectiva equilibrada entre a proibição do excesso e a vedação da proteção deficiente (FISCHER; VALDEZ, 2019, p. 39 e 80).

2 DADOS CADASTRAIS, DADOS DE CONEXÃO E DADOS DE CONTEÚDO COMUNICACIONAL

A partir da premissa de que os dados pessoais (salvo os cadastrais) são indevassáveis, exceto por ordem judicial, o MCI constrói um coeso modelo de proteção a informações pessoais sujeitas a tratamento em sistemas informáticos. Quando da entrada em vigor do MCI, o ponto de partida foi o direito à intimidade previsto no art. 5º, inciso X, da Constituição, garantia prevista também na Convenção Americana sobre Direitos Humanos, de 1969, e no Pacto Internacional de Direitos Civis e Políticos, de 1966 (ARAS, 2014). A partir de 2022, com a promulgação da Emenda Constitucional 115, a norma fundamental foi acrescida do direito à proteção de dados pessoais, agora previsto no inciso LXXIX do art. 5º da Constituição (BRASIL, 1988). A ideia força por trás dessas normas é a inviolabilidade relativa dos dados pessoais, o que inclui dados comunicacionais (*content data*); os dados de conexão – como os números de *Internet Protocol* (IP)[3] – e os dados de

[3] Conforme o art. 5º, III, do MCI, um endereço de protocolo de Internet é o "código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais". Em 2020, o Tribunal de Justiça da União Europeia entendeu que "os endereços IP, apesar de fazerem parte dos dados de tráfego, são gerados sem estarem ligados a uma comunicação específica e servem principalmente para identificar, por intermédio dos prestadores de serviços de comunicações eletrônicas, a pessoa singular proprietária de um equipamento terminal a partir do qual é efetuada uma comunicação através da Internet. Assim, em matéria de correio eletrônico e de telefonia através da Internet, desde que apenas sejam conservados os endereços IP da fonte da comunicação e não os do seu destinatário, esses endereços não revelam, enquanto tais, nenhuma informação sobre

acesso a aplicações de Internet,[4] como, por exemplo, os sites visitados, os aplicativos utilizados, os dados externos relativos ao *download* de arquivos etc (ARAS, 2014).

O exame dos conceitos das diversas categorias de dados no ambiente digital é fundamental para que se possa compreender os diferentes critérios adotados pelo legislador para regular as formas e requisitos de acesso a tais informações pessoais. Há três situações nas quais se permite o *acesso* a dados pessoais digitais, isto é, seu conhecimento ou revelação, no interesse da persecução criminal. A primeira diz respeito aos dados cadastrais, que podem ser requisitados diretamente pelo Ministério Público ou pela Polícia, no curso de uma investigação criminal. A segunda situação refere-se aos demais dados de internautas – dados de tráfego e conexão –, que também podem ser acessados, mas apenas mediante prévia autorização judicial, no curso de uma investigação civil, criminal ou administrativa, ou para a instrução de ação cível, trabalhista ou penal. (ARAS, 2014). Já os dados de conteúdo, dotados de maior proteção, só podem ser acessados por ordem judicial, exclusivamente para fins de persecução criminal, nos termos da Lei 9.296/1996 ou do MCI. (MOURA; BARBOSA, 2020, p. 485-486).

Conforme o §2º do art. 11 do Decreto 8.771/2016, que regulamenta o MCI, são considerados *dados cadastrais*: a filiação; o endereço; e a qualificação pessoal, entendida como nome, prenome,

terceiros que tenham estado em contato com a pessoa que está na origem da comunicação. Por conseguinte, esta categoria de dados tem um grau de sensibilidade menor que o dos outros dados de tráfego." (UNIÃO EUROPEIA, 2020). Este é o caso *La Quadrature du Net*.

[4] Por aplicações de Internet, segundo o art. 5º, VII, do MCI, entende-se o "conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet".

estado civil e profissão do usuário. Quanto a esses dados, diz o §3º do art. 11 do mesmo Decreto que as requisições feitas diretamente pela Polícia ou pelo MP "devem especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos."[5] Por sua vez, o inciso II do art. 10-A da Lei 12.850/2013, que disciplina a infiltração policial digital, conceitua *dados cadastrais* como "informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão".

A definição de *dados de conexão* está no art. 5º, V, do MCI, ali chamados de registros de conexão. Formam o "conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados". Conforme o art. 10-A, §1º, da Lei 12.850/2013, *dados de conexão* são "informações referentes a hora, data, início, término, duração, endereço de Protocolo de Internet (IP) utilizado e terminal de origem da conexão". Esses dados são denominados *dados de tráfego*[6] pelo art. 2º da Diretiva 2002/58/CE, da União Europeia, abrangendo "quaisquer dados tratados

[5] Os usuários de Internet devem ser minimamente identificados, quando se trata de obter dados cadastrais. Exigência semelhante inexiste quando em curso uma investigação com base no art. 22 do MCI, porque, em regra, os ilícitos praticados na Internet ou por meio dela, são cometidos por pessoas de autoria ignorada ou com o uso de pseudônimos. De fato, a criminalidade informática é mais um problema de autoria do que de materialidade.

[6] Em acórdão de 2022, o Tribunal Constitucional português distinguiu duas espécies no gênero metadados: os dados de base – "referem-se à conexão à rede, independentemente de qualquer comunicação" – e os dados de tráfego – como "os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede". (PORTUGAL, 2022).

para efeitos do envio de uma comunicação através de uma rede de comunicações eletrônicas ou para efeitos da faturação". (UNIÃO EUROPEIA, 2002).

Já os *dados de acesso a aplicações de Internet* são definidos pelo inciso VIII do art. 5º do MCI como os "registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP." O art. 2º da Diretiva 2002/56/CE, da União Europeia, designa essas informações *dados de localização*, como aqueles "dados tratados numa rede de comunicações eletrônicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrônicas publicamente disponível".

A Convenção de Budapeste sobre Cibercriminalidade (CETS 185), que está em vigor na Europa desde 1º de julho de 2004, foi aprovada no Brasil pelo Decreto Legislativo 37/2021 e entrou em vigor internacional para nosso País em 1º de março de 2023, findo o processo de adesão. Atualmente, tem 68 Partes (COUNCIL OF EUROPE, 2023), com sua promulgação pelo Decreto 11.491/2023, o texto ganhou vigência interna a partir de 13 de abril de 2023, data da publicação do tratado no Diário Oficial da União (BRASIL, 2023).

O art. 1º, alínea *d*, da Convenção de Budapeste especifica que a expressão *dados de tráfego* compreende "quaisquer dados de computador referentes a uma comunicação por meio de um sistema informatizado, gerados por um computador que seja parte na cadeia de comunicação, e que indiquem sua origem, destino, caminho, hora, extensão, duração ou tipo de serviço subordinado". Tais dados de tráfego integram o gênero *dados de computador*, descritos pelo art. 1º, alínea *b,* como "qualquer representação de fatos, informações ou conceitos numa forma adequada para o processamento" num sistema

informático, um conceito amplo o suficiente para acomodar inclusive *content data.*

Conforme o art. 18.1.b da Convenção de Budapeste, informações cadastrais de assinantes de serviços informáticos correspondem a qualquer informação "mantida em forma eletrônica ou em qualquer outra, que esteja em poder do provedor de serviço e que seja relativa a assinante de seus serviços, com exceção dos dados de tráfego e do conteúdo da comunicação, e por meio do qual se possa determinar o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas para esse fim e a época do serviço". São também dados cadastrais, no conceito convencional, "a identidade do assinante, o domicílio ou o endereço postal, o telefone e outros números de contato e informações sobre pagamento e cobrança, que estejam disponíveis de acordo com o contrato de prestação de serviço". Por fim, integram esse conceito "quaisquer outras informações sobre o local da instalação do equipamento de comunicação disponível com base no contrato de prestação de serviço".

Por fim, devemos considerar os dados informáticos de conteúdo comunicacional, isto é, as informações que são transmitidas entre usuários de Internet, no curso de uma telecomunicação, por meios telefônicos ou telemáticos, pela telefonia fixa, por canais celulares, por e-mails, ou ainda por comunicadores e mensageiros instantâneos, em canais criptografados ou não. Esses *dados de conteúdo* são os mais sensíveis no que se refere à privacidade e estão, por isso mesmo, protegidos pelo inciso XII do art. 5º da Constituição.

3 NÍVEIS DE ACESSO A DADOS PESSOAIS INFORMÁTICOS

Feitas as necessárias delimitações conceituais, vejamos como o MCI, a Convenção de Budapeste e a legislação correlata tratam da obtenção desses dados pessoais por autoridades públicas, no interesse

da persecução criminal, no contexto brasileiro. Pensemos num escalonamento dos requisitos de acesso aos dados cadastrais; aos dados de conexão e de acesso a aplicações de Internet; e aos dados de conteúdo, de acordo com o grau de intrusão estatal e com a natureza dos próprios dados. Nesta linha, Abreu (2021, p. 586) argumenta que existe uma série de leis no Brasil que regulam o acesso a dados pessoais, "cada um deles governado por níveis de sigilo diferentes, sob a presunção de que quão mais sensíveis os dados, maior deve ser a proteção".

Partindo do MCI, seu art. 10 diz que a disponibilização dos registros de conexão (dados de conexão) e de acesso a aplicações de internet (dados de acesso), dos dados pessoais (dados cadastrais) e do conteúdo de comunicações privadas (dados de conteúdo) deve "atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas". Este artigo atua como maestro no tema. Chama a atenção a referência a pessoas *indiretamente* envolvidas, o que amplia o conjunto de indivíduos que podem ser alcançados pela medida de acesso, tal como as vítimas de um crime.

O §1º do art. 10 do MCI estabelece que o provedor responsável pela guarda dos dados somente será obrigado a disponibilizar tais registros "de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma da Seção IV deste Capítulo"[7]. Em qualquer caso, deve ser respeitado o art. 7º do MCI, que estabelece os direitos do usuário da Internet no Brasil. (CASELLI, 2022, p. 54-55).

[7] A Seção IV do MCI diz respeito à Requisição Judicial de Registros e compreende os arts. 22 e 23.

Entre esses direitos estão a inviolabilidade da intimidade e da vida privada; a inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial; a inviolabilidade e sigilo das comunicações privadas armazenadas, salvo por ordem judicial; o não fornecimento a terceiros de dados pessoais, inclusive registros de conexão, e de acesso a aplicações de Internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; e o direito a informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção dos dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta, que não sejam vedadas pela legislação, e estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de Internet.

Vejamos nas subsecções seguintes o escalonamento dos níveis de acesso aos *dados de computador*, na expressão adotada pela Convenção de Budapeste. Tal gradação de requisitos é mencionada pelo §2º do art. 15 da referida Convenção. Conforme o tratado, essas condições "incluirão, quando seja apropriado, tendo em vista a natureza do poder ou do procedimento, entre outros, controle judicial *ou supervisão independente*, fundamentação da aplicação, e limitação do âmbito de aplicação e da duração de tais poderes ou procedimentos." (BRASIL, 2023).

3.1 Obtenção de dados cadastrais

Para os dados cadastrais (*subscriber information*), a proteção é mínima. O Ministério Público e a Polícia podem ter acesso a informações de cadastro de usuários de Internet, sem necessidade de autorização judicial. Há na lei brasileira autorização para esse acesso e uma regra de competência. É o que se vê no art. 17-B da Lei 9.1613/1998 e no art. 15 da Lei 12.850/2013. A essa categoria de dados

também se aplicam o art. 8º, IV e §2º, da Lei Orgânica do Ministério Público da União e o art. 2º, §2º, da Lei 12.830/2013, que regula o inquérito policial.

O MCI segue a mesma orientação. O §3º do art. 10 da Lei 12.965/2014 autoriza o acesso a "dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição." Como vimos, a Polícia e o Ministério Público têm poder de requisição de dados cadastrais, não se exigindo autorização judicial para que obtenham diretamente e conheçam tais informações, desde que no interesse de uma investigação regulamente instaurada.

Na Convenção de Budapeste, esse poder de requisição é objeto do art. 18.1.b, sob o título "ordem de exibição" (*production order*), aplicando-se a informações cadastrais do assinante (*subscriber information*), mas não a dados de tráfego (*traffic data*) – isto é, dados de conexão – nem a dados de conteúdo (*content data*). Discute-se se as normas *processuais* de tratados internacionais têm aplicação imediata ou não no Brasil. No âmbito do STF, há exemplos de pronta aplicação de normas decorrentes de tratados, em institutos como a extradição, a transferência de processos penais e a formalização de audiências de custódia, mesmo antes do Pacote Anticrime, dada a paridade normativa entre tratados e leis ordinárias:

> A eventual precedência dos tratados ou convenções internacionais sobre as regras infraconstitucionais de direito interno somente se justificará quando a situação de antinomia com o ordenamento doméstico impuser, para a solução do conflito, a aplicação alternativa do critério cronológico ("*lex posterior derogat*

> *priori*") ou, quando cabível, do critério da especialidade. (BRASIL, 1997).

Acompanhando a doutrina da hierarquização dos requisitos de acesso a dados, no caso *La Quadrature du Net*, o Tribunal de Justiça da União Europeia (TJUE) entendeu que os Estados Membros podem estabelecer obrigações de conservação de dados relativos à identidade civil de todos os usuários de serviços para prevenção, investigação, prova e repressão de infrações penais, mesmo que não sejam graves, e para a salvaguarda da segurança pública (UNIÃO EUROPEIA, 2020, § 159).

Em suma, no Brasil, dados cadastrais podem ser acessados pelas autoridades de persecução criminal, independentemente de autorização judicial.

3.2 Obtenção de dados de conexão à Internet e dados de acesso a aplicações

O tratamento legal para os dados de conexão à Internet e para os dados de acesso é mais rigoroso. Aqui já não será possível a obtenção direta pela Polícia ou pelo Ministério Público, sendo imprescindível uma ordem judicial. Subimos um degrau na escala de interferências do Estado sobre a vida privada. É que tal categoria de dados revela mais sobre os usuários de Internet do que as informações meramente cadastrais podem fazê-lo. Justifica-se, assim, pela mais intensa ingerência na privacidade, uma salvaguarda maior a esses conjuntos de dados.

Por isso, o §1º do art. 7º do MCI determina que o provedor responsável pela guarda desses dados "somente será obrigado a disponibilizar os registros de conexão e de acesso", seja isoladamente (de forma autônoma, diz a lei) ou conjuntamente com dados

cadastrais,[8] se houver prévia ordem judicial, na forma da Seção IV do Capítulo III (que cuida da requisição judicial de registros), e, ainda assim, respeitado o art. 7º do MCI, sobretudo os seus incisos II e III, que se referem expressamente à necessidade de ordem judicial para acesso.

Na Convenção de Budapeste, esta medida é objeto do art. 17.1.b – como ordem de revelação ainda que parcial de dados de tráfego (*traffic data*) que tenham sido preservados – e do art. 18.1.a – como uma ordem a alguém para exibição (*production order*) referente a dados armazenados.

O art. 19 do mesmo Tratado nº 185 regula medida de natureza e alcance diverso, a busca e apreensão de computadores, dispositivos de armazenamento e sistemas informáticos e dos dados neles armazenados. Esse mecanismo em regra se implementa sem prévio aviso ao detentor dos dados, e o acesso aos *dados de computador* (quaisquer deles) pode ocorrer de maneira remota ou mediante apreensão física dos dispositivos de armazenamento.

O acesso a dados de tráfego em tempo real é regulado pelo art. 20.1 da Convenção de Budapeste. Neste ponto, o dispositivo mais parecido existente na legislação brasileira é o art. 13-B do CPP, aplicável à investigação do tráfico de pessoas. No que diz respeito ao MCI, a norma reitora é o seu art. 22, que se refere ao fornecimento de registros de conexão ou de acesso a aplicações de Internet.

3.3 Obtenção de dados de conteúdo comunicacional

O acesso ao conteúdo das comunicações das pessoas que usam a Internet (*content data*) é regido tanto pelo MCI quanto pela Lei

[8] Refere-se aos dados "associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal".

9.296/1996. Em ambos os casos, exige-se prévia autorização judicial. São duas as situações.

O conteúdo de comunicações privadas armazenadas somente pode ser disponibilizado mediante ordem judicial, respeitados o inciso III do art. 7º e o §2º do art. 10 do MCI. No plano constitucional, as normas de regência são os incisos X e LXXIX do art. 5º. Tais dispositivos dialogam com o art. 18.1.a e com o art. 19 da Convenção de Budapeste, que, no entanto, se limitam a fins de investigação criminal.

Já para as comunicações privadas em tempo real, isto é, para acesso ao fluxo de comunicações não-públicas, o art. 7º, II, do MCI, igualmente exige prévia autorização judicial e se refere à Lei 9.296/1996, que regula as interceptações telefônicas (telefonia fixa e celular) e as interceptações telemáticas (por meios informáticos).[9] O §2º do art. 10 do MCI não discrepa desse tratamento, pois estabelece que "o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer".

A interceptação de conteúdo telemático é objeto do art. 21 da Convenção de Budapeste que, como vimos, tem disciplina no art. 7º, II, do MCI, e na Lei 9.296/1996.

Compreendidas as distinções entres as três categorias de dados e os requisitos escalonados de acesso a eles, vamos agora ao ponto principal da controvérsia: é possível o congelamento cautelar de dados de conteúdo, de dados de conexão e de dados de acesso a aplicações de Internet, no procedimento de *quick freeze,* sem autorização de um juiz*?*

[9] Essa distinção jurídica perde interesse, do ponto de vista tecnológico, diante da convergência digital, como se percebe no extenso uso de chamadas por voz em mensageiros instantâneos no sistema *voice over IP.*

4 PRESERVAÇÃO DE DADOS INFORMÁTICOS *VERSUS* OBTENÇÃO DESSES DADOS

É fundamental fazer a distinção entre a *retenção, conservação* ou *guarda de dados* (como atividades operacionais dos provedores e como atividades de tratamento)[10]; a *preservação de dados* (como atividade de fim probatório de natureza pré-cautelar ou como cautelar para fins de prova);[11] e o *acesso a dados* (a revelação ou a busca ou a interceptação dos dados para uso como prova em juízo).

Uma coisa é *preservar* ou congelar certo conjunto de dados para futura obtenção e uso num processo penal, sem acesso imediato a eles; outra coisa será acessar determinada coleção de dados, o que pode

---

[10] Refere-se à expressão *data retention*, que implica um prazo de guarda de dados para seu tratamento de acordo com a finalidade da recolha. Remete-se, portanto, à ideia de *storage limitation*, limitação do tempo de armazenamento dos dados. No considerando 39 do Regulamento 2016/679 da União Europeia (GDPR), explica-se que "é necessário assegurar que o *prazo de conservação dos dados* seja limitado ao mínimo (...). A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica". O princípio da limitação da conservação dos dados está previsto no art. 5.1.e do GDPR. (UNIÃO EUROPEIA, 2016).

[11] A expressão correspondente em inglês é *data preservation.* No considerando 65 do GDPR se lê que "o prolongamento da conservação dos dados pessoais deverá ser efetuado de forma lícita quando tal se revele necessário para o exercício do direito de liberdade de expressão e informação, para o cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, por razões de interesse público no domínio da saúde pública, para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial." Note-se a última finalidade: processo judicial. (UNIÃO EUROPEIA, 2016).

ocorrer com ou sem sua prévia preservação. O congelamento (*preservation*) dos dados somente será necessário se já estiver próximo o fim do prazo legal máximo de guarda desses dados (*data retention*). (COUNCIL OF EUROPE, 2001, p. 25). O êxito de investigações criminais que dependem de provas digitais depende de sua preservação, dadas as características que lhe são inerentes: sua intangibilidade, a facilidade de sua destruição e sua rápida e fácil transferibilidade ou mobilidade. (DAS; SARKAR, 2022, p. 63).

4.1 A natureza jurídica do congelamento de dados informáticos

O acesso ao *conteúdo* de comunicações telefônicas e telemáticas, em tempo real, é regulado pela Lei 9.296/1996, que implementa as regras de competência e de finalidade legítima exigidas pelo inciso XII do art. 5º da Constituição. (BRASIL, 1996). A porta de acesso é chamada de interceptação de telecomunicações e ingressa na categoria das técnicas especiais de investigação (TEI) ou meios de obtenção de prova, como prefere o art. 3º da Lei 12.850/2013.

Por outro lado, o regime jurídico do acesso a dados e comunicações privadas armazenadas tem o seu fundamento no art. 5º, incisos X e LXXIX, da Constituição. Embora no texto constitucional a necessidade de autorização judicial não esteja expressa, essa construção mais protetiva resultou do adensamento das cláusulas de respeito à vida privada e, mais recentemente, do robustecimento do direito à proteção de dados pessoais e do direito à autodeterminação informativa. Este direito corresponde, segundo Sarlet (2021, p. 26), ao "direito de cada indivíduo poder controlar e determinar (ainda não de modo absoluto) o acesso e uso de seus dados pessoais".

Essa evolução pode ser creditada à expansão das novas formas de comunicação, interação e armazenamento de dados, características da sociedade digital, na era das novas tecnologias da comunicação, da

informação e do conhecimento. Por isso, os arts. 7º, 10, 13, 15 e 22 do MCI exigem prévia autorização judicial para o acesso a dados ali identificados. É essa também a posição da jurisprudência quanto à apreensão de dispositivos de memória, especialmente *smartphones*. Mesmo em situações de flagrante, exige-se autorização judicial para o acesso ao seu conteúdo, como se fosse, mal comparando, uma busca e apreensão domiciliar. Sobre o assunto, no AgRg no HC 709.810/SP, decidiu o STJ:

> A jurisprudência das duas Turmas da Terceira Seção deste Tribunal Superior firmou-se no sentido de ser ilícita a prova obtida diretamente dos dados constantes de aparelho celular, decorrentes de mensagens de textos SMS, conversas por meio de programa ou aplicativos ('WhatsApp'), mensagens enviadas ou recebidas por meio de correio eletrônico, obtidos diretamente pela polícia no momento do flagrante, sem prévia autorização judicial para análise dos dados armazenados no telefone móvel. (BRASIL, 2023).

A preservação de dados de tráfego ou dos dados de conteúdo tem feição cautelar; visa a evitar o perecimento da prova. Embora as medidas cautelares, em regra, estejam marcadas por cláusula de reserva de jurisdição – tal como se dá com as providências cautelares pessoais e as acautelatórias patrimoniais – há exceções no ordenamento jurídico. Na tradição brasileira, entre essas exclusões estão a prisão e a autuação em flagrante delito (arts. 301 e 304 do CPP) por qualquer do povo; o arbitramento de fiança pelo delegado de Polícia (art. 322 do CPP); e as medidas preventivas de urgência de afastamento do agressor do lar da Lei Maria da Penha (art. 12-C, incisos II e III, da Lei 11.340/2006) e da Lei Henry Borel (art. 14, incisos II e III, da Lei 14.344/2022), que podem ser adotadas por qualquer policial. Nota comum a todas essas medidas é a possibilidade de serem revistas pelo juiz competente, o que revela sua pré-cautelaridade.

O art. 6º do Código de Processo Penal (CPP), que descreve as principais atividades do delegado de Polícia no início da investigação criminal, também abrange providências cautelares, sobretudo os deveres que tem a autoridade policial de *preservar* a cena do crime e de apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais. Cabe ao delegado, "logo que tiver conhecimento da prática da infração penal [...] dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais". (BRASIL, 1941). Trata-se, evidentemente, de cautelar administrativa voltada à produção da prova de determinada infração penal.

É esta também a natureza do meio especial de prova descrito nos arts. 13 e 15 do Marco Civil da Internet (KIST, 2019, p. 262),[12] para a preservação de informações eletrônicas relacionadas a um usuário de Internet. Esses dois dispositivos regulam TEIs que terão impacto na determinação da autoria e da materialidade de um crime grave[13]. A

[12] Referido autor situa a "conservação expedita de dados" entre os meios de obtenção de prova do MCI.

[13] Na formulação que adotamos, as técnicas especiais de investigação (TEI) só podem ser usadas para a apuração de crimes graves, pelo critério de limiar de pena, e de infrações penais conexas. Por crime grave, entende-se toda infração cuja pena é igual ou superior a 4 anos de prisão, nos termos do art. 2.b da Convenção das Nações Unidas contra o Crime Organizado Transnacional, promulgada no Brasil pelo Decreto 5.015/2004. Critério semelhante a este é adotado, por exemplo, para a interceptação ambiental do art. 8º-A, II, da Lei 9.296/1996, que, todavia, emprega o patamar de pena superior a 4 anos. Também são considerados crimes graves todos os crimes convencionais, isto é, aqueles que o Brasil se obrigou a tipificar em tratados internacionais. A gravidade do crime sujeito a uma TEI é um critério de proporcionalidade para a ingerência estatal. Note-se, porém, que o art. 22 do MCI permite a quebra do sigilo de dados de conexão e de dados de acesso a aplicações de Internet para prova em processos cíveis (inclusive os trabalhistas), o que põe em xeque o princípio da proporcionalidade.

preservação dos dados de conexão e dos dados de acesso a aplicações de Internet (no conjunto, *traffic data*) opera como providência cautelar que viabilizará a posterior quebra de sigilo desses mesmos dados, para a produção de prova digital útil à persecução criminal, já então com autorização judicial.

Assim, tal como ocorre com as providências do inciso I do art. 6º do CPP, a preservação dos dados a pedido da Polícia ou do MP tem função acautelatória, *ad perpetuam rei memoriam*, uma vez que dados de tráfego de Internet e de acesso a aplicações são usualmente apagados ou anonimizados quando cumprem suas finalidades técnico-operacionais, no provedor, ou quando findo o prazo de guarda.[14] Para os dados de conexão, o prazo legal de guarda é de um ano (art. 13 do MCI); para os registros de acesso a aplicações de Internet, o prazo é de 6 meses (art. 15 do MCI). Mas é de 5 anos o prazo de guarda dos registros de identificação dos números de origem e de destino de ligações telefônicas internacionais, interurbanas e locais, por telefonia móvel ou fixa (art. 17 da Lei 12.850/2013). É diante da iminência do termo final de guarda (*data retention*) que se coloca o problema da preservação expedita desses dados, para extensão momentânea e por tempo certo do período de custódia.

A medida de quebra de sigilo virá apenas depois e sempre dependerá de autorização judicial, sendo indispensável para as diversas categorias de dados, com exceção dos dados cadastrais. Assim, há reserva de jurisdição nos termos do art. 7º, incisos II (obtenção do fluxo

[14] Para os dados de conexão, o prazo legal de guarda é de um ano (art. 13 do MCI); para os registros de acesso a aplicações de Internet, o prazo é de 6 meses (art. 15 do MCI). (BRASIL, 2014). Mas é de 5 anos o prazo de guarda dos registros de identificação dos números de origem e de destino de ligações telefônicas internacionais, interurbanas e locais, por telefonia móvel ou fixa (art. 17 da Lei 12.850/2013). (BRASIL, 2013).

de comunicações em tempo real) e III (obtenção de dados de conteúdo armazenados); do art. 10 (obtenção de registros de conexão e de registros de acesso a aplicações de Internet); do §2º do art. 10 (obtenção de conteúdo de comunicações); do §5º do art. 13 (obtenção de registros de conexão); do §3º do art. 15 (obtenção de registros de acesso a aplicações de Internet); e do art. 22 do MCI (obtenção de registros de conexão e de registros de acesso a aplicações de Internet).

Caselli (2022, p. 75) pontua corretamente que a palavra "congelamento" dos dados não deve ser interpretada como sendo uma indisponibilidade, pois o instituto em questão é um "procedimento cautelar preparatório" que tem por fim apenas "resguardar futuro acesso" pela autoridade investigativa, não impedindo que o titular dos dados aceda a eles; estes "continuarão disponíveis". Por isso mesmo, a 5ª Turma do Superior Tribunal de Justiça (STJ), no Habeas Corpus 626.983/PR – que deu origem ao HC 222.141 no STF – afirmou acertadamente que "o pedido de congelamento do Ministério Público [...] não precisa necessariamente de prévia decisão judicial para ser atendido pelo provedor, mesmo porque [...] não equivale a que o requerente tenha acesso aos dados congelados sem ordem judicial". (BRASIL, 2021). Não, há, portanto, ofensa ao direito à autodeterminação informacional, garantia autônoma reconhecida pelo STF em 2020 na ADI 6390 MC-Ref/DF, como uma "parcela fundamental do seu direito de desenvolver livremente sua personalidade", o que compreende o direito de tomar diversas decisões sobre seus dados pessoais (BRASIL, 2020, p. 61 e 101). Este direito se refere, portanto, à faculdade do titular dos dados de controlar suas informações a seu respeito, como das maneiras de legitimar o tratamento desses dados (BIONI, 2016, p. 150).

Em suma, a preservação de quaisquer dados de computador tem feição cautelar – ou mais precisamente, *pré-cautelar*, pois dependerá

de posterior ordem judicial. Sua concretização pode ocorrer mediante congelamento solicitado pelo MP ou pela Polícia, sem autorização judicial, no tocante aos dados de conexão e aos dados de acesso a aplicações de Internet, nos termos do MCI. Já a preservação de dados de conteúdo (e de qualquer dado de computador armazenado) – *data preservation* – tem disciplina no art. 16 da Convenção de Budapeste (COUNCIL OF EUROPE, 2001, p. 25).

4.2 O procedimento de preservação e acesso a dados informáticos

Tendo em conta o princípio da proporcionalidade, mencionado no art. 15 da Convenção de Budapeste, há diferentes níveis de proteção nas etapas de interferência sobre o direito à privacidade, partindo-se do menos para o mais. No caso dos dados cadastrais, a obtenção é direta, sem necessidade de autorização judicial. Para os dados de conteúdo, de acesso e de conexão, é preciso ordem judicial. Devido a contingências da investigação – como, por exemplo, a proximidade do esgotamento do prazo legal de guarda/conservação dos dados – pode ser necessário garantir sua integridade, para que não sejam descartados, alterados ou apagados pelo provedor ou pelo usuário. Aqui é preciso compatibilizar a necessidade de proteção do direito à privacidade com as legítimas necessidades do processo penal e da segurança pública, o que exige uma política criminal equilibrada, que não gere leis excessivamente limitadoras ou outras que sejam insuficientemente protetivas. (POLLACK, 2019, p. 80).

Havendo necessidade de acautelar informações digitais, a Polícia e o Ministério Público notificarão o agente de tratamento dos dados sobre a necessidade de sua preservação (*data preservation*), isto é, da necessidade de prolongamento do prazo de conservação (*data retention*). Segundo o MCI, tais autoridades poderão requisitar (o texto legal utiliza o verbo "requerer") aos provedores a preservação pré-

cautelar dos registros (*logs*) de conexão e acesso. A partir daí, ainda conforme o MCI, esses órgãos de persecução terão sessenta dias para requerer em juízo a validação do congelamento e a revelação dos dados de conexão e de acesso a aplicações. Esgotado esse prazo sem que advenha alvará judicial autorizativo, o guardião dos registros – isto é, o agente de tratamento de dados – estará exonerado do dever de prorrogação da guarda (*data preservation*). Quito (2020, p. 174) tem a mesma compreensão, sustentando que, conforme o art. 10 do MCI, as empresas que prestam serviços de conexão e de acesso têm o dever de "manter esses registros pelo prazo de um ano e de seis meses, respectivamente, ou por tempo superior, a pedido das autoridades policiais ou membros do Ministério Público, quando maior período for necessário à obtenção de ordem judicial para as correspondentes quebras de sigilo".

Conforme o art. 13 do MCI, os *registros de conexão* à Internet só precisam ser mantidos por um ano. No interesse de uma investigação criminal, a autoridade policial ou administrativa ou o Ministério Publico "poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput." Obviamente, essas autoridades devem requerer a preservação ao provedor que detenha os registros de conexão e de acesso, isto é, ao responsável pelo tratamento dos dados, nos termos da Lei Geral de Proteção de Dados (LGPD).

É somente no §3º do art. 13 do MCI que aparece a necessidade de autorização judicial, não para a preservação dos dados (extensão do prazo de guarda), mas para o acesso da Promotoria e da Polícia a tais dados. O §3º é amarrado ao §2º do mesmo artigo, para evidenciar a sucessão procedimental: primeiro uma coisa (pedido cautelar ao provedor para preservar os dados); depois a outra (petição ao juiz competente em sessenta dias, para acesso aos dados antes preservados).

De fato, somente "na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput".

Evidentemente, a autorização judicial é exigida para o acesso aos dados, não para sua preservação pré-cautelar. Se esses dados não forem preservados de imediato, não haverá razão para requerimento judicial algum, pois a essa altura os dados já terão sido apagados ou anonimizados, como são regularmente deletados ou despersonalizados ao final do prazo de um ano (*data retention*) a que se refere o caput do art. 13 do MCI.

Para que medidas de investigação para obtenção de provas digitais de crimes comuns ou de cibercrimes funcionem, obviamente, os dados do usuário que eventualmente seja suspeito de um crime devem estar disponíveis, tendo em conta o prazo máximo de retenção pelos provedores de acesso e de aplicações de Internet, consideradas as regras de tratamento de dados pessoais a que estão sujeitos. Para este tipo de dados, o prazo de guarda ou conservação é de seis meses, o que impacta os direitos à vida privada e à autodeterminação informativa (PORTUGAL, 2022). O Tribunal Constitucional português reconhece o direito à autodeterminação comunicativa como um direito de liberdade:

> [...] de liberdade para comunicar, sem receio ou constrangimentos de que a comunicação ou as circunstâncias em que a mesma é realizada possam ser investigadas ou divulgadas. Sem essa confiança, o indivíduo sentir-se-á coartado na liberdade de poder comunicar com quem quiser, quando quiser, pelo tempo que quiser e quantas vezes quiser. Trata-se, pois, de permitir um livre desenvolvimento das relações interpessoais e, ao mesmo tempo, de proteger a confiança que os indivíduos depositam nas suas comunicações

> privadas e no prestador de serviços. (PORTUGAL, 2022, § 11).

Se o procedimento escalonado para preservação cautelar dos dados de conexão e sua posterior obtenção está regulado no art. 13, *caput*, e §§2º e 3º, do MCI,[15] o roteiro para as mesmas providências, sobre os *dados de acesso a aplicações de Internet*, estará no art. 15 do MCI.[16] Pode ser necessário, primeiramente, preservar os registros de acesso a aplicações de Internet, evitando seu apagamento. Policiais e membros do Ministério Publico podem requerer, administrativamente, ao provedor de aplicações a extensão do prazo de guarda, ou seja, o aumento do prazo de *data retention,* para fins cautelares. O §2º do art. 15 da Lei é expresso ao dizer que esse requerimento cautelar é endereçado ao provedor, isto é, a qualquer empresa de aplicações de Internet. O segundo passo será o acesso aos dados, só possível mediante ordem judicial, aplicando-se, neste caso, o §§ 3º e 4º do art. 13 do MCI, por determinação do seu art. 15.

A aplicabilidade do §4º do art. 13 aos dois procedimentos de acesso a dados – art. 13 para os *dados de conexão*; art. 15 para os *dados de acesso a aplicações* – indica que, em ambos, a preservação cautelar dos dados em questão é uma medida administrativa, extrajudicial, prévia à judicialização de pedido de quebra de sigilo de dados. Se o §2º do art. 13 do MCI estabelece um prazo decadencial de sessenta dias para a petição em juízo, o §4º do mesmo artigo determina que a preservação cautelar a pedido da Polícia ou do MP "perderá sua eficácia caso o pedido de autorização judicial" (faço ênfase aqui) seja

[15] O art. 13 trata da guarda de registros de conexão. Para essa categoria de dados, o prazo ordinário de guarda é de doze meses.

[16] O art. 15 trata da guarda de registro de acesso a aplicações de Internet. Para essa categoria de dados, o prazo ordinário de guarda é de seis meses.

indeferido pelo juiz ou não seja protocolado nos sessenta dias contados do requerimento administrativo ao provedor.

Conclui-se, então, que, para evitar que os dados de interesse de uma investigação criminal sejam alterados ou eliminados quando houverem cumprido sua finalidade (quanto ao motivo e à utilidade da recolha pelo provedor), diante da política de tratamento de dados adotada pela empresa de Internet, eventualmente pode ser necessário preservá-los cautelarmente, sob pena de não poderem ser conhecidos pelos investigadores nem utilizados em juízo, pois já não existirão.

Do procedimento de preservação dos dados (*data preservation*) também cuida o art. 16.1 da Convenção de Budapeste. Os Estados Partes do tratado devem adotar medidas legislativas[17] para "permitir que a autoridade competente[18] ordene ou obtenha a expedita preservação de dados de computador[19] especificados", entre os quais se inserem os dados de conteúdo e os dados de tráfego armazenados,[20]

---

[17] Trata-se de um mandado expresso de adaptação da legislação processual dos Estados Partes, que deve ser cumprido o quanto antes, uma vez que o tratado está em vigor interno desde 13 de abril de 2023.

[18] Ao usar a expressão "autoridade competente", a Convenção não exige decisão de autoridade judiciária, deixando a cada Estado Parte definir em seu ordenamento quem será ela. Vide o art. 15.2 do Tratado, que cuida da necessidade de "controle judicial" ou apenas de "supervisão independente" sobre procedimentos probatórios intrusivos, o que significa que tanto pode haver intervenção de juiz quanto de outra autoridade independente, numa formulação compatível com o ordenamento jurídico brasileiro.

[19] Os "dados de computador" são definidos do art. 1.b da Convenção como "qualquer representação de fatos, informações ou conceitos numa forma adequada para o processamento num sistema de computador que inclua um programa capaz de fazer o sistema realizar uma tarefa". Vide o art. 3º da Convenção, que emprega a mesma expressão quando cuida do crime de interceptação ilícita.

[20] Conforme o art. 1.d da Convenção de Budapeste, "dados de tráfego" são "quaisquer dados de computador referentes a uma comunicação por meio de um sistema

"quando haja razões para admitir que os dados de computador estão particularmente sujeitos a perda ou modificação". A parte final do art. 16.1 da Convenção 185 deixa claro que a preservação ocorrerá de maneira cautelar quando houver risco de perda, apagamento, destruição ou modificação de dados já armazenados, sem que haja necessariamente a indisponibilidade dos dados para seu usuário ou titular (COUNCIL OF EUROPE, 2001, p. 25-26), pois faz-se cópia de segurança. Fica evidenciado na *Explanatory Note* que o congelamento dos dados não obriga a torná-los inacessíveis. (COUNCIL OF EUROPE, 2001, p. 26, § 159).

O §2º art. 16 da Convenção de Budapeste estabelece que o prazo máximo de preservação dos dados informáticos em geral será previsto em lei, não podendo ser superior a noventa dias, prorrogáveis. Como vimos, o MCI instituiu, para os dados de conexão, prazo não superior a sessenta dias. O provedor deve cumprir o requerimento administrativo, "a fim de permitir à autoridade competente buscar sua revelação". (BRASIL, 2014). Ou seja, o prazo de extensão será o necessário para que as autoridades obtenham judicialmente o acesso aos dados preservados, inclusive aos dados de conteúdo.

Já o §3º do art. 16 do tratado proíbe o *tipping off,* exigindo do provedor que recebeu a notificação da autoridade investigadora "manter em sigilo o início do procedimento investigativo por um período de tempo estabelecido na sua legislação interna". A obrigação de confidencialidade é instituída em prol da investigação e da privacidade do investigado (COUNCIL OF EUROPE, 2001, p. 27). O Brasil já cumpre esse mandado convencional ao dispor, no §4º do art.

---

informatizado, gerados por um computador que seja parte na cadeia de comunicação e que indicam sua origem, destino, caminho, hora, data, extensão, duração ou tipo de serviço subordinado".

13 do MCI, que "o provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento" da autoridade.

Uma vez congelados os dados, no provedor, por solicitação da autoridade investigante em medida pré-cautelar – pensemos na prisão em flagrante como modelo e sua posterior confirmação e conversão ou não em audiência de custódia –, uma ordem judicial deve determinar sua posterior revelação à autoridade investigadora, nos termos do art. 16.2 ou do art. 17.1.b ou do art. 18.1.a da Convenção de Budapeste.[21] É exatamente o mesmo procedimento que vimos no §3º do art. 13 do MCI, com a diferença de que a Convenção 185 estipula um só rito para a preservação cautelar de todos os tipos de dados (*computer data*), não os distinguindo, como faz o MCI.

A legislação portuguesa também prevê medida semelhante, sob o titulo de "preservação expedita de dados". O §1º do art. 12 da Lei do Cibercrime, de 2009, estatui que, se, no curso da persecução, houver a necessidade de obter dados computacionais específicos que possam ser alterados, destruídos ou indisponibilizados, "a autoridade judiciária competente[22] ordena a quem tenha disponibilidade ou controlo desses dados" que os preserve.

Conforme o §2º do art. 12 da lei portuguesa, a preservação também pode ser determinada "pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata (...) à autoridade judiciária". O destinatário da medida deve preservar "de imediato os dados em causa, protegendo e

[21] O art. 18.1.b da Convenção de Budapeste regula o que se denomina no Brasil de requisição de dados cadastrais, isto é, a exibição de informações sobre o assinante de serviços de Internet.

[22] No direito português, a expressão "autoridade judiciária" engloba juízes e membros do Ministério Público, todos lá denominados de "magistrados". (PORTUGAL, s/d).

conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual." (PORTUGAL, 2009).

4.3 A preservação de dados de conteúdo por meio da Convenção de Budapeste

O MCI não regula a medida cautelar de preservação de conteúdo de dados (*content data*). Seus arts. 13 e 15 limitam-se a determinar a possibilidade de congelamento expedito de dados de tráfego e de dados de acesso a aplicações de Internet. Contudo, a Convenção de Budapeste abrange tanto uma quanto a outra forma de *quick freeze.*

De fato, ao se referir, no seu art. 16, à preservação expedita de *dados de computador,* a Convenção 185 abarca todas as categorias de dados armazenados (*stored data*), inclusive os dados de conteúdo e os dados de tráfego. Deste modo, os Estados Partes ficam obrigados – e o Brasil, entre eles, desde a vigência do tratado – a adotar providências legislativas para dar lugar a medidas cautelares e de obtenção de provas digitais. O relatório explicativo da Convenção 185 esclarece que os procedimentos probatórios "referem-se a todos os tipos de dados, incluindo três tipos específicos de dados de computador (dados de tráfego, dados de conteúdo e dados de assinantes), que podem existir em duas formas (armazenados ou em processo de comunicação)" (COUNCIL OF EUROPE, 2001, p. 21).

Com exceção das normas de direito penal – que dependem de lei em função do princípio da legalidade penal estrita –, as normas conceituais e as de natureza processual da Convenção de Budapeste têm aplicação instantânea, nos termos do art. 1º, inciso I do CPP – que prevê o principio da especialidade –, e do art. 2º do CPP, que institui o princípio do efeito imediato. (BRASIL, 1941).

Desta maneira, desde 13 de abril de 2023,[23] diante da mora legislativa, a Polícia Judiciária e o Ministério Público podem invocar os arts. 16 e 17 da Convenção de Budapeste para as medidas de preservação expedita de dados de computador (inclusive *traffic data* e *content data*), pelo prazo máximo de sessenta dias, independentemente de ordem judicial. Conforme o relatório explicativo da Convenção nº 185, em comentário ao art. 16, o acesso aos dados, a depender do sistema jurídico, pode decorrer de autorização judicial ou administrativa ou de requisição da Polícia ou do MP (COUNCIL OF EUROPE, 2001, p. 26, § 160).

Os arts. 13 e 15 do MCI servirão como parâmetros de aplicação *analógica* (art. 3º do CPP), regendo o procedimento escalonado de duas etapas (primeiro o congelamento e depois o acesso) e estipulando o prazo máximo de preservação (sessenta dias),[24] também para quando o pedido de congelamento (*quick freeze*) disser respeito a dados de conteúdo (COUNCIL OF EUROPE, 2001, p. 27). Esses dados deverão ser devidamente especificados na notificação e somente poderão ser revelados por ordem judicial. Numa justiça criminal cada vez mais orientada por dados e dependente deles (*data driven criminal justice*), que a tornou "datocêntrica" (LOGAN; FERGUSON, 2016, p. 549), é essencial a existência de mecanismos para a prova preservação de provas digitais.

5 CONCLUSÃO

[23] Vale anotar a posição de Mazzuoli (2020, p. 304), para quem os tratados entram em vigor no Brasil no momento da publicação do decreto legislativo, não havendo na Constituição exigência de publicação de decreto de promulgação pelo Executivo.

[24] A futura lei de implementação (*enabling legislation*) da Convenção de Budapeste poderá estabelecer prazo de até 90 dias para preservação cautelar de todas as espécies de dados. Vide o art. 16.2 do Tratado.

Vimos que a legislação brasileira distingue *dados cadastrais; dados de conexão* e *dados de acesso a aplicações* de Internet; e *dados de conteúdo*, sujeitando-os a diferentes requisitos de acesso por autoridades de persecução criminal.

Os *dados de conteúdo* são uma categoria à parte, que merece proteção especial, tanto do MCI quanto da Lei 9.296/1996. Por isso, o § 2º do art. 10 do MCI estabelece que "o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial", observando-se os incisos II e III do art. 7º, que, como visto, asseguram o sigilo do fluxo das comunicações dos usuários pela internet, salvo por ordem judicial, na forma da lei; e o sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.

Essa distinção entre diferentes classes de *dados de computador* pode ser facilmente percebida pelo exame dos arts. 16 a 20 da Convenção de Budapeste. Este tratado entrou em vigor no Brasil em 13 de abril de 2023. Desde então, suas regras conceituais e as de natureza processual, inclusive as de preservação expedita de dados (*quick freeze*), incidem por especialidade (art. 1º, I, do CPP), têm aplicação imediata (art. 2º, CPP) e servem de parâmetro para analogia (art. 3º, CPP) no tocante ao mecanismo de congelamento de *content data*.

Qualquer forma de intervenção estatal sobre a privacidade deve estar prevista em lei, com indicação de regras claras de competência e de autorização. Os requisitos de previsão em lei, justificativa no interesse público e de necessidade numa sociedade democrática são os parâmetros adotados pelo TEDH (1984) para aferir a convencionalidade desse tipo de interferência do Estado na vida

privada.[25] Tratados internacionais são recebidos na ordem jurídica interna, ao mesmo no nível de leis federais ordinárias, o que faculta a interseção entre o MCI e a Convenção de Budapeste. Apesar disto, tal tratado deve merecer do Congresso Nacional uma lei para sua completa implementação (*enabling legislation*), resolvendo-se o déficit legislativo.

No particular, o MCI é suficiente para lidar com a questão da preservação dos dados menos sensíveis. De qualquer modo, no congelamento de registros de conexão (art. 13 do MCI) e de registros de acesso a aplicações de Internet (art. 15), ou de dados de conteúdo (art. 16 da Convenção de Budapeste) o titular dos dados não perde o controle sobre eles. Não há analogia entre *dados* e *coisas* corpóreas, como se o mero congelamento interferisse no direito de propriedade tal como se dá quando da apreensão física de um bem. O titular dos dados continua a ter a oportunidade de exercer os seus direitos de informação, acesso, oposição, retificação e apagamento, quando for o caso, ainda que de forma diferida, nos termos da Súmula Vinculante 14 do STF. No período de preservação (*quick freeze*), o titular poderá acessá-los (pois não ficam bloqueados para este fim), solicitar retificações, pedir seu apagamento ou exercer o direito de portabilidade. A preservação cautelar ou pré-cautelar desses mesmos dados não impede o exercício desses direitos pelo seu titular. O direito à autodeterminação informacional está salvaguardado.

Certos dados, porém, sequer estarão sujeitos a direitos de retificação, por serem automatizados, como é o caso de coordenadas geográficas obtidas por sistemas GPS, números IP, endereços MAC e

[25]Ali houve discussão sobre a aplicabilidade do art. 8º da Convenção Europeia de Direitos Humanos ao procedimento de bilhetagem (*metering)*, usado pela Polícia britânica para acesso a dados de chamadas originadas e recebidas e ao seu tempo de duração.

códigos IMEI dos dispositivos eletrônicos, aparelhos móveis de telefonia e da Internet das Coisas (IoT). Se o titular dos dados pode pedir a correção de dados cadastrais em um provedor, não pode pedir que a companhia altere o registro de seu número IP em uma determinada conexão já ocorrida.

Conclui-se então que os procedimentos dos arts. 13 e 15 do MCI e dos arts. 16 e 17 da Convenção de Budapeste para *quick freeze* de dados específicos (*content and non-content data*) não ferem o direito à privacidade nos quesitos divulgação ou revelação, pois a solicitação administrativa do Ministério Público ou da Polícia não exporá os dados de tráfego, conexão, localização ou conteúdo. O acesso a eles não é feito diretamente por essas autoridades – como ocorre com os dados cadastrais – mas sempre com intermediação de um juiz, servindo o congelamento para lidar com a volatilidade desses dados.

Conclui-se também que não há ofensa às normas de proteção de dados pessoais. Lamentavelmente, a LGPD estabelece expressamente que ela não se aplica a questões de natureza criminal (art. 4º, III, da Lei 13.709/2018). Logo, no tocante às categorias de dados de que tratamos, a aplicação do princípio previsto no art. 3º, incisos II e III, do MCI[26] é intermediada pelos arts. 10, 13 e 15 do próprio MCI e, eventualmente, pelas Leis 9.296/1996 e 12.850/2013.

Como se vê no seu art. 22, o MCI não regula separadamente ou exclusivamente o acesso a dados para investigações criminais. Diversamente, o art. 3º, IV, da Lei 12.850/2013 estabelece que "em qualquer fase da persecução penal", serão permitidos como meios de obtenção de prova o acesso a registros de ligações telefônicas e

[26] MCI: "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: (...) II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei."

telemáticas (o que abrange dados de conexão) e o acesso a dados cadastrais.

No contexto do MCI e da legislação civil e criminal brasileira, é possível a uma pessoa prejudicada, agindo por si mesma ou por meio de seu advogado, notificar extrajudicialmente um provedor de Internet para remoção de conteúdo ilegal (em casos de violação de direitos autorais, veiculação de pedopornografia ou exposição indevida de nudez, por exemplo) e para a preservação de dados para fins probatórios mesmo na instância cível.

Essa notificação extrajudicial, tal como a solicitação administrativa regulada pelo MCI, destina-se à salvaguarda de direitos de uns (particulares) ou de todos (público em geral). Ambos os mecanismos de congelamento são providências preparatórias para medidas judiciais, que manterão sua utilidade, se os dados ainda estiverem com sua confidencialidade, integridade e disponibilidade resguardadas. É crucial, assim, que a medida de preservação de dados seja bem compreendida e interpretada, quanto a seus pressupostos, limites e alcance, à luz do MCI e da Convenção de Budapeste, notadamente por sua importância para a elucidação de crimes graves, como os que vitimam crianças e adolescentes ou atentam contra a segurança da sociedade e do Estado.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Jaqueline. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD. *In*: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel Ferreira; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro, RJ: Editora Forense, 2021. p. 583–603.

ARAS, Vladimir. "Breves comentários ao Marco Civil da Internet". **Blog do Vlad**, 5 de maio de 2014. Disponível em: https://vladimiraras.blog/2014/05/05/breves-comentarios-ao-marco-civil-da-internet/. Acesso em: 13 out. 2023.

ARAS, Vladimir. A título de introdução: segurança pública e investigações criminais na era da proteção de dados. *In*: ARAS, Vladimir; MENDONÇA, Andrey Borges de; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira; COSTA, Marcos Antonio da Silva (org.). **Proteção de dados pessoais e investigação criminal**. Brasília: Associação Nacional dos Procuradores da República, 2020. p. 14–31.

BIONI, Bruno Ricardo. **Autodeterminação informacional.** Dissertação [Mestrado em Direito Civil]. – Universidade de São Paulo, São Paulo, 2016

BRASIL. Comitê Gestor da Internet no Brasil. **Resolução CGI.br/RES/2009/003/P**, de 2009. Disponível em: https://www.cgi.br/resolucoes/documento/2009/003/. Acesso em: 13 out. 2023.

BRASIL. **Constituição da República Federativa do Brasil**. Promulgada em 5 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 out. 2023.

BRASIL. Decreto 11.491, de 12 de abril de 2023. **Promulga a Convenção sobre o Crime Cibernético**, concluída em Budapeste, em 23 de novembro de 2001 e objeto de adesão pelo Brasil em 30 de novembro de 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11491.htm. Acesso em: 13 out. 2023.

BRASIL. Decreto-lei nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 13 out. 2023.

BRASIL. Lei 12.850, de 2 de agosto de 2013. **Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 13 out. 2023.

BRASIL. Lei 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13 out. 2023.

BRASIL. Lei 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13 out. 2023.

BRASIL. Lei 9.296, de 24 de julho de 1996. **Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 13 out. 2023.

BRASIL. Superior Tribunal de Justiça. 5ª Turma. **Agravo Regimental no Habeas Corpus 709.810/SP**. Relator Ministro Joel Ilan Parcionik. Acórdão de 6 de março de 2023.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus 626.983/PR**. 6ª Turma. Relator Ministro Olindo Menezes. Acórdão de 8 de fevereiro de 2022. Disponível em:

https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=127222095&num_registro=202003003135&data=20220222&tipo=5&formato=PDF . Acesso em: 10 out. 2023.

BRASIL. Supremo Tribunal Federal. **Agravo Regimental no Habeas Corpus 222.141/PR**. Relator Ministro Ricardo Lewandowski. Voto do Ministro André Mendonça em 8 de setembro de 2023. Disponível em: https://sistemas.stf.jus.br/repgeral/votacao?texto=5849791 . Acesso em: 10 out. 2023.

BRASIL. Supremo Tribunal Federal. **Agravo Regimental no Habeas Corpus 222.141/PR.** Relator Ministro Ricardo Lewandowski. Voto do relator em 8 de setembro de 2023. Disponível em: https://sistemas.stf.jus.br/repgeral/votacao?texto=5741049. Acesso em: 10 out. 2023.

BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Ação Direta de Inconstitucionalidade 1480.** Relator Ministro Celso de Mello. Tribunal Pleno. Acórdão de 4 de setembro de 1997. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=347083. Acesso em: 13 out. 2023.

BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6390/DF.** Relatora Ministra Rosa Weber. Tribunal Pleno. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754358567. Acesso em: 13 out. 2023.

CASELLI, Guilherme. **Manual de investigação digital**. 2. ed. São Paulo: Editora Juspodivm, 2022.

COUNCIL OF EUROPE. **Explanatory Report to the Convention on Cybercrime**. Budapest, 23 XI 2001. Disponível em: https://rm.coe.int/16800cce5b. Acesso em: 13 out. 2023.

COUNCIL OF EUROPE. **Chart of signatures and ratifications of Treaty 185**. Status as of 13/04/2023. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 . Acesso em: 13 out. 2023.

COUNCIL OF EUROPE. **Convention 108 +**: Convention for the protection of individuals with regard to the processing of personal data. Strasbourg: COE, 2018. Disponível em: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. Acesso em: 10 out. 2023.

DAS, Pratyusha; SARKAR, Pradeepta. The Importance of Digital Forensics in the Admissibility of Digital Evidence. **NUJS Journal of Regulatory Studies**, *[S. l.]*, v. 7, p. 60, 2022.

FACHIN, Zulmar; DA SILVA, Deise Marcelino. "Avanços tecnológicos e a pessoa humana no século XXI: a (des)proteção do direito à privacidade no Marco Civil da Internet". **Revista Jurídica (0103-3506)**, *[S. l.]*, v. 5, n. 67, p. 230–254, 2021.

FISCHER, Douglas; VALDEZ, Frederico. **As obrigações processuais penais positivas: segundo as cortes Europeia e Interamericana de Direitos Humanos**. 2. ed. Porto Alegre: Livraria do Advogado Editora, 2019.

KERR, Orin S. "Digital Evidence and the New Criminal Procedure". **Columbia Law Review**, *[S. l.]*, v. 105, n. 1, p. 279–318, 2005.

KIST, Dario José. **Prova digital no processo penal**. Leme (SP): Mizuno, 2019.

LOGAN, Wayne A.; FERGUSON, Andrew Guthrie. "Policing Criminal Justice Data". **Minnesota Law Review**, [S. l.], v. 101, p. 541, 2016.

MAZZUOLI, Valerio de Oliveira. **Curso de direito internacional público.** 13. ed. Rio de Janeiro: Editora Forense, 2020.

MOURA, Maria Thereza Rocha de Assis; BARBOSA, Daniel Marchionatti. Dados digitais: interceptação, busca e apreensão e requisição. In: LUCON, Paulo Hnerique dos Santos; WOLKART, Erik Navarro; LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos (org.). **Direito, processo e tecnologia**. São Paulo: Thomson Reuters Brasil, 2020. p. 478–502.

POLLACK, Michael C. "**Taking Data**". University of Chicago Law Review, [S. l.], v. 86, p. 77, 2019.

PORTUGAL. **Lei nº. 109, de 15 de setembro de 2009**, que aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime. Disponível em: https://dre.pt/dre/detalhe/lei/109-2009-489693 . Acesso em: 13 out. 2023.

PORTUGAL. **Ministério Público:** o que são autoridades judiciárias, [s/d]. Disponível em: https://www.ministeriopublico.pt/perguntas-frequentes/intervenientes#:~:text=O%20que%20s%C3%A3o%20autoridades%20judici%C3%A1rias,o%20juiz%20(de%20julgamento). Acesso em: 13 out. 2023.

PORTUGAL. **Tribunal Constitucional.** Acórdão nº 268/2022, Rel. Cons. Afonso Patrão, j. em 19/04/2022, p. em 03/06/2022. Disponível

em: https://dre.pt/dre/detalhe/acordao-tribunal-constitucional/268-2022-184356510. Acesso em: 13 out. 2023.

QUITO, Carina. As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito às comunicações armazenadas. *In*: LUCON, Paulo Hnerique dos Santos; WOLKART, Erik Navarro; LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos (org.). **Direito, processo e tecnologia**. São Paulo: Thomson Reuters Brasil, 2020. p. 163–185.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz. **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021.

TEJERIZO, María de Arcos. "Digital evidence and fair trial rights at the International Criminal Court". **Leiden Journal of International Law**, *[S. l.]*, v. 36, n. 3, p. 749–769, 2023. DOI: 10.1017/S0922156523000031.

TRIBUNAL EUROPEU DE DIREITOS HUMANOS. **Case of Malone v. United Kingdom.** Judgment 2 August 1984, § 84. Disponível em: https://data.guardint.org/en/entity/7dczy15vda9?page=33. Acesso em: 13 out. 2023.

TZANOU, Maria; KARYDA, Spyridoula. Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga? **European Public Law**, [S. l.], v. 28, n. 1, p. 123–154, 2022. DOI: 10.2139/ssrn.3970756.

UNIÃO EUROPEIA. **Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002**, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações

electrónicas (Diretiva relativa à privacidade e às comunicações electrónicas). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32002L0058. Acesso em: 13 out. 2023.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE** (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 10 out. 2023.

UNIÃO EUROPEIA. Tribunal de Justiça da União (Grande Seção). **Acórdão de 6 de outubro de 2020,** Processos apensos C 511/18, C 512/18 e C 520/18. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=1866913 . Acesso em: 13 out. 2023.

UNIÃO EUROPEIA. Tribunal de Justiça da União. **Acórdão de 9 de novembro de 2010,** Processos apensos C 92/09 e C 93/09. Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) contra Land Hessen. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=79001&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=525431 . Acesso em: 13 out. 2023.