UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO

YASMIN RODRIGUES CALDAS

O CONGELAMENTO EXTRAJUDICIAL DE DADOS PARA FINS DE PERSECUÇÃO PENAL A PARTIR DO HC 222.141/DF

Brasília
2025

Yasmin Rodrigues Caldas

O CONGELAMENTO EXTRAJUDICIAL DE DADOS PARA FINS DE PERSECUÇÃO PENAL A PARTIR DO HC 222.141/DF

Monografia apresentada à Faculdade de Direito da Universidade de Brasília, como requisito parcial à obtenção do grau de Bacharel em Direito.

Orientador: Prof. João Costa-Neto

Brasília
2025

O Congelamento Extrajudicial de Dados para Fins de Persecução Penal a Partir do *Habeas Corpus* 222.141/DF

Monografia apresentada à banca examinadora abaixo qualificada em / / , para fins de avaliação.

_____

Pro. Dr. João Costa-Neto

Orientador

_____

Examinador

_____

Examinador

AGRADECIMENTOS

Ao longo desta jornada acadêmica repleta de desafios e de superações, um vasto e profundo agradecimento se faz necessário àqueles que, de maneira singular e irrepetível, contribuíram para que eu chegasse a este momento de conclusão. Cada passo dado foi sustentado por mãos generosas e corações dispostos a compartilhar sabedoria e afeto.

A Deus, expresso minha eterna gratidão, pois é por Sua orientação, força e eterna graça que fui capaz de ultrapassar os momentos de incerteza e perseverar na busca pelo conhecimento.

A minha amada mãe, Angela Maria, pela entrega incondicional, pelo amor imensurável e pelos sacrifícios feitos com coragem e generosidade, sou eternamente grata. Sua confiança irrestrita em meu potencial, cada ensinamento, gesto de carinho e incentivo, foram pilares fundamentais que sustentaram minha caminhada e me deram forças para seguir adiante. Dedico a ela minha mais profunda e sincera gratidão, que transcende palavras.

Ao meu pai, Salviano, que nos momentos que esteve comigo em tenra infância, me ensinou valiosas lições de vida que até hoje carrego.

Ao meu companheiro, Thiago Alexandre, pelo apoio e pelos momentos felizes compartilhados. Estendo também minha gratidão à sua família, nas pessoas de Danielle Filadelpho, Joaquim Santoro, Dulce Filadelpho, Karine Filadelpho, Flávia Filadelpho e Maria Eduarda Filadelpho, que são um exemplo de união e irradiam luz, generosidade e carinho.

A minha filha, Aurora, que me apresentou um amor puro jamais antes inscrito em minha cosmovisão, e com seu doce olhar me relembra todos os dias a beleza da vida.

Aos amigos-irmãos que tive a oportunidade de cultivar durante essa jornada, Raimundo Benvindo Neto, Rayra Benvindo e Rayssa Benvindo, que me fizeram sentir como parte de sua própria família ao compartilhar momentos de luta e de alegria.

Também expresso minha gratidão aos amigos Luís Fernando e Ana Júlia, Rafaella Krauspenhar e Rafael Muller e Thiago Maciel, companheiros de jornada, que com seu afeto e palavras de ânimo nos corredores da FD-UnB tornaram esta trajetória ainda mais significativa.

A minha amiga de infância, Kristina Borja, por sua amizade leal e constante apoio ao longo dos anos. Sua presença sempre foi um alicerce de carinho e confiança em minha vida.

A meu amigo Marcos Próbio e família, expresso profunda gratidão, especialmente nas pessoas de Íris Evangelista e Deocleciano Próbio, que me encorajaram a preservar frente aos desafios do início dessa trajetória, e generosamente me apoiaram fortalecendo minha determinação e acreditando no meu potencial.

A equipe de Direito Penal do Mudrovitsch Advogados, nas pessoas de Felipe Fernandes de Carvalho, Caroline Scandelari Raupp e Haderlann Chaves, pelo apoio e valioso aprendizado durante meu primeiro estágio na área.

Ao meu orientador, João Costa-Neto, expresso minha profunda gratidão. Sua dedicação incansável à excelência acadêmica, sua paciência ao esclarecer minhas dúvidas e sua generosidade em compartilhar conhecimentos foram pilares essenciais para a concretização deste trabalho. Suas orientações, sempre precisas e inspiradoras, iluminaram os momentos de incerteza, conduzindo-me com sabedoria e incentivando-me a alcançar novos horizontes do conhecimento jurídico.

Expresso também minha gratidão aos professores da Faculdade de Direito da Universidade de Brasília. Cada aula ministrada, cada debate instigante e cada orientação oferecida foram decisivos para minha formação acadêmica e pessoal. Com seu compromisso incansável com o ensino e a pesquisa, vocês não apenas transmitiram conhecimentos técnicos, mas também valores que moldaram minha visão crítica e ética.

Aos servidores e técnicos da Faculdade de Direito da Universidade de Brasília, por tornarem possível o funcionamento de nossa instituição, assegurando um ambiente acolhedor e propício ao aprendizado.

Por fim, deixo meu agradecimento aos que, de forma direta ou indireta, fizeram parte desta jornada e contribuíram para o meu crescimento.

RESUMO

Este trabalho analisa, criticamente, a admissibilidade do congelamento extrajudicial de dados no ordenamento jurídico brasileiro, com ênfase na preservação de dados de conteúdo para fins de persecução penal. Adotou-se, como ponto de partida, o *Habeas Corpus* 222.141/DF, que suscitou controvérsia sobre a aplicação dessa medida a dados de conteúdo, uma vez que a aplicabilidade da medida sobre dados cadastrais, registros de conexão e de acesso a aplicações de internet já era conformada pelo Marco Civil da Internet. Aborda-se o aparente conflito com a Convenção de Budapeste, cuja superveniência teria ampliado o escopo da medida também para os dados de conteúdo. Argumenta-se que a prática do congelamento extrajudicial de dados de conteúdo, sem a devida autorização judicial, viola a estrutura de proteção escalonada consagrada na legislação brasileira e contraria o princípio constitucional da privacidade. Conclui-se, de modo semelhante ao decidido no *Habeas Corpus* 222.141/DF, que embora a efetividade das investigações seja necessária, ela não pode se sobrepor aos direitos fundamentais, de modo que o congelamento extrajudicial de dados de conteúdo é incompatível com a sistemática jurídica brasileira e não deve ser admitido.

Palavras-chave: Congelamento extrajudicial de dados. Preservação de dados em nuvem. Conservação expedita de dados. Autodeterminação informativa. Privacidade. HC 222.141/DF. Marco Civil da Internet. Convenção de Budapeste. Proteção de dados pessoais. Direitos fundamentais.

ABSTRACT

This paper critically analyzes the admissibility of the extrajudicial freezing of data within the Brazilian legal system, with an emphasis on the preservation of content data for criminal prosecution purposes. The starting point of the analysis is HC 222.141/DF, which raised controversy over the application of this measure to content data, given that the applicability of the measure to registration data, connection records, and access to internet applications had already been established under the Brazilian internet Civil Framework (MCI), which sets out a tiered protection framework for data. This framework appeared to conflict with the Budapest Convention, whose supervening provisions seemingly expanded the scope of the measure to also cover content data. It is argued that the practice of extrajudicially freezing content data, without proper judicial authorization, violates the tiered protection structure established by Brazilian law and contradicts the constitutional principle of privacy. This also results in a violation of the newly incorporated right to informational self-determination, which guarantees individuals control over their personal data. It is concluded, similarly to the decision in HC 222.141/DF, that although the effectiveness of investigations is necessary, it cannot override fundamental rights. Therefore, the extrajudicial freezing of content data is incompatible with the Brazilian legal framework and should not be permitted.

Keywords: Extrajudicial data freezing. Data cloud preservation. Expedited data retention. Informational self-determination. Privacy. HC 222.141/DF. Civil Rights Framework for the Internet. Budapest Convention. Data protection. Fundamental rights.

SUMÁRIO

INTRODUÇÃO

Cada interação digital realizada gera um rastro de dados, que pode abarcar desde a localização geográfica até os padrões e os conteúdos encadeados da comunicação digital.[1] Atividades aparentemente triviais, como as transações comerciais em plataformas digitais ou o emprego de serviços de transporte via aplicativos, igualmente se inscrevem no universo da coleta e uso de dados. As companhias de transporte por aplicativo, a exemplo, fazem uso de dados de localização e itinerários prévios para otimizar trajetos, antever a demanda e aprimorar a experiência do usuário.[2]

As comunicações, principalmente, foram afetadas pela revolução digital, revelando-se um terreno fértil para a coleta e para a análise de dados. Cada mensagem trocada, cada e-mail enviado e, até mesmo, as interações em redes sociais são sistematicamente registradas. Este cenário, inimaginável há cerca de 20 anos, suscita uma série de questões éticas e jurídicas. A privacidade dos indivíduos, outrora considerada um direito fundamental arraigado ao texto da Constituição Federal de 1988, enfrenta novos desafios à medida que as fronteiras entre o privado e o público se tornam cada vez mais tênues, fenômeno causado pelos avanços tecnológicos.[3]

Atualmente, como reflete Vladimir Aras, a quantidade de dados disponibilizados ao se realizar uma viagem, por exemplo, permite que terceiros tenham acesso desde as pesquisas sobre as condições da viagem até a chegada ao hotel no destino; um número impressionante de dados pessoais, incluindo e-mail, número de passaporte, nome de cônjuge ou companheiro e filhos e informações financeiras, além da localização, da condição de saúde, da imagem recolhida em postos de checagem nos aeroportos e fronteiras, de nomes de acompanhantes em voos de companhias aéreas e de companheiros de hospedagem em hotéis.[4]

---

[1] PEREIRA, Marcelo Cardoso. **Direito à Intimidade na Internet.** Curitiba: Juruá, 2011, p. 114.

[2] MACHADO, Pedro Antônio de Oliveira. Prefácio. In: ARAS, Vladimir B.; MENDONÇA, Andrey B.; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno F. da; COSTA, Marcos Antônio da S. (Org.) **Proteção de Dados Pessoais e Investigação Criminal**. Ministério Público Federal. Brasília: ANPR, 2020, p. 14.

[3] FRAZÃO, Ana. Plataformas digitais, Big Data e riscos para os direitos da personalidade. In: TEPEDINO, Gustavo; MENEZES, Joyceane. (Org.) **Autonomia Privada, Liberdade Existencial e Direitos Fundamentais.** Belo Horizonte: Fórum, 2019, p. 333-349.

[4] ARAS, Vladimir Barros. A título de introdução: segurança pública e investigações criminais na era da proteção de dados. In: ARAS, Vladimir B.; MENDONÇA, Andrey B.; CAPANEMA, Walter Aranha;

Em síntese, a vida cotidiana, na era digital contemporânea, é marcada pela incessante coleta e utilização de dados. A quantidade de dados gerados e armazenados digitalmente tem se revelado uma fonte sem precedentes de imbróglios jurídicos clássicos, porém com contornos trazidos pela "revolução 4.0[5]", inéditos no âmbito da persecução penal.

Emerge, dessa conjuntura, uma multiplicidade de nuances que refletem a dificuldade de assimilação da nova realidade tecnológica pelo aparato de persecução penal estatal: a manutenção da cadeia de custódia e, obrigatoriamente, da proteção dos dados pessoais, que esbarra na complexidade técnica intrínseca ao procedimento de obtenção e utilização das provas digitais. Isso deságua no já arcaico e incessante dilema do equilíbrio entre proteção da privacidade e efetividade penal, que há muito constituem desafios intrínsecos à ordem constitucional acusatória e podem servir como sismógrafo do grau de democracia de um Estado.[6]

É no intrincado rol de circunstâncias acima descrito que se insere o caso do *Habeas Corpus* 222.141/DF, foco deste trabalho, que inaugurou uma controvérsia no Brasil: é admissível o congelamento extrajudicial de dados de conteúdo à luz do ordenamento jurídico brasileiro?

Frente a isso, o objetivo deste trabalho é analisar, criticamente, a admissibilidade do congelamento extrajudicial de dados no ordenamento jurídico brasileiro, com ênfase na preservação de dados de conteúdo para fins de persecução penal

---

SILVA, Carlos Bruno F. da; COSTA, Marcos Antônio da S. (Org.) **Proteção de Dados Pessoais e Investigação Criminal**. Ministério Público Federal. Brasília: ANPR, 2020, p. 14.

[5] Segundo Klaus Schwab, a Revolução 4.0, também conhecida como Quarta Revolução Industrial (4IR), teve suas raízes na evolução tecnológica que começou no final do século XX e início do século XXI. Ela sucede três grandes revoluções industriais: a primeira, no século XVIII, marcada pela mecanização e o uso do vapor; a segunda, no final do século XIX, com a eletricidade e a produção em massa; e a terceira, a partir dos anos 1960, com a digitalização e o advento dos computadores e da internet. O termo "Quarta Revolução Industrial" foi popularizado pelo economista Klaus Schwab, fundador do Fórum Econômico Mundial, em 2015. Ele destacou que a 4ª Revolução Industrial se diferencia das anteriores pela fusão das tecnologias físicas, digitais e biológicas, com avanços em inteligência artificial, robótica, internet das coisas e biotecnologia. A 4IR não apenas impacta a forma como produzimos e consumimos, mas também como vivemos e nos relacionamos, redefinindo indústrias, economias e sociedades globalmente. SCHWAB, Klaus. **The fourth industrial revolution.** 1. ed. New York: Currency, 2017. p. 28-109.

[6] ARABI, Abhner Youssif Mota. Utilização de dados pessoais no combate ao crime organizado: limites e possibilidades de técnicas especiais de investigação em meio digital. **Revista Judicial Brasileira**, v. 2, n. 1, 2022. p.71.

Ressalta-se que o caso versa, essencialmente, “apenas” sobre a preservação extrajudicial dos dados pelas empresas que o tutelam e não sobre a obtenção em si, que, em tese, ocorreria em momento posterior, após a prolação de decisão judicial específica para esse fim. Assim, a preservação dos dados teria a finalidade cautelar de resguardar a integralidade do acervo probatório detido pela empresa de tecnologia, de modo que, na hipótese de concessão de quebra de sigilo informacional, as evidências sejam encontradas incólumes de eventuais alterações realizadas pelo usuário titular das informações ou terceiros.

Essa particularidade, à primeira vista, pode parecer uma formalidade preliminar concernente apenas ao plano teórico e conceitual, dissociada de importância prática e substancial. Porém, diferentemente, muito ao revés, é exatamente o aspecto antecipado e dito cautelar da preservação dos dados que torna o caso paradigmático, trazendo à baila um dos novos bens jurídicos advindos da era digital: a autodeterminação informativa.

O desfecho do *Habeas Corpus* 222.141/DF não apenas traz um novo capítulo para o debate sobre a preservação de dados no contexto penal, mas também evidencia um ponto de tensão fundamental, que reside no cerne principiológico que orienta todo o sistema: até onde pode ir a persecução penal na nova sociedade em redes,[7] sem que os direitos constitucionais sejam violados?

Portanto, o caso vertido no *Habeas Corpus* 222.141/DF ilustra de forma muito clara o complexo panorama contemporâneo das provas digitais, percorrendo problemas que decorrem da necessidade de equilíbrio entre a privacidade e a efetividade investigatória.

O tema é relevante porque se situa no bojo de discussões internacionais relativas aos efeitos da evolução da tecnologia sobre a forma e os meios de comunicação nas relações sociais. De um lado, a ausência de fronteiras espaço-temporais no caráter virtual dessa comunicação tanto pode levar a uma extensão de conceitos dos direitos fundamentais e da respectiva incidência, quanto a uma eventual identificação de nuances deles. De outro, a legislação que vem sendo produzida muitas vezes não alcança a realidade do que se vive, seja pelo lapso entre o novo que se apresenta e sua regulação, seja pela novidade do assunto, cuja abordagem requer sutileza nas observações e correspondência jurídica.

---

[7] Termo cunhado na obra CASTELLS, Manuel. **A sociedade em rede:** a era da informação, economia, sociedade e cultura. 8. ed. São Paulo: Paz e Terra, 2005.

Metodologicamente, o trabalho foi feito por meio de uma pesquisa bibliográfica, sendo consultadas publicações nacionais e internacionais sobre o tema. Foi feita também uma pesquisa documental sobre jurisprudências nacionais e de outros países. Respectivamente, o marco teórico foi constituído pelas obras de Vladimir Aras e de André Machado Maya (em menor escala), e o exemplo jurisprudencial básico foi o *Habeas Corpus* 222.141/DF.

O trabalho foi estruturado em três capítulos. No primeiro capítulo, enfoca-se a controvérsia vertida no *Habeas Corpus/DF*, expondo basicamente em que consiste a medida de congelamento extrajudicial de dados. Para melhor elucidação da discussão, analisar-se-á a legislação aplicável ao tema, perpassando pela análise da estrutura escalonada de proteção de dados estabelecida no Marco Civil da internet, que diferencia dados cadastrais, registros de conexão e dados de conteúdo, e limita o escopo do congelamento extrajudicial de dados apenas às duas primeiras espécies. Também serão cotejadas as disposições da Convenção de Budapeste que, ao recomendar a "conservação expedita" de dados aos países signatários, amplia o escopo da medida ao genérico escopo de "dados de computador".

No segundo capítulo, após a exposição do panorama legal do congelamento extrajudicial de dados e compreensão da lacuna quanto à aplicação da medida sobre dados de conteúdo, são analisados os fundamentos e as controvérsias suscitadas, tanto no julgamento prévio pela 6ª Turma do Superior Tribunal de Justiça, quanto na paradigmática decisão proferida pelo Supremo Tribunal Federal. Também são explorados os vieses doutrinários que se posicionam de forma contrária à decisão, e defendem a ampliação do congelamento extrajudicial para além das hipóteses do MCI, isto é, também sobre dados de conteúdo.

No terceiro capítulo, são apresentados argumentos pessoais referentes ao tema objeto de estudo, os quais foram desenvolvidos com base nas leituras realizadas durante a seleção do material coletado para esta pesquisa. Alguns pontos são especificamente abordados: cotejo entre segurança jurídica e persecução penal efetiva; ausência de regulamentação específica para a preservação de dados de conteúdo, o que põe em tensão normas nacionais e internacionais, gerando um cenário de insegurança jurídica; o Marco Civil da Internet, que regula o congelamento extrajudicial de outras duas espécies de dados, mas deixa de contemplar os dados de conteúdo.

Além do preenchimento da lacuna por meio da interpretação sistemática dos próprios dispositivos desse Marco, o art. 5º, inciso XII da Constituição Federal e a respectiva regulamentação da Lei 9.296/1996 evidenciam um “silêncio eloquente” relativo à clara impossibilidade do congelamento extrajudicial de dados de conteúdo. Demonstra-se como o princípio da autodeterminação informativa, que exige que o titular dos dados mantenha o controle sobre sua utilização, mesmo em investigações criminais, se mostra um princípio integrador útil para solucionar a lacuna evidenciada.

Nesse capítulo, analisa-se também a superveniência da Convenção de Budapeste e demonstra-se que, pela análise cautelosa de seus artigos, não há impositividade do congelamento extrajudicial da dados, mas tão somente a rápida e efetiva conservação das provas, ainda que submetida ao crivo judicial, dada a relevância das provas no combate à cibercriminalidade transnacional. Demonstra-se, também, que eventual ampliação da medida não apenas é divorciada da sistemática do próprio tratado e da legislação brasileira, como também afronta limites constitucionais cuja flexibilização não se mostra razoável. Isso, porque a preservação extrajudicial de dados é suficientemente assistida por disposições do ordenamento brasileiro, harmonizando a necessidade de persecução penal com as garantias fundamentais.

1 O QUE É CONGELAMENTO EXTRAJUDICIAL DE DADOS? FUNDAMENTOS E PANORAMA JURÍDICO DA MEDIDA

1.1 Delimitação da controvérsia

O congelamento extrajudicial de dados refere-se à prática por meio da qual empresas de tecnologia, como provedores de serviços de internet, plataformas de redes sociais e aplicativos de comunicação, preservam temporariamente dados armazenados em seus servidores a pedido de autoridades (Ministério Público ou autoridade policial), mesmo antes de uma ordem judicial ser expedida. A medida tem como objetivo garantir que as informações sejam mantidas intactas, evitando sua exclusão ou alteração, enquanto as autoridades competentes buscam a autorização judicial necessária para acessá-las de fato.[8]

Essa preservação é especialmente utilizada em investigações criminais, quando há risco iminente de que provas digitais relevantes sejam perdidas. Discute-se a possibilidade de aplicação da medida aos dados de conteúdo, isto é, se se pode solicitar, a uma plataforma, que preserve registros de acesso, mensagens ou arquivos compartilhados por um usuário até que o pedido formal seja apreciado pelo Poder Judiciário.

A prática encontra previsão expressa na Lei n.º 12.965, de 2014, o Marco Civil da internet (MCI), como se verá detalhadamente adiante, ao regular o dever de guarda de algumas espécies de dados pelas empresas, o que, até então, não era alvo de controvérsias significativas. A controvérsia sobre os limites e a legalidade dessa medida teve origem no julgamento do citado *Habeas Corpus* (HC) 222.141/DF pelo Supremo Tribunal Federal (STF), Segunda Turma, de relatoria do Ministro Ricardo Lewandowski, relatoria do acórdão Ministro Gilmar Mendes, julgado em 06/2/2024. O julgamento trouxe à tona o debate acerca da compatibilidade da preservação de dados, especificamente de conteúdo, com as disposições processuais penais e o próprio MCI, além da proporcionalidade, considerando os direitos fundamentais.

O HC 222141/DF versa sobre uma requisição, do Ministério Público do Estado do Paraná, de preservação ou “congelamento” de dados cadastrais, de histórico de pesquisa, de todo conteúdo de *e-mail* e de *iMessages*/*hangouts*, de fotos,

[8] SUPREMO TRIBUNAL FEDERAL. **Habeas Corpu**s n. 222.141/DF.

de contatos e de histórico de localização, relativos à investigada. Isso, sem autorização judicial para que a diligência, consistente na manutenção integral daqueles dados, gerados de 01/06/2017 a 22/11/2019, fosse realizada.[9]

O cerne da discussão residiu, essencialmente, na interpretação sistemática dos artigos 10, 13 e 15 do MCI, autorizam a preservação extrajudicial dos dados de conexão e de aplicação de internet,[10] não abrangendo, contudo, os dados de conteúdo, compreendidos como os dados telemáticos e comunicações.

A Convenção de Budapeste, que entrou em vigor no Brasil em 2023, inseriu uma aparente ampliação do escopo de dados sujeitos à preservação extrajudicial ou, mais precisamente, a “preservação expedita” de dados, conforme expresso em seu artigo 16.[11]

Diferentemente do MCI, que estabelece a preservação extrajudicial de dados de acordo com a organização das respectivas categorias específicas, a Convenção de Budapeste reza que a medida deve incidir sobre "dados de computador especificados, incluindo dados de tráfego, que tenham sido armazenados por meio de um sistema de computador."[12] Segundo a interpretação de Cortez, essa definição abrange informações pessoais, seja do usuário, do dispositivo eletrônico ou do conteúdo trocado entre dois ou mais interlocutores.[13] Representa, portanto, um escopo muito mais amplo que o estabelecido pelo MCI para a dita preservação.

O HC 222141/DF, nesse cenário, suscitou a controvérsia sobre o tema, ilustrando concretamente como a questão impacta a persecução penal cotidiana. O caso, ao abranger a questão das provas digitais, envolve discussões contemporâneas sobre temas, há muito, caros ao Direito: a dicotomia entre o público e o privado e a segurança jurídica dos cidadãos, em face do poder/dever de persecução penal estatal.[14]

---

[9] Ibid.
[10] LEI n.º 12.965, de 23 de abril de 2014. **Marco Civil da internet.** Artigos 10, 13 e 15.
[11] CONSELHO DA EUROPA. Convenção sobre o Crime Cibernético. **Convenção de Budapeste**, artigo 16.
[12] Ibid. Artigo 1º.
[13] CORTEZ, Raphaela Jéssica Reinaldo. **Prova digital no processo penal brasileiro: o uso de dados de geolocalização na segurança pública e na investigação criminal**. Orientador: Walter Nunes da Silva Júnior. 2023. 104f. Dissertação (Mestrado em Direito) - Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2023. p. 83.
[14] BLEDLIN, Felipe. Análise da lei n. 12.654/2012, que prevê a identificação e a investigação criminal genética, à luz dos direitos fundamentais. In: ARAS, Vladimir B.; MENDONÇA, Andrey B.; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno F. da; COSTA, Marcos Antônio da S. (Org.) **Proteção de Dados Pessoais e Investigação Criminal**. Ministério Público Federal. Brasília: ANPR, 2020, p. 310.

Convém pontuar que a discussão fulcral do acórdão se refere tão somente à preservação extrajudicial de dados e não ao acesso extrajudicial propriamente dito. Esse detalhe traz ao caso especial relevância, pois a preservação extrajudicial de dados, a depender da espécie dos dados e do nível de proteção conferido pela legislação brasileira, não encontra regulamentação expressa e clara no ordenamento. É o que ocorre com os dados de conteúdo, os quais, ao se fazer uma correspondência legal entre as classificações trazidas pelo MCI e pela Convenção de Budapeste, têm a preservação extrajudicial vedada pelo primeiro regramento e autorizada pelo segundo, aparentemente.

O procedimento fica, portanto, na lacuna das leis, atraindo conflitos sobre aplicação extensiva das normas, uma vez que questões de privacidade, de proteção de dados e de direitos fundamentais entram em choque com as necessidades de investigação e de persecução penal, erigindo um desafio adicional de ponderação principiológica para resolver a questão da (in)admissibilidade da concessão extrajudicial da medida. E é justamente o fato de a controvérsia limitar-se ao “mero congelamento de dados”, sem autorização judicial específica e antes da prolação da decisão de disponibilização das informações, que torna o caso notório.

Diante do surgimento recente da discussão, desencadeada pelo caso concreto do HC 222141/DF, a doutrina e a produção acadêmica sobre o caso são de notória escassez. Embora haja trabalhos que expõem a possibilidade de conservação extrajudicial disposta no MCI e na Convenção de Budapeste, o tema não se mostrava problemático, e a divergência entre essas legislações também não suscitava maiores entraves. Assim, não se havia questionado judicialmente, até então, a possibilidade de preservação, mediante requisição do MP, de dados de conteúdo.

Até a finalização desta monografia, o trabalho disponível mais proeminente sobre o tema é o artigo "Congelamento de Dados Informáticos para Fins de Prova no Processo Penal", escrito por Vladimir Aras e publicado no final de 2023 na revista *Delictae*. Nesse artigo, Aras defende uma posição divergente da adotada pela Suprema Corte, argumentando a favor da possibilidade ampla da preservação extrajudicial de dados, isto é, de todos os tipos de dados, incluindo comunicações privadas.[15]

[15] ARAS, Vladimir. O congelamento de dados informáticos para fins de prova no processo. **Delictae Revista de Estudos Interdisciplinares sobre o Delito**, v. 8, n. 15, 2023. p. 180-223.

No caso objeto de estudo, a ordem de HC foi concedida para anular provas obtidas após pedido de congelamento de dados armazenados pelas plataformas Google e Apple. O Ministério Público do Estado do Paraná e, subsequentemente, o Ministério Público Federal defenderam que as provas só foram efetivamente disponibilizadas após autorização judicial específica para esse fim, de modo que o procedimento estaria em conformidade com o MCI e a Convenção de Budapeste.[16]

Após deliberação, a 2ª Turma do Supremo Tribunal Federal concedeu, por três votos (votaram pela nulidade das provas o Ministro Ricardo Lewandowski, Ministro Gilmar Mendes e Nunes Marques) contra dois votos (votaram pela validade das provas o Ministro André Mendonça e o Ministro Edson Fachin), decisão favorável à impetrante, no sentido de declarar nulas as provas oriundas do congelamento extrajudicial de dados.

O desfecho do paradigmático HC 222.141/DF representa um marco significativo na jurisprudência brasileira em relação à proteção dos direitos fundamentais no ambiente digital. Como observa Vladimir Aras, ao refletir sobre a relevância dessa decisão, é de se projetar que outros casos semelhantes chegarão às cortes superiores brasileiras, de modo que o impacto futuro desse precedente é inegável.[17]

1.2. Legislação conexa ao congelamento extrajudicial de dados

Entender os dispositivos que versam sobre o congelamento extrajudicial de dados é fundamental para compreender as particularidades da discussão, surgida de uma lacuna entre o escopo de cada dispositivo.

A inquietude quanto à temática da regulação do ambiente digital e tutela de dados no Brasil foi inaugurada pelo MCI.[18] Embora o MCI tenha lançado as redes para iniciar um movimento regulatório acerca das inovações trazidas pela internet, a legislação mais notória específica sobre proteção de dados pessoais é a Lei nº 13.709 de 2018, a Lei Geral de Proteção de Dados (LGPD), resultado do Projeto de Lei nº 53, de 2018, que se originou após o mundialmente famoso escândalo entre a Cambridge

[16] SUPREMO TRIBUNAL FEDERAL. **Habeas Corpus n. 222.141/DF**.
[17] ARAS, Vladimir. O congelamento de dados informáticos para fins de prova no processo. **Delictae Revista de Estudos Interdisciplinares sobre o Delito**, v. 8, n. 15, 2023. p. 185
[18] PONTE, A. Da necessidade de limites ao tratamento e compartilhamento de dados por órgãos de inteligência do Estado à luz da Lei Geral de Proteção de Dados em matéria penal. **Caderno Virtual**, Brasília, v. 1, n. 54, 2022. p. 67.

Analytic e o Facebook, ocorrido em 2016.[19] Tal escândalo acentuou a preocupação sobre a tutela dos dados pessoais e o grande impacto que a falta de balizas legais pode acarretar, até mesmo em relação à manutenção da estrutura democrática.

A LGPD foi formulada com inspiração na Diretiva 679/2016, conhecida como *General Data Protection Regulation* (GDPR) da União Europeia, regramento pioneiro em assegurar aos cidadãos europeus direitos significativos, relativos à transparência no processamento de seus dados pessoais, incluindo informações sobre onde e com que finalidade seus dados são tratados, aumentando a proteção para os titulares dos dados.[20]

De acordo com Ana Frazão, em paralelo ao regramento europeu, a LGPD visa garantir que a coleta e o uso de dados pessoais sejam realizados de maneira transparente e adequada, preservando assim os direitos fundamentais dos indivíduos em relação à privacidade e proteção de seus dados pessoais.[21]

Todavia, a despeito da completude e da solidez conceitual e regulatória da LGPD, sua aplicação não abrange o tratamento de dados no âmbito da segurança pública e da persecução penal. Pelo disposto em seu artigo 4º, inciso III, alíneas “a” e “d”, tal legislação não se aplica ao tratamento de dados pessoais realizado exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e de repressão de infrações penais.[22]

Assim, embora seja posterior ao MCI, a LGPD não contempla a regulação específica das questões relativas à coleta, tratamento e compartilhamento de dados no contexto penal, deixando um vácuo regulatório sobre o tema.

---

[19] O escândalo da Cambridge Analytica centrou-se na aquisição de dados pessoais sensíveis obtidos por meio de uma pesquisa realizada com usuários do Facebook e seu subsequente uso pela empresa, que na época trabalhava para o candidato republicano Donald Trump. Conforme retratado no documentário "The Great Hack", da Netflix, os dados sensíveis compartilhados com a Cambridge Analytica conseguiram capturar as preferências e inclinações políticas de milhões de pessoas através de seus perfis na plataforma do Facebook. Com isso, mensagens promovendo Trump e criticando sua adversária foram impulsionadas de maneira personalizada para os usuários, influenciando suas ações e decisões conforme as notícias apareciam em seus perfis. O caso teve um impacto global devido à percepção de manipulação, que se considerou ter interferido na escolha eleitoral de uma sociedade democrática. TOSCHI, Aline Seabra; LOPES, Herbert Emílio Araújo. **Dados de Tróia**. Proteção de dados pessoais e investigação criminal. 2020, p. 24. Disponível em: http://www.anpr.org.br/. Acesso em: 24 dez. 2024.

[20] Ibid., p. 68.

[21] FRAZÃO, Ana. Direitos básicos dos titulares de dados pessoais. **Revista do Advogado**, v. 39, n. 144, p. 33-46.

[22] LEI Nº 13.709 de 2018. (LGPD) Art 4º III - realizado para fins exclusivos de: a) segurança pública; [...] d) atividades de investigação e repressão de infrações penais; ou [...] § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

A regulação do tratamento de dados na seara penal regressa, então, ao MCI, com disposições que deram à luz a discussão vertida no HC 222.141/DF, revelando um panorama legal circular. Um dos pontos centrais dessa discussão é a interpretação do art. 13 da legislação referida, que permite à autoridade policial, administrativa ou ao Ministério Público requererem, cautelarmente, aos provedores de conexão de internet, a preservação dos registros de conexão por um prazo superior ao previsto inicialmente (um ano), conforme estipulado no § 2º. Tal preservação pode ocorrer sem autorização judicial prévia, com o intuito de proteger dados essenciais para investigações.

De acordo com as denominações trazidas pelo art. 5º do MCI, registros de conexão são "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".[23] Esses registros não contêm o conteúdo acessado, mas fornecem dados técnicos que podem ser úteis para identificar o momento e o local de uma conexão, além de permitir a identificação do dispositivo conectado à rede.[24] Por exemplo, um registro de conexão pode indicar que um dispositivo iniciou a conexão à internet em 24.12.2024 às 08:00 e encerrou às 09:30, utilizando o endereço IP 123.456.78.90, com uma duração total de 1h30min, e que o IP estava vinculado a uma rede localizada em São Paulo, Brasil.

Foi precisamente com base nesses artigos que, no HC 222.141/DF, o Ministério Público requereu diretamente às empresas Google e Apple o congelamento de dados cadastrais, histórico de pesquisa, todo conteúdo de *e-mail* e *iMessages*/hangouts, fotos, contatos e histórico de localização da investigada no âmbito do procedimento investigatório que originou o caso em análise[25], informações que em muito extrapolam a delimitação de "registros de conexão", mencionado no artigo em comento. Versa o referido artigo 13 do MCI que:

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
> § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

---

[23] LEI N. 12.965, de 23 de abril de 2014.
[24] LEITE, George S.; LEMOS, Ronaldo. **Marco Civil Da Internet.** Rio de Janeiro: Atlas, 2014. *E-book.* p.323. Disponível em: https://integrada.minhabiblioteca.com.br/ Acesso em: 16 out. 2024.
[25] SUPREMO TRIBUNAL FEDERAL. **Habeas Corpus n. 222.141/DF**.

> § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.
> § 3º 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.
> § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º , que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º .
> § 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

Como se pode extrair do dispositivo, o § 3º do artigo impõe um limite temporal e a reserva de jurisdição para acesso efetivo às informações, exigindo que a autoridade requerente solicite a autorização judicial de acesso propriamente dito dentro de 60 dias.

Embora não tenha sido alvo direto da controvérsia do caso em estudo, o art. 15 do MCI também autoriza o congelamento extrajudicial de dados. O § 2º do referido artigo permite que a autoridade policial, administrativa ou o Ministério Público requeiram, cautelarmente, a preservação dos registros de acesso a aplicações de internet por prazo superior a seis meses, de modo similar ao procedimento previsto para os registros de conexão no art. 13 do MCI, mas com prazo diferente.

Já os registros de acesso a aplicações de internet, de acordo com as definições do art. 5ª do MCI, por sua vez, consistem no conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.[26] Embora haja certa controvérsia técnica sobre a delimitação desse conceito, uma vez que a denominação “uso” pode ser mais ou menos abrangente, esses registros não abarcam o conteúdo das comunicações ou dados telemáticos em si. Eles se referem aos metadados de acesso — ou seja, informações sobre quando e como a aplicação foi utilizada, isto é, um resumo das interações realizadas, mas não sobre o que foi acessado ou trocado em termos de conteúdo.[27] Por exemplo, um registro de acesso a aplicações pode indicar que o dispositivo acessou o *Instagram* às 08:15 e *Netflix* às 20:00, ambos utilizando o IP 123.456.78.90, sem revelar quais fotos foram visualizadas ou quais filmes foram assistidos.

---

[26] LEI nº 12.965, de 23 de abril de 2014..
[27] LEITE, George S.; LEMOS, Ronaldo. **Marco Civil da Internet.** Rio de Janeiro: Atlas, 2014. E-book. p.323-324. Disponível em: https://integrada.minhabiblioteca.com.br Acesso em: 16 out. 2024.

Em qualquer hipótese, conforme os §§ 5º do art. 13 e 3º do art. 15 do MCI, a disponibilização desses registros ao requerente — ou seja, o acesso efetivo aos dados — depende de autorização judicial, reafirmando o papel do Judiciário na proteção dos direitos fundamentais, especialmente à vida privada e intimidade.

Os únicos dados cujo acesso é franqueado à autoridade ministerial, sem autorização judicial, são os dados cadastrais, conforme se depreende da leitura do § 3º do art. 10 do MCI[28].

Para fins de delimitação conceitual, o regulamento do MCI[29] define de forma mais completa quais são os dados considerados cadastrais: filiação, endereço e qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário. Esses dados podem ser preservados por meio de requisição direta do MP ou da autoridade policial, embora dispensem esse procedimento cautelar, uma vez que podem ser diretamente acessados pelo Ministério Público sem ordem judicial, conforme exposto acima. Os dados cadastrais, portanto, são informações com menor grau de proteção na sistemática do MCI, ocupando o degrau inicial de sigilo, conforme destaca Vladimir Aras.[30]

Já os dados de conexão e de acesso às aplicações, como sobredito, não podem ser acessados diretamente pelo Ministério Público, sendo necessária a obtenção de autorização judicial prévia para tal. Esses dados, conforme destaca Vladimir Aras, envolvem um grau mais profundo de interferência estatal na vida privada dos indivíduos, pois revelam informações que vão além dos meros dados cadastrais.[31]

Enquanto os dados cadastrais se limitam a identificar o usuário, os dados de conexão e de acesso expõem detalhes mais sensíveis, como os momentos exatos em que o usuário esteve conectado à internet e o IP utilizado, permitindo traçar um perfil mais completo de sua atividade online.[32]

---

[28] LEI n.º 12.965, de 23 de abril de 2014 (MCI). Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. § 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

[29] DECRETO 8.771/2016, art. 11, §2º .

[30] ARAS, Vladimir. O congelamento de dados informáticos para fins de prova no processo. **Delictae Revista de Estudos Interdisciplinares sobre o Delito**, v. 8, n. 15, 2023. p. 178-194.

[31] Ibid.

[32] LEITE, George S.; LEMOS, Ronaldo. **Marco Civil da Internet**. Rio de Janeiro: Atlas, 2014. *E-book.* p.323-324. Disponível em: https://integrada.minhabiblioteca.com.br/ Acesso em: 16 out. 2024.

Por isso, Aras observa que, ao permitir o acesso a esses dados, sobe-se "um degrau na escala de interferências do Estado sobre a vida privada[33]", o que exige uma maior cautela e proteção mais robusta, por parte do ordenamento jurídico. Como se nota na leitura dos dispositivos citados, o MCI apenas permite o congelamento extrajudicial de limitado rol de dados, quais sejam, os registros de conexão e registros de acesso a aplicações de internet.

Os dados de conteúdo comunicacional, embora não sejam expressamente mencionados no MCI, são considerados, em uma interpretação sistemática, como extremamente sensíveis. Esses dados abrangem as informações efetivamente trocadas entre usuários na internet durante uma telecomunicação, seja por meio de telefonia fixa, dispositivos celulares, e-mails ou mensageiros instantâneos, por meio de canais criptografados ou não.[34] Tais informações refletem o conteúdo das comunicações em si, diferenciando-se dos dados cadastrais ou de conexão, e revelam detalhes íntimos sobre as interações entre indivíduos.

Além da proteção conferida pelo inciso XII do art. 5º da Constituição Federal, que assegura a inviolabilidade do sigilo das comunicações, os incisos II e III do art. 7º do MCI[35] também garantem a inviolabilidade e o sigilo tanto do fluxo das comunicações pela internet, quanto das comunicações privadas armazenadas, permitindo seu acesso apenas mediante ordem judicial. Os dispositivos citados asseguram um alto grau de proteção a esses dados, reconhecendo sua natureza especialmente sensível e vinculada diretamente ao direito à privacidade e à intimidade dos indivíduos.

Ao tratar da proteção de dados no contexto investigatório, segundo Vladimir Aras, o MCI estabelece um modelo coeso de proteção às informações pessoais sujeitas a tratamento em sistemas informatizados. Esse modelo é estruturado em diferentes níveis de segurança, conforme o tipo de dado envolvido: dados cadastrais possuem o nível mais baixo de proteção, dados de conexão têm proteção

---

[33] ARAS, Vladimir. O Congelamento de Dados Informáticos para Fins de Prova no Processo. **Delictae Revista de Estudos Interdisciplinares sobre o Delito**, v. 8, n. 15, 2023. p. 194.
[34] Ibid. p.190.
[35] LEI n.º 12.965, de 23 de abril de 2014 (MCI). Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

intermediária, enquanto os dados de conteúdo comunicacional são resguardados por uma segurança elevada, dada sua maior sensibilidade.[36]

É o que se denominará, no presente trabalho, como nível escalonado de proteção de dados, já que as instâncias de proteção e sigilo podem ser organizadas em três níveis e organizadas em uma estrutura piramidal.

Nesse sentido, Aras identifica três situações distintas em que se permite o acesso a dados pessoais digitais para fins de persecução criminal: a primeira envolve os dados cadastrais, que podem ser requisitados diretamente pelo Ministério Público ou pela polícia no curso de uma investigação criminal, sem necessidade de autorização judicial; a segunda refere-se aos dados de tráfego e de conexão, que exigem prévia autorização judicial para seu acesso, seja no contexto de investigações criminais, cíveis, trabalhistas ou administrativas; a terceira situação diz respeito aos dados de conteúdo que, por sua elevada proteção, só podem ser acessados mediante ordem judicial e exclusivamente para fins de persecução criminal, conforme previsto na Lei 9.296/1996.[37]

No HC 222.141/DF, um dos fundamentos denegatórios do congelamento extrajudicial de dados, fora das hipóteses expressamente previstas no MCI, foi precisamente a distinção entre as diferentes espécies de dados e os diversos níveis de proteção conferidos a cada uma dessas classificações, considerando o grau de sensibilidade das informações.[38]

Como visto, o MCI é, de fato, o único regramento atualmente em vigor sobre o congelamento extrajudicial de dados, embora não preveja expressamente a preservação de dados de conteúdo. O voto condutor do acórdão no HC 222.141/DF se alinhou corretamente a essa normativa, reconhecendo o silêncio do MCI quanto à preservação de dados de conteúdo, que parece refletir uma escolha legislativa deliberada de não incluir essa possibilidade precisamente para proteger as comunicações privadas.

As divergências levantadas no julgamento do caso não se aprofundaram muito nessa questão, reconhecendo prontamente que a requisição direta realizada pelo Ministério Público extrapolou os limites estabelecidos pelo MCI. Trata-se de uma

---

[36] ARAS, Vladimir. O Congelamento De Dados Informáticos Para Fins De Prova No Processo. **Delictae Revista de Estudos Interdisciplinares sobre o Delito**, v. 8, n. 15, 2023. p. 178-194.
[37] Ibid.
[38] SUPREMO TRIBUNAL FEDERAL. **Habeas Corpus n. 222.141/DF.**

carência significativa na legislação, quanto à regulação específica das provas digitais no processo penal, as quais se inserem em uma realidade digital cada vez mais vasta e complexa. Não à toa, estudiosos, como Costa, Júnior defendem a necessidade de um marco processual específico para a internet, que possa suprir essa lacuna.[39]

Nesse cenário, o MCI emerge como a única legislação de abrangência nacional capaz de fornecer, ainda que de forma inicial e limitada, critérios básicos para nortear a solução das questões complexas discutidas no HC 222.141/DF. Embora ele represente um avanço nos procedimentos relacionados às provas digitais, carece do detalhamento necessário para o tema. Alguns autores, como Eduardo Tomasevicius Filho, argumentam que o MCI não trouxe inovações significativas ao ordenamento jurídico, repetindo disposições já previstas na Constituição Federal, como a inviolabilidade da intimidade e o direito ao sigilo e à liberdade de expressão.[40] Já Freitas, Silva e Souza destacam que, apesar dos entraves, foi por meio dessa norma que se conquistaram medidas cautelares e urgência na preservação de evidências digitais. No entanto, afirmam que os procedimentos ainda são truncados e que a falta de clareza gera desafios,[41] os quais podem, inclusive, ser ilustrados pela controvérsia do caso em estudo.

A falta de normatização acerca das provas digitais e toda a complexidade de procedimentos, decorrentes de sua emergência, não são um desafio enfrentado apenas pela legislação brasileira.[42] Isso se dá, especialmente, em função do fenômeno da “globalização das evidências criminais”, expressão cunhada por Wilson Antônio Paese Segundo. Para o autor, essa expressão descreve a situação em que provas essenciais para elucidar delitos cometidos em um país estão frequentemente armazenadas em território estrangeiro, que não tem qualquer conexão direta entre o

---

[39] COSTA JR., Ivan Jezler. A busca por um marco processual da internet: requisitos para colheita dos dados armazenados em compartimentos eletrônicos. 2018. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica do Rio Grande do Sul, Programa de Pós-Graduação em Ciências Criminais, Porto Alegre, 2018. p. 132-137.

[40] TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. Estudos Avançados, São Paulo, Brasil, v. 30, n. 86, p. 269–285, 2016. p. 279.

[41] FREITAS, Elison A.; SILVA, Pedro Henrique Aguiar; SOUZA, Márcio Cabral de. Crimes cibernéticos: desafios da investigação e preservação das provas. **Facit Business and Technology Journal**, v. 1, n. 44, 2023, p. 178-194. Tocantins, 2023.

[42] BORTOT, Jessica Fagundes. Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. **VirtuaJus,** v. 2, n. 2, p. 343- 348, 2017.

caso sob investigação e o Estado onde os dados estão localizados ou onde se encontra a sede do prestador de serviços[43].

Além da incidência do Marco Civil da Internet, o caso atrai a aplicação da Convenção de Budapeste, regramento internacional desenvolvido no intento de homogeneizar a política criminal contra os crimes cibernéticos entre os países signatários. Isso, por meio da criação de legislação nacional, processual e material, em consonância com os preceitos fixados nos objetivos daquele documento, para possibilitar a persecução penal dos crimes cibernéticos, conforme reflete Bortot.[44]

A autora menciona os seguintes objetivos principais da Convenção de Budapeste:

> a) A criminalização de um conjunto de delitos contra e através de computadores no direito doméstico e a harmonização dos elementos normativos relativos às infrações;
>
> b) Definição dos poderes necessários às autoridades competentes, de acordo com o código de processo penal pátrio, para proteger as provas digitais de qualquer crime, como mandado de busca e apreensão, etc. E ainda, limitar tais poderes, a fim de evitar abuso de poder e proteger os princípios fundamentais dos Estados;
>
> c) Instigar uma cooperação internacional rápida e eficaz, além de uma cooperação das forças policiais e do judiciário. A criminalização de condutas específicas, mas também sobre a definição de procedimentos para investigação e produção de provas referentes aos crimes virtuais.[45]

O referido tratado internacional de justiça criminal foi criado em 2001, na Hungria, pelo Conselho da Europa e entrou em vigor em 2004. O Brasil foi convidado a aderir a tal norma em 2019 e, após o convite, pôde participar, como observador, das reuniões sobre a Convenção e seus protocolos.[46] Porém, somente em 2021, com a publicação do Decreto Legislativo nº 37/2021, consolidou-se a aderência formal à Convenção de Budapeste, com o depósito dos documentos que sinalizam a intenção

---

[43] PAESE SEGUNDO, Wilson Antônio. Aquisição de provas criminais eletrônicas no Brasil à luz da Convenção de Budapeste, do Cloud Act dos Estados Unidos Da América e do direito da União Europeia. **Galileu. Revista de Direito e Economia,** v. XXII, p. 65, 2022.

[44] BORTOT, J. F. **Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com Base nas Legislações Brasileira e Internacional**. Belo Horizonte. Virtuajus, v. 2, n. 2, p. 338-362, 8 ago. 2017. p. 346-347.

[45] Ibid.

[46] DUARTE, Ana Luísa Vieira. **Análise do encaixe da Convenção de Budapeste no ordenamento jurídico brasileiro.** 2022. 48 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) — Universidade de Brasília, Brasília, 2022. p. 18.

de adesão ao tratado referido.[47] Entrou em vigor, efetivamente, em 12 de abril de 2023, data de publicação do Decreto nº 11.491.[48]

O referido dispositivo legal transnacional, como dito, tem como finalidade geral o combate à cibercriminalidade, abrangendo tanto a tipificação de delitos propriamente digitais ou aqueles cujos *modus operandi* foi facilitado pelas novas tecnologias. Respectivamente, quanto à implementação de medidas processuais, em especial que facilitem a rápida preservação e a obtenção de provas digitais de delitos informáticos ou comuns,[49] são classificados pela doutrina majoritária como delitos digitais próprios ou puros e impróprios ou impuros.[50]

Nesse sentido, o artigo 14 dessa Convenção dispõe expressamente, como escopo, a adoção de medidas legislativas e outras providências necessárias a cada parte, para estabelecer os poderes e procedimentos que promovam investigações ou processos criminais. Além disso, prevê que tais poderes e procedimentos sejam aplicados não apenas aos crimes tipificados nos artigos 2 a 11, mas também a outros cometidos por meio de algum sistema de computador e à coleta de provas eletrônicas relacionadas à prática de crimes[51], abrangendo também provas digitais de delitos digitais impróprios ou impuros, como é o caso do HC 222.141/DF.

Relativamente à Convenção de Budapeste, um dos pontos centrais discutidos no acórdão desse processo é a preservação expedita de dados de computador, abordada em seu artigo 16. Esse artigo exige que os Estados signatários implementem medidas para garantir a preservação rápida de dados armazenados em sistemas de computador, a fim de assegurar que tais informações estejam disponíveis

---

[47] SOUZA, Wesley Wadim Passos Ferreira de. A Convenção de Budapeste e seus reflexos sobre a competência para o processo e julgamento dos crimes cibernéticos no Brasil. **Revista Judiciária Brasileira**. Especial Direito Digital, 2023, p. 39-68.

[48] DECRETO n. 11.491, de 19 de setembro de 2023.

[49] SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. A Convenção de Budapeste e as leis brasileiras. **Anais do 1° Seminário Cibercrime e Cooperação Penal Internacional**, 2009, p. 5. João Pessoa, maio de 2009. Disponível em: https://www.academia.edu/ Acesso em: 17 out. 2024.

[50] WENDT, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos:** ameaças e procedimentos de investigação.São Paulo: Editora Brasport, 2012, p. 65

[51] Convenção de Budapeste. Artigo 14 - Âmbito de aplicação dos dispositivos processuais. 1. Cada Parte adotará medidas legislativas e outras providências necessárias para estabelecer os poderes e procedimentos previstos nesta seção para o fim específico de promover investigações ou processos criminais. 2. Salvo se especificamente previsto no Artigo 21, cada Parte aplicará os poderes e procedimentos referidos no parágrafo 1 deste Artigo: a. aos crimes tipificados de acordo com os Artigos de 2 a 11 desta Convenção;
b. a outros crimes cometidos por meio de um sistema de computador; e c. para a coleta de provas eletrônicas da prática de um crime.

para investigações criminais. A preservação abrange tanto dados de conteúdo quanto dados de tráfego.[52]

> Artigo 16 - Preservação expedita de dados de computador
>
> 1. Cada Parte adotará medidas legislativas e outras providências necessárias para permitir que a autoridade competente ordene ou obtenha a expedita preservação de dados de computador especificados, incluindo dados de tráfego, que tenham sido armazenados por meio de um sistema de computador, especialmente quando haja razões para admitir que os dados de computador estão particularmente sujeitos a perda ou modificação.
>
> 2. Se a Parte der efeito ao parágrafo 1 acima por meio de uma ordem a uma pessoa para preservar dados de computador determinados que estejam sob sua posse, detenção ou controle, o Estado adotará medidas legislativas e outras providências necessárias para obrigar essa pessoa a preservar e manter a integridade desses dados de computador pelo período de tempo necessário, até o máximo de 90 (noventa) dias, a fim de permitir à autoridade competente buscar sua revelação. Qualquer Parte pode estipular que tal ordem possa ser renovada subsequentemente.
>
> 3. Cada Parte adotará medidas legislativas e outras providências necessárias para obrigar o detentor dos dados ou terceiro encarregado da sua preservação, a manter em sigilo o início do procedimento investigativo por um período de tempo estabelecido na sua legislação interna.
>
> 4. Os poderes e procedimentos referidos neste Artigo estão sujeitos aos Artigos 14 e 15.

Para melhor compreender o escopo da “preservação expedita”, referida no caput desse artigo, é necessário se fazer uma incursão nas definições de dados trazidas pelo mesmo regramento, o que já é aclarado em seu art. 1º, colacionado integralmente abaixo:

> Artigo 1º – Definições Para os efeitos desta Convenção:
>
> a “sistema informático” significa qualquer dispositivo ou grupo de dispositivos interligados ou relacionados, um ou mais dos quais, de acordo com um programa, efetuam processamento automático de dados;
>
> b “dados informáticos” significa qualquer representação de factos, informações ou conceitos numa forma adequada para processamento num sistema informático, incluindo um programa adequado para fazer com que um sistema informático desempenhe uma função;
>
> c “provedor de serviços” significa: eu qualquer entidade pública ou privada que proporcione aos utilizadores do seu serviço a capacidade de comunicar através de um sistema informático, e eu qualquer outra entidade que processe ou armazene dados informáticos em nome desse serviço de comunicação ou dos utilizadores desse serviço;
>
> d “dados de tráfego” significa quaisquer dados informáticos relativos a uma comunicação através de um sistema informático, gerados por um sistema informático que faz parte da cadeia de comunicação, indicando a origem, destino, rota, hora, data, tamanho, duração da comunicação ou tipo de serviço subjacente.

[52] ARAS, Vladimir. O congelamento de dados informáticos para fins de prova no processo. **Delictae Revista de Estudos Interdisciplinares sobre o Delito**, v. 8, n. 15, 2023. p. 182.

O tratado em estudo não esgota de maneira demasiadamente técnica[53] as classificações de dados. As definições trazidas são mais genéricas que as contidas no MCI. Principalmente o trecho destinado às definições legais é bem mais sucinto que o do regramento brasileiro; apenas traz as definições de dados informáticos e dados de tráfego. O termo “dados informáticos”, conforme sua denominação, abrange basicamente qualquer informação transitável por meio digital, independentemente do grau de sigilo. De acordo com o *Explanatory Report to the Convention on Cybercrime Budapest,* tais dados devem ser interpretados como qualquer dado eletrônico ou não que possa ser processado diretamente por um computador, com ou sem uso de programas específicos.[54]

No ordenamento brasileiro não há definição legal correspondente ao conceito referido.[55] Em uma interpretação comparativa desse dispositivo com as definições do MCI, pode-se dizer que dados informáticos compreendem, assim, dados cadastrais, registros de conexão e registros de acesso a aplicações, bem como dados de conteúdo, pois todas essas espécies, previstas no MCI, se adequam à definição genérica de “dados informáticos” da Convenção.

Os dados de tráfego, conforme conceituação quase literal da apresentada na Convenção, são aqueles que surgem da transmissão de mensagens pela rede, podendo demonstrar tempo, duração, formato de envio de mensagem e também a localização geográfica do equipamento utilizado pelo emitente e destinatário.[56]

Também não há, no MCI, definição que guarde relação perfeita com essa denominação. Contudo, possui muita semelhança com os conceitos de registros de conexão e registros de acesso a aplicações[57], que parecem ostentar maior detalhamento técnico. É que o primeiro diz respeito a metadados, isto é, pegadas

---

[53] SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. A Convenção de Budapeste e as leis brasileiras. **Anais do 1° Seminário Cibercrime e Cooperação Penal Internacional**, 2009, p. 5. João Pessoa, maio de 2009. Disponível em: https://www.academia.edu/ Acesso em: 17 out. 2024.

[54] COUNCIL OF EUROPE. **Explanatory report to the Convention on Cybercrime. Budapest,** 23 XI 2001. p. 5-6. Disponível em: https://rm.coe.int/16800cce5b. Acesso em: 17 out. 2024.

[55] BORTOT, J. F. Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. **Virtuajus**, v. 2, n. 2, p. 347, 8 ago. 2017.

[56] CORTEZ, Raphaela Jéssica Reinaldo. **Prova digital no processo penal brasileiro: o uso de dados de geolocalização na segurança pública e na investigação criminal**. Orientador: Walter Nunes da Silva Júnior. 2023. 104f. Dissertação (Mestrado em Direito) - Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2023.

[57] SMANIO, Gianluca Martins. A busca reversa por dados de localização na jurisprudência do Superior Tribunal de Justiça: análise crítica do RMS 61.302/RJ. **Revista Brasileira de Ciências Policiais,** v. 12, n. 5, p. 55-57, 2021.

digitais sobre a conexão, enquanto o segundo se refere às informações relativas ao acesso das funcionalidades hospedadas na rede.[58]

Embora não haja, no texto da Convenção de Budapeste, definição do termo “dados de conteúdo”, o respectivo Relatório Explicativo esclarece, em seu ponto 209, que ele se refere ao “conteúdo informativo da comunicação, ou seja, o significado ou o teor da comunicação, ou a mensagem ou informação veiculada pela comunicação (que não a relativa os dados de tráfego)”. Esse esclarecimento, contudo, é um tanto redundante e apenas diferencia esses dados da espécie “dados de tráfego” e não os exclui do amplo escopo abrangido pela denominação “dados informáticos”.

Feitas essas considerações conceituais, de fato, a conservação expedita de dados, prevista no artigo 16, de acordo com a própria Convenção, recai sobre todas as espécies de dados classificados na legislação brasileira, inclusive os dados de conteúdo, haja vista que estão abarcados nos temos “dados informáticos” e “dados de tráfego”. A divergência entre o escopo de incidência da conservação de dados do tratado e do MCI é notável, pois a denominação geral de “dados informáticos”, no qual estão também os dados de tráfego, citada no artigo 16 daquele, é realmente mais ampla que o dos registros de conexão e de acesso a aplicações, citados nos artigos 13 e 15 desse.

Há uma clara colisão entre os dispositivos legais mencionados. Diferentemente do MCI, que, conforme a interpretação legal e doutrinária, condiciona a conservação de dados a uma análise do seu grau de sensibilidade, a Convenção de Budapeste não impõe essa mesma exigência. Ao classificá-los, ela adota uma abordagem simplificada, agrupando todos os dados sob a denominação genérica de "dados informáticos". Não há, como no MCI, uma estrutura escalonada de proteção. Em vez disso, os dados são diferenciados apenas por aspectos técnicos, divididos em “dados de tráfego” e “dados de conteúdo”, sem levar em consideração o grau de interferência na intimidade e na privacidade.

Isso significa que, na Convenção de Budapeste, não há distinção quanto à natureza sensível dos dados, o que resulta na possibilidade de sua conservação de maneira única. No MCI, há diferentes níveis de proteção, conforme seu potencial de impacto na esfera privada do indivíduo.

---

[58] LEITE, George S.; LEMOS, Ronaldo. **Marco Civil da Internet**. Rio de Janeiro: Atlas, 2014. *E-book.* p.321-324. Disponível em: https://integrada.minhabiblioteca.com.br/ Acesso em: 17 out. 2024.

Essa discrepância é de importante para a conformação do congelamento extrajudicial de dados no Brasil, pois impacta diretamente os limites e garantias que devem ser observados nesse procedimento. Enquanto o MCI reflete preocupação com a proteção da intimidade e da privacidade, ancorada no princípio da autodeterminação informativa — que permite ao indivíduo controlar o uso de seus dados conforme sua sensibilidade —, a Convenção de Budapeste, ao adotar uma classificação simplificada de "dados informáticos", desconsidera a gradação de proteção baseada no impacto potencial sobre a esfera privada.

No âmbito penal, a autodeterminação informativa se consolida como um princípio integrador emergente, reconhecendo que a coleta e o uso de dados, especialmente em investigações, devem ser proporcionalmente equilibrados com a preservação de direitos fundamentais. A ausência de distinções mais detalhadas na Convenção de Budapeste, como as previstas no MCI, pode gerar uma aplicação indiscriminada e uniforme do congelamento de dados, ampliando os riscos de interferências desnecessárias na privacidade.

Portanto, a harmonização normativa entre os dispositivos legais é essencial para que o Brasil, ao aderir a instrumentos internacionais como a Convenção de Budapeste, assegure que o congelamento de dados respeite os preceitos constitucionais, como a proporcionalidade, a razoabilidade e a proteção à intimidade. Isso exige não apenas a adoção de limites claros e rigorosos, mas também a incorporação de critérios que reflitam a complexidade dos dados tratados, garantindo que práticas investigativas sejam compatíveis com a promoção da justiça sem violar direitos fundamentais.

2 A DECISÃO DO *HABEAS CORPUS* 222.141/DF E CORRENTES DIVERGENTES NA DOUTRINA E JURISPRUDÊNCIA

2.1 Decisões proferidas no caso: entendimentos no Superior Tribunal de Justiça e no Supremo Tribunal Federal

2.1.1 Julgamento prévio no Superior Tribunal de Justiça

Antes de chegar ao STF, o caso, HC n. 626.983/PR, foi julgado pela Sexta Turma do STJ, sob a relatoria do Ministro Olindo Menezes (Desembargador

Convocado do TRF 1ª Região), em 8/2/2022. O entendimento do Ministro relator foi diametralmente oposto ao adotado pela Suprema Corte posteriormente. No STJ, o voto condutor, de relatoria do Ministro Olindo Menezes, inicialmente destacou que a disciplina conferida pelos art. 13, § 2º e art. 15, § 2º do MCI permitia a medida cautelar consistente no congelamento extrajudicial de dados. Isso, porque “o ponto nodal da discussão, visto em face do direito à preservação da intimidade, da vida privada, da honra e da imagem das partes (CF- art. 5º, X, e Lei 12.965/2014 - art. 10)” restaria protegido, pois a preservação extrajudicial “não equivale a que o requerente tenha efetivo acesso aos dados "congelados" sem ordem judicial”. [59]

A decisão destacou que a devassa dos dados propriamente dita, conforme exigência do art. 13, § 4º,

> deverá ser precedida de autorização judicial, sendo estabelecido, inclusive, um prazo de 60 dias, contados a partir do requerimento de preservação dos dados, para que o Ministério Público ingresse com esse pedido de autorização judicial de acesso aos registros, sob pena de caducidade (pois a) simples guarda dos registros de acesso a aplicações de internet ou registros de conexão não viola o postulado constitucional do sigilo de informações eletrônicas, assim como também não ofende o princípio da jurisdicionalidade o fato de o provedor de aplicações de internet atender o pedido do Ministério Público, ainda que sem autorização judicial, haja vista que a disponibilização dos registros, esta sim deve ser por meio de autorização judicial, que deverá ser requerida no prazo legal após a guarda dos referidos registros.[60]

Ao analisar a decisão de primeira instância, justificou a medida e a validade das provas obtidas após o congelamento extrajudicial de dados no fato de que “os investigados podem trocar informações de cunho relevante ao deslinde da investigação em virtude da recente instauração de processo no Tribunal de Contas do Estado Paraná”. [61]

O voto condutor rebateu a argumentação da impetrante, de que a Arguição de Descumprimento do Preceito Fundamental (ADPF) 403/SE e a Ação Direta de Inconstitucionalidade (ADI) 5527/DF tratam da inconstitucionalidade de certos dispositivos da Lei 12.965/2014 (art. 13, §2°, e art. 15, § 2°, da Lei n. 12.965/2014 e o inciso II do art. 7º, e do inciso III do art. 12, da Lei 12.965/2014, respectivamente). Abordam a quebra de sigilo telemático sem autorização judicial e o acesso a conteúdos criptografados – temas não pertinentes ao presente caso, pois se refere ao acesso excepcional a mensagens criptografadas. Desse modo, as teses desse

---

59 SUPERIOR TRIBUNAL DE JUSTIÇA. **HC n. 626.983/PR**.
60 Ibid.
61 Ibid.

julgado não se aplicariam à discussão relativa ao congelamento extrajudicial de dados.[62]

Ao analisar quais dados foram preservados extrajudicialmente no caso, a decisão manteve seu posicionamento favorável à medida, afirmando que o pedido de preservação, feito pelo Ministério Público, incluiu *e-mails*, fotos e históricos de localização. Assim, considerou-se que esse pedido estava em conformidade com a legislação vigente.

Na decisão, rebateram-se os argumentos defensivos de que o conteúdo de *e-mail* e *iMessages*, fotos, contatos e históricos de localização não faziam parte do conceito de "registros de acesso a aplicações de internet" ou "registros de conexão", cuja preservação extrajudicial é permitida pelo MCI. Afirmou-se, simplesmente, que tais dados estariam inseridos no conceito legal do dispositivo referido.[63]

Para tanto, invocou-se um cotejo superficial das definições, afirmando que “o art. 5°, VIII define que "registros de acesso a aplicações de internet" são o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP". Já o inciso VII define que "aplicações de internet" são o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet.”[64]

Entendeu-se, na decisão, que a alegação de nulidade arguida seria relativa, portanto, deveria ser acompanhada da demonstração de prejuízo. Assim, a decisão concluiu que “não se perfaz a pretendida nulidade do pedido de 'congelamento' dos registros, além do tempo legal, pelo Ministério Público do Estado do Paraná” e que o acesso aos dados foi deferido com a devida ordem judicial. Manteve-se a decisão de primeira instância, pois a preservação extrajudicial dos dados e a subsequente autorização judicial para acesso estariam em conformidade com a lei.[65]

Embora o Ministro Sebastião Reis não tenha divergido do entendimento esposado no voto condutor, proferiu voto-vista no qual acrescentou que a decisão devia considerar o poder geral de cautela dos órgãos de persecução penal e o poder de requisição do Ministério Público. Ele reiterou que, embora a requisição de

---

[62] Ibid.
[63] Ibid.
[64] Ibid.
[65] Ibid.

preservação de dados fosse permitida sem autorização judicial, o acesso ao conteúdo dessas informações requeria ordem judicial.[66]

Sebastião Reis Júnior defendeu que “é patente, e isso foi respeitado no caso, que a devassa sobre o conteúdo depende de autorização judicial”, referindo-se à requisição ministerial de “preservação do conteúdo das seguintes informações: histórico de pesquisa, todo o conteúdo de *e-mail* e *iMessages*, fotos, contatos e históricos de localização”. Ele comparou a situação à apreensão de um celular, onde a guarda do dispositivo é permitida, mas o acesso ao conteúdo só pode ocorrer com autorização judicial.

O Ministro concluiu que o “direito em tensão”, que poderia ser invocado no caso, seria o de excluir definitivamente os dados, “prerrogativa, prevista no art. 7º, X do Marco Civil da internet, tem, como limite, justamente as hipóteses de guarda obrigatória de registros previstas nesta Lei.”[67]

Os Ministros Laurita Vaz, Sebastião Reis Júnior, Rogério Schietti Cruz e Antonio Saldanha Palheiro votaram com o Ministro Relator, sendo, portanto, unânime a denegação do *Habeas Corpus*. Foram declaradas válidas as provas obtidas após o congelamento extrajudicial de dados, ainda que a medida houvesse incidido sobre dados de conteúdo.

2.1.2 Votos e divergências na 2ª Turma do Supremo Tribunal Federal

Ao se manifestarem sobre o caso, o Ministério Público Estadual e o Federal aduziram que a preservação de dados foi realizada de acordo com o artigo 13 do MCI, pois solicitou-se à Apple e ao Google a preservação dos dados da investigada. Posteriormente, ingressou-se com pedido de quebra do sigilo desses dados, obtendo-se autorização judicial para devassa do conteúdo previamente conservado.[68]

Ambos os Ministérios destacaram que o objetivo não era requisitar aos provedores da internet a indisponibilidade de dados sem autorização judicial, mas sim, gerar um dever de preservação dos dados para os provedores, a fim de proteger elementos de prova indispensáveis à comprovação dos crimes. Alegram ainda que

---

[66] SUPREMO TRIBUNAL FEDERAL. **Habeas Corpu**s n. 222.141/DF.
[67] Ibid.
[68] Ibid.

não houve violação à legislação aplicável, à inviolabilidade do sigilo das comunicações ou ao direito à privacidade.[69]

Enfatizaram também sobre a inaplicabilidade da LGPD ao processo penal, conforme seu artigo 4º, III, d. Dessa forma, sustentaram que não deveria ser reconhecida a nulidade dos elementos de prova obtidos em desfavor da paciente, a partir do congelamento prévio requisitado pelo Ministério Público; não houve violação à legislação, e o acesso aos dados ocorreu mediante autorização judicial.[70]

O Ministro Ricardo Lewandowski, relator do caso, proferiu voto no qual considerou ser a diligência extrajudicial incompatível com a legislação e inadmissível, quando confrontada com as garantias fundamentais. Afirmou que essa ação violou direitos individuais da parte investigada, extrapolando os limites legais estabelecidos. Para embasar sua posição, destacou a importância do MCI e da LGPD como referências legais que estabelecem salvaguardas para a privacidade e o acesso a dados telemáticos. Destacou também que qualquer acesso a esses dados deveria ser realizado dentro dos parâmetros legais, mediante autorização judicial. De acordo com o voto, o texto legal é claro, ao permitir que autoridades policiais ou administrativas, incluindo o Ministério Público, solicitem cautelarmente a preservação dos registros de conexão, mas apenas com autorização judicial para acesso em um prazo determinado. Essa ênfase na necessidade de autorização judicial, nos termos do voto, reflete a importância da reserva de jurisdição na proteção dos direitos individuais.[71]

Além disso, o Ministro Ricardo Lewandowski argumentou que a submissão da medida, requerida pelo Ministério Público, à prévia autorização judicial não entrava em conflito com a Convenção de Budapeste, destacando a necessidade de respeitar as garantias constitucionais mesmo em contextos de cooperação internacional.[72] Em seu voto, destacou que o MCI permite a preservação de registros de conexão por parte das autoridades administrativas, mas veda qualquer acesso a dados privados sem autorização judicial prévia:

> O que se afirma nesta seara diz respeito a um procedimento ofensivo às balizas legais, para além do que é autorizado, por mais tempo do que se determina. [...] Não há dúvidas de que o congelamento de dados telemáticos violou, por diversas formas, uma gama de direitos individuais da paciente, ao

[69] Ibid.
[70] Ibid.
[71] Ibid.
[72] Ibid.

> retirar-lhe o controle sobre informações pessoais, mesmo sem qualquer decisão judicial impondo essa proibição.[73]

Ainda, o voto do Ministro Lewandowski determinou não apenas a exclusão das provas ilícitas dos autos, mas também a reavaliação da justa causa para prosseguimento da ação penal e a extensão da decisão a outros envolvidos no caso. Essas medidas, de acordo com o voto, seriam fundamentais para garantir a conformidade com a legislação e proteger os direitos fundamentais dos indivíduos envolvidos no processo.[74]

O Ministro Gilmar Mendes acompanhou o relator, adicionando que o congelamento de dados retira do titular o direito de gestão sobre eles, o que feria o direito à autodeterminação informacional do titular das informações congeladas de maneira extrajudicial. Gilmar Mendes reforçou que o acesso a dados como histórico de localização, mensagens e outros conteúdos é inadmissível sem autorização judicial expressa, destacando que a medida adotada neste caso não respeitou a proporcionalidade exigida para ações dessa natureza. O Ministro entendeu que as informações solicitadas pelo Parquet extravasavam o conceito de “dados de conexão”, cujo congelamento é autorizado pelo MCI, de modo que a medida realizada foi ilícita e as provas, consequentemente, nulas.[75]

Já em seu voto, o Ministro André Mendonça enfatizou o princípio da presunção de inocência, ressaltando que este era um pilar fundamental do direito penal, no qual o réu deveria ser considerado inocente até que sua culpa fosse comprovada de forma irrefutável.[76]

Além disso, o Ministro defendeu a necessidade de uma análise criteriosa dos requisitos legais para a concessão de *habeas corpus*, especialmente em casos envolvendo crimes graves. Destacou a gravidade do crime em questão como um fator relevante a ser considerado na tomada de decisão, argumentando que a manutenção da prisão preventiva poderia ser necessária para garantir a ordem pública e para prevenir a prática de novos delitos, medida que se equipararia ao congelamento extrajudicial de dados.[77]

O Ministro também enfatizou a importância de proteger a sociedade contra indivíduos que representam um potencial perigo, especialmente quando há evidências

---

[73] Ibid.
[74] Ibid.
[75] Ibid.
[76] Ibid.
[77] Ibid.

de envolvimento em crimes graves. Nesse sentido, ressaltou a necessidade de se levar em conta não apenas os direitos individuais do acusado, mas também o bem-estar coletivo, posicionando-se favorável ao congelamento extrajudicial de dados realizado no caso.[78]

O Ministro André Mendonça destacou que a determinação judicial para acesso aos dados ocorreu em novembro de 2019 e em janeiro de 2020, por meio de ofícios requisitórios. No entanto, os dados já estavam sob guarda dos provedores há mais de um ano, o que levantava dúvidas sobre o cumprimento da exigência legal de manter os dados por um período mínimo, como estabelecido no MCI. Além disso, afirmou que a preservação dos dados não ocorreu unicamente por força da requisição do Ministério Público, mas também por uma política de prazo dilatado adotada pelos provedores e pela decisão judicial. Essa observação sugeria que os provedores já estavam em guarda das informações mesmo antes da requisição, o que tornava questionável a alegação de que a preservação se deu apenas em resposta ao pedido do Ministério Público. [79]

O Ministro ponderou, ainda, que não havia evidências de que o pedido de preservação tinha interferido no conteúdo das informações disponibilizadas como prova; isso era crucial para a análise da legalidade das provas obtidas, pois a falta de nexo causal podia invalidar a alegação de ilicitude das mesmas. Em suma, como dito, o Ministro André Mendonça foi favorável à aplicação da medida realizada no HC 222.141/DF.[80]

O Ministro Edson Fachin também votou de forma divergente, afirmando que medidas cautelares de preservação de dados são permitidas em situações de urgência, desde que acompanhadas de posterior autorização judicial. Destacou que o MCI prevê a possibilidade de autoridades administrativas requisitarem a preservação de registros de conexão sem autorização judicial inicial, desde que o acesso ao conteúdo seja submetido ao crivo judicial em prazo hábil.[81]

Por fim, no voto vogal, o Ministro Fachin explicou que, conforme o artigo 13 do MCI, os registros de conexão de internet devem ser mantidos sob sigilo por um ano, com possibilidade de prorrogação do prazo mediante autorização judicial. No

[78] Ibid.
[79] Ibid.
[80] Ibid.
[81] Ibid.

caso analisado, o Ministério Público requereu a preservação dos dados, mas a solicitação ultrapassou o período de um ano, abrangendo registros desde junho de 2017 até o momento do pedido, o que ele considerou ilegal.[82]

O Ministro Fachin votou no sentido de que qualquer acesso a dados conservados antes de 3 de dezembro de 2018 fosse anulado, por ultrapassar o prazo de um ano estabelecido pela lei. Além disso, esclareceu que o Ministério Público não tem autorização para solicitar a preservação de dados pessoais ou de comunicações privadas sem autorização judicial, como previsto pela legislação. O voto seguiu o entendimento do Ministro relator, limitando a validade do congelamento extrajudicial aos dados que se enquadravam nos "registros de conexão" e excluindo conteúdos que não se encaixavam nessa definição (*e-mails,* fotos e históricos de localização).[83]

2.2 Vieses doutrinários favoráveis ao amplo congelamento extrajudicial da dados

Como foi demonstrado, a possibilidade de realizar o congelamento extrajudicial de dados de forma ampla goza de algum apelo doutrinário. Por isso, vale esclarecer qual é a tese preconizada no trabalho que critica a decisão proferida no HC 222.141/DF (único localizado nesta pesquisa), defendendo maior flexibilidade ao instituto referido, de autoria do professor e Procurador Regional da República em Brasília, Vladimir Aras.[84] Ele reconhece que o ordenamento brasileiro segue uma lógica de proteção escalonada dos dados e explica o nível de proteção de cada um dos dados, com base nos dispositivos legais aplicáveis.

Segundo o autor, os dados pessoais podem ser divididos em três categorias principais: cadastrais, de conexão e de conteúdo, cada uma com diferentes graus de proteção. Os dados cadastrais, definidos pelo art. 11 do Decreto 8.771/2016 e pelo art. 5º, VII do MCI possuem proteção mínima e podem ser requisitados diretamente pelo Ministério Público ou pela Polícia, sem necessidade de autorização judicial. Já os dados de conexão e de acesso a aplicações de internet, como previsto no art. 7º, incisos II e III, e nos arts. 13 e 15 do MCI, demandam prévia autorização judicial, devido à maior ingerência que representam na privacidade do indivíduo. O autor confirma que os dados de conteúdo, dotados de maior sensibilidade, estão

---

[82] Ibid.
[83] Ibid.
[84] ARAS, Vladimir. O congelamento de dados informáticos para fins de prova no processo. **Delictae Revista de Estudos Interdisciplinares sobre o Delito**, v. 8, n. 15, 2023. p. 180-223.

protegidos pelo art. 5º, inciso XII da Constituição Federal, e sua obtenção somente é permitida mediante autorização judicial específica, conforme a Lei 9.296/1996.[85]

A tese defendida por Aras, que se posiciona contrário à decisão do STF, é bem similar aos argumentos trazidos pelo MPF no caso do HC 222.141/DF, pode ser dividida em três ideias centrais: i) a precautelaridade da medida, que não se confunde com o acesso propriamente dito do dados; ii) a ampliação da medida pela Convenção de Budapeste, de modo que, em respeito à ratificação do tratado, as disposições restritivas do MCI deveriam ser consideradas superadas; iii) a necessidade da flexibilização em prol da celeridade investigativa, haja vista que crimes graves, com possibilidades de elucidação por meio de provas digitais, cujo perecimento é rápido, legitimam a aplicação da medida mesmo para dados de conteúdo.

Inicialmente, Aras destaca que o intuito da medida do congelamento não é alijar o titular da possibilidade de fazer uso de seus dados afetados por este instituto, tampouco vedar o acesso deles ao usuário que está sendo investigado.[86] Em verdade, ao ser requerido pelo MP ou pela autoridade policial, o instituto tem como fito impedir o descarte/destruição dos dados. É medida evidentemente acautelatória, que não constitui, segundo essa posição doutrinária, qualquer violação à legislação vigente.[87]

Conforme lição de Aras, a medida deve ser entendida à luz dos apontamentos da Lei 9.296/1996, a qual tem como intuito regular o inciso XII, parte final, do art. 5° da Constituição Federal, que institui em partes a inviolabilidade das comunicações privadas.[88] Isso porque, dentro dessa ótica, o acesso efetivo às informações dessa estirpe é viabilizado pela técnica de interceptação de telecomunicação. Assim sendo, constitui técnica especial de investigação ou, noutras palavras, meio especial de obtenção de provas, conforme preconiza o art. 3° da Lei 8.250/2013, e não se confundiria com o congelamento extrajudicial de dados. Esse não objetiva obtenção de provas, mas consistiria em uma medida precautelar para conservá-las, diante da facilidade de destruição das evidências digitais.

O autor ressalta que a natureza de medida precautelar é fundamental para compreender a prescindibilidade de decisão judicial. É que, enquanto a obtenção dos registros armazenados, por meio da interceptação telefônica, efetivamente esbarra na

---

[85] Ibid., p. 5 – 8.
[86] Ibid.
[87] Ibid., p.19 – 30.
[88] Ibid.

relativização da privacidade e, por essa razão, exige ordem judicial, o mesmo não se verificaria na medida precautelar de congelamento de dados.[89]

Além disso, de acordo com Aras, em que pese a proteção aos dados pessoais ser um direito assegurado no art. 5°, LXXIX da Constituição Federal, a medida precautelar de seu congelamento extrajudicial não desrespeita a LGPD, a qual assevera, em seu art. 4°, inc. III, alínea d, que o diploma não se aplica a fins exclusivo de atividades de investigação e de repressão de infrações penais.[90]

Ao se considerar que a autodeterminação informativa é um direito garantido de forma mais explícita pela LGPD – que traz eficácia no plano concreto ao art. 5°, inc. LXXIX da Constituição Federal e que afasta expressamente à aplicabilidade do diploma nas situações em que o congelamento extrajudicial de dados é aplicado –, parece que a utilização desse critério para balizar a tese da necessidade de requisição judicial para viabilizar o congelamento dos dados é equivocada.

De mais a mais, o autor menciona que, diferentemente do congelamento extrajudicial de dados, regulado sistematicamente pelos arts. 7º,10,13,15 e 22 do MCI, o acesso aos dados armazenados por meio de apreensão de dispositivos de memória, por representar devassa efetiva das informações, exige autorização judicial. Ele traz como exemplo o que foi decidido pelo STJ, no AgRg no HC 709.810/SP:

> 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.

Aras reconhece que, na sistemática brasileira, qualquer flexibilização de direitos constitucionalmente previstos atrai imprescindível reserva de jurisdição. Entretanto, sobram exemplos que demonstram, de forma cristalina, que nem todas as medidas cautelares estão abarcadas pela reserva de jurisdição. Faz, assim, menção aos arts. 301[91] e 304[92] do Código de Processo Penal (CPP), que versam sobre a

---

[89] Ibid.
[90] Ibid.
[91] CÓDIGO DE PROCESSO PENAL. Art. 301. Qualquer do povo poderá e as autoridades policiais e seus agentes deverão prender quem quer que seja encontrado em flagrante delito.
[92] CÓDIGO DE PROCESSO PENAL. Art. 304. Apresentado o preso à autoridade competente, ouvirá esta o condutor e colherá, desde logo, sua assinatura, entregando a este cópia do termo e recibo de entrega do preso. Em seguida, procederá à oitiva das testemunhas que o acompanharem e ao interrogatório do acusado sobre a imputação que lhe é feita, colhendo, após cada oitiva suas respectivas assinaturas, lavrando, a autoridade, afinal, o auto. (Redação dada pela Lei nº 11.113, de 2005) § 1o Resultando das respostas fundada a suspeita contra o conduzido, a autoridade mandará

prisão e a autuação em flagrante delito, ao arbitramento de fiança pelo delegado de polícia, nos termos do art. 322,[93] e às medidas preventivas de urgência do afastamento do agressor do lar, previstas pela Lei nº 11.340/2006, Lei Maria da Penha[94] (art.12-C, incisos II e III) e da Lei nº14.344/2022, Lei Henry do Borel[95] (art.14, incisos II e III).

Dessa forma, ele compara o congelamento extrajudicial de dados com um desses exemplos que não está inserido no rol da reserva de jurisdição. Todavia, o autor observa que tal instituto, assim como os demais, está sujeito à possibilidade de revisão judicial posterior pelo Juízo competente, tratando-se de medida evidentemente precautelar que não exige crivo judicial pela própria natureza urgente da medida. [96]

Para reforçar este argumento, Aras preconiza que o CPP, em seu art. 6°, trata de forma expressa a necessidade de o delegado preservar a cena do crime e os objetos que tiverem relação com o fato até a chegada dos peritos criminais. [97] O

---

recolhê-lo à prisão, exceto no caso de livrar-se solto ou de prestar fiança, e prosseguirá nos atos do inquérito ou processo, se para isso for competente; se não o for, enviará os autos à autoridade que o seja. § 2o A falta de testemunhas da infração não impedirá o auto de prisão em flagrante; mas, nesse caso, com o condutor, deverão assiná-lo pelo menos duas pessoas que hajam testemunhado a apresentação do preso à autoridade. § 3o Quando o acusado se recusar a assinar, não souber ou não puder fazê-lo, o auto de prisão em flagrante será assinado por duas testemunhas, que tenham ouvido sua leitura na presença deste. (Redação dada pela Lei nº 11.113, de 2005) § 4o Da lavratura do auto de prisão em flagrante deverá constar a informação sobre a existência de filhos, respectivas idades e se possuem alguma deficiência e o nome e o contato de eventual responsável pelos cuidados dos filhos, indicado pela pessoa presa. (Incluído pela Lei nº 13.257, de 2016)

[93] CÓDIGO DE PROCESSO PENAL Art. 322. A autoridade policial somente poderá conceder fiança nos casos de infração cuja pena privativa de liberdade máxima não seja superior a 4 (quatro) anos. (Redação dada pela Lei nº 12.403, de 2011). Parágrafo único. Nos demais casos, a fiança será requerida ao juiz, que decidirá em 48 (quarenta e oito) horas. (Redação dada pela Lei nº 12.403, de 2011).

[94] Lei nº 11.340/2006. Art. 12-C. Verificada a existência de risco atual ou iminente à vida ou à integridade física ou psicológica da mulher em situação de violência doméstica e familiar, ou de seus dependentes, o agressor será imediatamente afastado do lar, domicílio ou local de convivência com a ofendida: (Redação dada pela Lei nº 14.188, de 2021) II - pelo delegado de polícia, quando o Município não for sede de comarca; ou (Incluído pela Lei nº 13.827, de 2019). II - pelo policial, quando o Município não for sede de comarca e não houver delegado disponível no momento da denúncia

[95] Lei nº14.344/2022. Art. 14. Verificada a ocorrência de ação ou omissão que implique a ameaça ou a prática de violência doméstica e familiar, com a existência de risco atual ou iminente à vida ou à integridade física da criança e do adolescente, ou de seus familiares, o agressor será imediatamente afastado do lar, do domicílio ou do local de convivência com a vítima: II - pelo delegado de polícia, quando o Município não for sede de comarca; III - pelo policial, quando o Município não for sede de comarca e não houver delegado disponível no momento da denúncia.

[96] ARAS, Vladimir. O congelamento de dados informáticos para fins de prova no processo. **Delictae Revista de Estudos Interdisciplinares sobre o Delito**, v. 8, n. 15, 2023. p. 20.

[97] CÓDIGO DE PROCESSO PENAL. Art. 6° Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá: I - dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais; (Redação dada pela Lei nº 8.862, de 28.3.1994)II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais; (Redação dada pela Lei nº 8.862, de 28.3.1994)III - colher todas as provas que servirem

objetivo primário da medida é evitar o perecimento de evidências digitais, dada a fragilidade e a efemeridade desses dados, sem implicar violação imediata da privacidade. O congelamento tem caráter preparatório, resguardando a possibilidade de acesso futuro, desde que devidamente autorizado judicialmente.[98] Nesse sentido, a medida do congelamento dos dados de forma extrajudicial estaria na esteira do "espírito" desse Código e do sistema processual como um todo.

Para o autor, tal distinção é essencial, pois, enquanto o acesso aos dados demanda decisão judicial em virtude da reserva de jurisdição, a precautelaridade permite a preservação administrativa de dados como uma medida excepcional e urgente, aplicada a situações de risco iminente de sua destruição.

Aras também enfatiza que, durante o período de preservação, o titular dos dados não perde o controle sobre eles, mantendo a possibilidade de exercer seus direitos de informação, de acesso, de oposição, de retificação e de apagamento, ainda que de forma diferida, em conformidade com a Súmula Vinculante 14 do STF.[99] Isso asseguraria o direito à autodeterminação informacional do titular, pois ele não perderia o direito de gerir livremente seus dados.

Outro ponto abordado por Aras é a importância da preservação de dados para obtenção de provas digitais. Devido à intangibilidade, à facilidade de destruição e à rápida transferibilidade, o congelamento de dados é crucial para garantir que essas informações não sejam descartadas, alteradas ou apagadas.[100] Esse processo permitiria a coleta de provas substanciais e fundamentais para o sucesso das investigações criminais

Nesse contexto, Aras ressalta que o congelamento não constitui, por si só, uma invasão de privacidade, uma vez que não implica análise, coleta ou manipulação

---

para o esclarecimento do fato e suas circunstâncias; IV - ouvir o ofendido; V - ouvir o indiciado, com observância, no que for aplicável, do disposto no Capítulo III do Título Vll, deste Livro, devendo o respectivo termo ser assinado por duas testemunhas que Ihe tenham ouvido a leitura; VI - proceder a reconhecimento de pessoas e coisas e a acareações; VII - determinar, se for caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias; VIII - ordenar a identificação do indiciado pelo processo datiloscópico, se possível, e fazer juntar aos autos sua folha de antecedentes;I X - averiguar a vida pregressa do indiciado, sob o ponto de vista individual, familiar e social, sua condição econômica, sua atitude e estado de ânimo antes e depois do crime e durante ele, e quaisquer outros elementos que contribuírem para a apreciação do seu temperamento e caráter. X - colher informações sobre a existência de filhos, respectivas idades e se possuem alguma deficiência e o nome e o contato de eventual responsável pelos cuidados dos filhos, indicado pela pessoa presa. (Incluído pela Lei nº 13.257, de 2016)

[98] ARAS, Vladimir. O congelamento de dados informáticos para fins de prova no processo. **Delictae Revista de Estudos Interdisciplinares sobre o Delito**, v. 8, n. 15, 2023. p. 19 – 30.

[99] Ibid.

[100] Ibid.

dos dados preservados. A medida busca, apenas, garantir que as informações digitais permaneçam íntegras e disponíveis para eventual uso futuro, caso uma decisão judicial autorize seu acesso. A justificativa está na natureza transitória e altamente volátil dos dados digitais, que podem ser facilmente apagados ou alterados, especialmente em casos de crimes cibernéticos, onde a rapidez na preservação é crucial para evitar a perda de provas essenciais. Diante disso, a preservação precautelar é compatível com os princípios constitucionais de proteção à privacidade, uma vez que não há acesso imediato aos dados sem autorização judicial. ref

A Convenção de Budapeste trouxe o tratamento de crimes cibernéticos, ampliando as possibilidades de preservação de provas digitais por meio do mecanismo denominado “conservação expedita”, previsto no artigo 16. Com a incorporação desse tratado, ocorrida no fim de 2023, suas disposições se sobrepõem aos dispositivos do MCI.[101]

A extrajudicialidade da medida é fundamental para alcançar o intuito da norma internacional, já que se preza pela rapidez da conservação dos dados. O referido artigo 16 permite que autoridades investigativas solicitem a preservação de dados de tráfego, de acesso e de conteúdo por até 90 dias, prorrogáveis, com o objetivo de evitar o perecimento de informações essenciais antes de uma autorização judicial formal.[102]

Aras argumenta que essa previsão atende à volatilidade característica dos dados digitais e à urgência que situações de cibercriminalidade exigem. Esse dispositivo da Convenção de Budapeste pode ser invocado pela Polícia Judiciária e pelo Ministério Público para solicitar a conservação expedita de todos os dados de computador ali definidos, os quais incluem dados de conteúdo. de modo que os arts. 13 e 15 do MCI servirão apenas para aplicação analógica, estabelecendo o prazo máximo de sessenta dias para a hipótese de congelamento de dados de conteúdo.[103]

Aras ressalta que qualquer intervenção estatal na privacidade, em uma sociedade democrática, exige previsão legal, justificativa do interesse público e necessidade, conforme os critérios do Tribunal Europeu de Direitos Humanos. Assim,

[101] Ibid. p, 30 – 36.
[102] Ibid.
[103] Ibid.

apesar da aplicação imediata da Convenção, ainda é exigida uma lei específica para sua completa implementação, dado o déficit legislativo.[104]

Contudo, após leitura atenta aos argumentos de Aras, vê-se que ele se alinha ao entendimento do STJ, sendo clara sua posição, ao defender que o congelamento extrajudicial de dados é uma prática essencial para assegurar a efetividade da persecução penal e a integridade das provas digitais. Explica que a medida mantém incólume o equilíbrio necessário entre a proteção da privacidade e a segurança pública.

[104] Ibid. p. 38.

3 SEGURANÇA JURÍDICA E PERSECUÇÃO PENAL EFETIVA: LIMITES E REFLEXÕES SOBRE O CONGELAMENTO EXTRAJUDICIAL DE DADOS NO BRASIL

3.1 Direito à privacidade e "mera preservação" de dados: os novos contornos trazidos pelo princípio da autodeterminação informativa

Conforme exposto no capítulo anterior, um dos argumentos primordiais empregado pela doutrina favorável ao amplo congelamento extrajudicial de dados, isto é, todas as espécies de dados, inclusive as comunicações privadas, consiste na diferença entre o acesso efetivo aos dados em contraposição ao mero congelamento das informações, sendo esta última menos gravosa que a primeira.[105]

As garantias constitucionais de proteção à intimidade e à vida privada foram inicialmente concebidas para resguardar o sigilo de correspondências e as comunicações telefônicas contra acessos não autorizados; visavam prevenir abusos, especialmente de parte do Estado. Vale lembrar que, quando esses dispositivos foram elaborados, comunicações instantâneas ainda não existiam, e a proteção legal foi explicitamente direcionada ao "sigilo da correspondência e das comunicações telegráficas, de dados e telefônicas"[106], cuja dinâmica é totalmente diferente das comunicações instantâneas mais recentes.

As comunicações analógicas, como cartas e especialmente telefonemas, se desvaneciam após o uso, deixando poucos ou nenhum registro duradouro. No caso das correspondências físicas, seu acesso dependia da interceptação do próprio documento, restringindo significativamente as possibilidades de monitoramento. [107]

Em contraste, correspondências eletrônicas são instantâneas, amplamente acessíveis e permitem um monitoramento constante, com mensagens, metadados e arquivos armazenados permanentemente em servidores e acessíveis a qualquer momento. Essa permanência transforma a dinâmica da privacidade, pois os dados

---

[105] ARAS, Vladimir. O congelamento de dados informáticos para fins de prova no processo. **Delictae Revista de Estudos Interdisciplinares sobre o Delito**, v. 8, n. 15, 2023. p. 182.

[106] CONSTITUIÇÃO FEDERAL. Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

[107] COELHO, Luiza Tângari. A proteção da intimidade na correspondência eletrônica: extensão da tutela da correspondência tradicional. **Revista da Faculdade de Direito da UFMG**, Belo Horizonte, v. 61, p. 365-369, 2012.

digitais ficam sujeitos a uma vigilância retrospectiva e a uma análise em larga escala, o que não é possível em meios analógicos as comunicações telefônicas.

Além disso, as comunicações digitais geram um volume de metadados (como localização e duração) “altamente” reveladores e úteis em investigações, mas que podem comprometer a privacidade individual.[108]

Essa realidade complexa, muito além do que as proteções originais previam, exige uma adaptação das interpretações legais para proteger efetivamente os direitos fundamentais na era digital. É necessária uma transição jurídica que amplie a proteção à privacidade do contexto analógico para o digital.[109] Essa transição deve perpassar a absorção de conceitos capazes de explicar a nova dimensão dos princípios basilares da privacidade e da dignidade da pessoa humana na vida digital/virtual, cada vez mais integrada e transformadora da “vida real”/realidade material. É dizer que são necessários novos elementos jurídicos específicos, capazes de materializar esses direitos constitucionais, ainda que pela criação de bens e metaprincípios com base em interpretações que melhor contemplem a pós-modernidade.[110]

Embora não seja um conceito novo, a autodeterminação informativa, mencionada na decisão do HC 222.141/DF, esclarece satisfatoriamente o estreito caminho da proteção de garantias constitucionais em meio à realidade digital. Na decisão em análise, a autodeterminação informativa, em articulação com as interpretações dos dispositivos do MCI e da Convenção de Budapeste, desponta como um elemento central para integração e harmonização da interpretação dos dispositivos legais aplicáveis à controvérsia.

A autodeterminação informativa (*informationelle selbstbestimmung*) é um conceito jurídico que se refere ao direito do indivíduo de controlar a divulgação e o uso de seus dados pessoais. O conceito surgiu do paradigmático caso BVerfGE 65, 1

---

[108] SILVA, Gabriela Buarque Pereira; MOURA, Tâmara. Prisão em flagrante e acesso a dados de celular: desafios entre a privacidade e a investigação criminal. In: In: ARAS, Vladimir B.; MENDONÇA, Andrey B.; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno F. da; COSTA, Marcos Antônio da S. (Org.) **Proteção de Dados Pessoais e Investigação Criminal**. Ministério Público Federal. Brasília: ANPR, 2020, p.400.

[109] SOLOVE, Daniel J. **Nothing to hide**: the false tradeoff between privacy and security. London: Yale University Press, 2011. p. 8.

[110] Para melhor compreensão da complexidade social na sociedade em rede, ver CASTELLS, Manuel. A sociedade em rede. 6 ed. Tradução Roneide Venancio M. São Paulo: Paz e Terra, 1999, p. 124 e ss.

– 71 (Recenseamento), julgado pelo Tribunal Constitucional Alemão de 1983[111], e, desde então, foi amplamente desenvolvido pela jurisprudência.

Muito a propósito, conforme reflete a professora Laura Schertel Mendes acerca do julgado alemão, uma das preocupações que levou à formulação do princípio referido foi justamente resguardar o exercício da personalidade, frente ao avanço da tecnologia,[112] como se verá adiante. A provocação se deu a partir de diversas reclamações constitucionais,[113] ajuizadas por grupos de cidadãos que contestavam a Lei Federal de Recenseamento Alemã, editada em 1982 e aprovada por unanimidade, tanto pelo Parlamento quanto pelo Conselho Federal.[114]

Essa lei estabelecia que, em 1983, seria realizado um censo por funcionários públicos e demais agentes encarregados, cujo escopo não se limitava a contar o número de habitantes do país, mas incluía a coleta de vários dados pessoais dos cidadãos: nome completo, endereço, número de telefone, idade, sexo, data de nascimento, estado civil, nacionalidade, religião, uso da moradia como domicílio ou residência, fonte principal de sustento, ocupação profissional, formação profissional e duração, formação escolar, eventual formação técnico-profissionalizante, endereço profissional ou do local de estudos, informações sobre os ramos de atuação do empregador, função desempenhada no emprego e meio de locomoção utilizado para o trabalho ou estudo. E para alcançar melhor qualificação das informações relativas à população, a Lei do Censo Alemã permitia o cruzamento de informações sobre cidadãos, ainda que para fins estatísticos, sem o consentimento deles, já que o recolhimento das informações era obrigatório.[115]

Em sede de liminar, o Tribunal Constitucional Federal suspendeu os efeitos dessa Lei, solicitando uma análise mais aprofundada de sua constitucionalidade. No julgamento final, a Corte declarou parcialmente procedentes as reclamações constitucionais e determinou a continuidade do censo, porém, com significativas alterações para garantir a proteção aos dados pessoais dos cidadãos. Entre as medidas impostas, destacou-se a proibição da transferência de dados como nome e

---

[111] BVerfGE 209/83.
[112] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Pensar Revista de Ciências Júridicas Universidade de Fortaleza (Unifor),** v. 25, n. 4. Fortaleza, 2020. p.11.
[113] BvR 209/83,1 BvR 269/83,1 BVR 362/83, 1 BVR 420/83,1 BVR 440/83, e1 BVR 484/83.
[114] BVerfGE 209/83, BVerfGE 65, 1 (2)
[115] BVerfGE 65, 1 (47).

endereço para outros órgãos governamentais, com o objetivo de resguardar a autodeterminação informativa dos cidadãos.[116]

A decisão resultou da hermenêutica combinada dos artigos 1.1 e 2.1 da *Grundgesetz für die Bundesrepublik Deutschland,* a Lei Fundamental da República Federal da Alemanha, desenvolvendo-se, a partir desses dispositivos, o direito fundamental à autodeterminação informativa, a partir do direito geral à personalidade e à dignidade humana.

Os artigos 1.1 e 2.1 da Lei Fundamental da República Federal da Alemanha dispõem o seguinte[117]:

> 1.1 A dignidade humana é inviolável. Respeitá-los e protegê-los é obrigação de todas as autoridades estatais.
> 2.1 Toda pessoa tem direito ao livre desenvolvimento da sua personalidade, desde que não violem os direitos dos outros e não violem a ordem constitucional ou a lei moral.

Na oportunidade, o Tribunal assentou que, especialmente nas condições do processamento moderno de dados, a proteção do indivíduo contra coleta, armazenamento, uso e divulgação ilimitados de seus dados pessoais é garantida pelo direito fundamental, contida nos artigos acima referidos, para resguardar o direito do indivíduo de decidir por si próprio sobre a divulgação e a utilização dos seus dados pessoais.[118]

É valido destacar que a preocupação foi adiantada nos idos da década de 80 (séc. XX), quando a maioria das tecnologias da informação hoje vigentes sequer eram imaginadas ou o eram, apenas, em nível de ficção, como uma realidade distante. O processamento massivo de dados na realidade europeia ainda era realizado por computadores centralizados. Portanto, encontrava-se em um estágio inicial, que não se distanciava muito da realidade analógica, pois não havia a dinamicidade e a instantaneidade hoje prevalentes.[119]

Ao comentar a decisão alemã, Fabiano Menke explica que a preocupação quanto ao tema se devia ao contexto histórico atravessado à época do julgamento. Além da realidade geopolítica, é possível que a intensa onda de protestos contra o censo tenha sido impactada pelo receio dos cidadãos alemães em relação às previsões descritas na obra “1984”, de George Orwell, que alertava para os riscos de

---

[116] BVerfGE 65, 1 (207).
[117] Todas as traduções do julgado referido são livres.
[118] BVerfGE 65,1 (42).
[119] MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **RJLB, ano** v. 5, p.784, 2019.

um Estado vigilante. Essa preocupação foi potencializada pela proximidade temporal entre o ano de realização do censo, em 1983, e o simbólico título do referido livro "1984".[120]

Nas razões do acórdão, proferiu-se o comentado trecho, que merece menção expressa, por ser especialmente esclarecedor quanto à justificativa e ao conteúdo protegido pela autodeterminação informativa idealizada à época. Veja-se:

> [...] a autodeterminação individual pressupõe - mesmo nas condições das modernas tecnologias de processamento de informação - que o indivíduo tenha liberdade para decidir sobre as ações a serem tomadas ou não, incluindo a oportunidade de realmente se comportar de acordo com essa decisão. Qualquer pessoa que não consiga ver com suficiente certeza quais as informações que lhe dizem respeito são conhecidas em determinadas áreas do seu ambiente social e que não consiga estimar razoavelmente o conhecimento de possíveis parceiros de comunicação pode ter a sua liberdade de planear ou decidir com base na sua própria autodeterminação significativamente inibida. Uma ordem social e o sistema jurídico que a permite, em que os cidadãos já não possam saber quem sabe o quê, quando e em que ocasião, não seria compatível com o direito à autodeterminação informativa. Qualquer pessoa que não tenha certeza se um comportamento desviante será observado a qualquer momento e permanentemente armazenado, usado ou repassado como informação tentará não chamar a atenção para tal comportamento. Qualquer pessoa que espere que a participação numa reunião ou numa iniciativa de cidadania seja oficialmente registada e que daí possam surgir riscos, pode renunciar ao exercício dos seus direitos básicos (artigos 8.º e 9.º da Lei Básica). Isto não afetaria apenas as oportunidades de desenvolvimento do indivíduo, mas também o bem comum, porque a autodeterminação é uma condição funcional elementar de uma comunidade livre e democrática baseada na capacidade dos seus cidadãos de agir e participar.[121]

Essa garantia, à primeira vista, pode soar excessivamente protetiva, especialmente em um contexto de persecução penal, completamente diferente do contexto de elaboração do conceito, qual seja, o recenseamento populacional. Contudo, a preocupação reside não na garantia desmedida da privacidade, tema que sequer é debatido no caso, mas sim, na proteção da esfera pública e da participação popular, que não é possível sem um núcleo essencial de desenvolvimento da personalidade na esfera privada, ou mais profundamente, na esfera íntima do cidadão.

A autodeterminação informativa, longe de significar proteção absoluta da esfera privada em detrimento do interesse público ou do sentido de propriedade privada aos dados, como fossem bens privados, foi concebida como uma garantia de oposição à vigilância estatal. Isso, justamente em prol do interesse público,

---

[120] Ibid.
[121] BVerfGE 65,1 (146).

resguardando o elemento do desenvolvimento da personalidade, o qual depende do núcleo íntimo, sem o qual não se vislumbra o exercício de uma vida pública[122].

É de se observar que, em sua essência, o conceito não foi idealizado para suprimir o interesse público. Ao contrário, resguardou a possibilidade de flexibilização, quando necessária, para assegurar a prevalência de valores coletivos ou a proteção a direitos fundamentais, desde que respeitados os limites legais e a proporcionalidade no caso concreto, após devido sopesamento.

Vale, para tal observação, fazer menção expressa aos trechos do julgado BVerfGE 65, 1 que versam sobre o tema:

> [...] Nas condições modernas de processamento de dados, o livre desenvolvimento da personalidade exige a proteção do indivíduo contra a recolha, armazenamento, utilização e divulgação ilimitadas dos seus dados pessoais. Esta proteção é, portanto, abrangida pelo direito fundamental do artigo 2.º, n.º 1, em conjugação com o artigo 1.º, n.º 1 GG. A este respeito, o direito fundamental garante o direito do indivíduo decidir por si próprio sobre a divulgação e utilização dos seus dados pessoais.
>
> b) Este direito à "autodeterminação informativa" não é garantido sem restrições. O indivíduo não tem direito no sentido de controle absoluto e irrestrito sobre "seus" dados; Pelo contrário, ele é uma personalidade que se desenvolve dentro da comunidade social e depende da comunicação. A informação, mesmo que seja pessoal, representa um reflexo da realidade social que não pode ser atribuída exclusivamente ao interessado. Como já foi repetidamente sublinhado na jurisprudência do Tribunal Constitucional Federal, a Lei Básica resolveu a tensão entre o indivíduo e a comunidade no sentido da relação comunitária e dos laços comunitários da pessoa (BVerfGE 4, 7 [15]; 8 , 274 [329]; Em princípio, o indivíduo deve, portanto, aceitar restrições ao seu direito à autodeterminação informativa no esmagador interesse geral.
>
> De acordo com o Artigo 2, Parágrafo 1 da Lei Básica - como também foi corretamente reconhecido na Seção 6, Parágrafo 1 da Lei Federal de Estatística - essas restrições exigem uma base legal (constitucional) a partir da qual os requisitos e o escopo das restrições sejam claros e reconhecíveis ao cidadão e que, portanto, corresponde à exigência do Estado de direito de clareza das normas (BVerfGE 45, 400 [420] com outras referências). Ao elaborar a sua regulamentação, o legislador deve também observar o princípio da proporcionalidade. Este princípio, que tem estatuto constitucional, decorre da natureza dos próprios direitos fundamentais, que, como expressão do direito geral do cidadão à liberdade do Estado, só pode ser restringido pela autoridade pública na medida em que seja essencial para proteger interesses públicos (BVerfGE 19, 342 [348]; st. Tendo em conta os riscos já delineados da utilização do processamento automático de dados, o legislador deve, mais do que antes, tomar precauções organizacionais e processuais que contrariem o risco de violação dos direitos pessoais (cf. BVerfGE 53, 30 [65]; 63.131 [143]).
>
> As reclamações constitucionais não suscitam uma discussão exaustiva sobre o direito à autodeterminação informacional. A única coisa que precisa de ser

[122] A necessidade de preservação do núcleo íntimo para coexistência do indivíduo na esfera pública foi referida na pioneira obra de Warren e Brandeis, e até hoje é uma ponderação que baliza trabalhos atuais sobre o avanço da tecnologia X tutela da privacidade, como as obras de Cohen e Solove, referidas neste trabalho. WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. Harvard Law Review, v. 4, n. 5, p. 193-220, Dec. 1890.

> decidida é o alcance deste direito para intervenções através das quais o Estado exige que os cidadãos forneçam dados pessoais. O tipo de informação não pode ser confiável sozinho. Sua usabilidade e possíveis usos são cruciais. Estas dependem, por um lado, da finalidade da recolha e, por outro, das opções de processamento e ligação inerentes às tecnologias de informação. Isto significa que uma data que é em si irrelevante pode assumir um novo significado; A este respeito, nas condições de tratamento automático de dados, já não existe uma data "insignificante".
>
> Na medida em que a informação é sensível não pode, portanto, depender apenas do facto de se tratar de processos íntimos. Em vez disso, para determinar o significado de uma data para os direitos pessoais, é necessário conhecer o contexto da sua utilização: só quando estiver claro para que finalidade a informação é necessária e quais as possíveis ligações e utilizações existentes é que a questão de uma restrição permissível pode ser resolvida. do direito à autodeterminação informacional seja respondida. Deve ser feita uma distinção entre os dados pessoais recolhidos e tratados de forma individualizada e não anonimizada (ver alínea a) e aqueles que se destinam a fins estatísticos (ver alínea b).

Fato é que, mais uma vez, o conceito cunhado à frente de seu tempo acertou na previsão de que a automatização do processamento de dados impactaria a vida pública. Exemplo disso é o caso do *Facebook*, no escândalo acerca das eleições estadunidenses, já citado anteriormente.

Contemporaneamente, o conceito tem sido ampliado de suas bases originais, isto é, a dignidade da pessoa humana e o direito geral de personalidade, para abranger também a proteção à privacidade, especificamente voltado para a proteção de dados pessoais, frente à exploração comercial exercida por empresas. Esse é o foco principal da LGPD que, inclusive, incorporou a autodeterminação informativa como um princípio, como expressa o inciso II de seu art. 2º .[123]

A autodeterminação informativa, após sua criação jurisprudencial, ocorrida em 1983, incentivou a criação de legislações e da jurisprudência não apenas a alemã, como a mundial, tanto no âmbito interno dos países – com influências nas leis e nas jurisprudências nacionais –, quanto no âmbito externo. Nesse, o impacto diz respeito à cooperação internacional para empenhar esforços protetivos aos dados pessoais e, mais atualmente, à privacidade.[124]

Ao difundir-se pelo globo ao longo do tempo, a autodeterminação informativa acompanhou o desenvolvimento tecnológico que, ao expandir as possibilidades de trocas instantâneas de informação, aumentou, de igual modo, as

---

[123] LEI GERAL DE PROTEÇÃO DE DADOS. Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
[...] II - a autodeterminação informativa;

[124] MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **RJLB**, v. 5, p. 786, 2019.

vias que permitem a vigilância, não apenas estatal, mas também de entes privados. Por essa razão, e talvez também pela conveniência temporal (quando da emergência das novas tecnologias, ele estava bem definido em relação à esfera de oposição da privacidade frente ao Estado), o conceito, que se reveste da natureza de princípio, mostra-se importante ferramenta para frear o processamento indevido de dados pessoais de qualquer espécie, na nova seara digital, decorrente da emergência da revolução 4.0.

No Brasil, a autodeterminação informativa, incorporada pela jurisprudência do STF, será operacionalizada pelos demais tribunais, embora esse processo de assimilação ainda esteja em estágio inicial.

Curiosamente, o conceito de autodeterminação foi invocado com notoriedade, pela primeira vez, na jurisprudência brasileira, no julgamento da ADI 6387/DF,[125] que também versa sobre o recenseamento da população, reforçando seu caráter protetivo do cidadão em face de possíveis abusos estatais.

Essa ADI 6387/DF foi proposta pelo Conselho Federal da Ordem dos Advogados do Brasil (OAB), questionando a constitucionalidade da Medida Provisória (MP) nº 954/2020, que determinava o compartilhamento de dados pessoais dos usuários de serviços telefônicos com o Instituto Brasileiro de Geografia e Estatística (IBGE), na emergência de saúde pública decorrente da pandemia de Covid-19.

O STF, por maioria, decidiu referendar a medida cautelar que suspendia a eficácia dessa MP, com decisão baseada nos seguintes fundamentos: proteção da privacidade e autodeterminação informativa, garantidas pela LGPD, são direitos fundamentais assegurados pela Constituição Federal. O tratamento e a manipulação de dados pessoais devem observar os limites constitucionais para evitar lesões a esses direitos. Conforme o Regulamento Sanitário Internacional (RSI 2005), o tratamento de dados pessoais para avaliação e manejo de riscos em saúde pública deve ser adequado, relevante, não excessivo e limitado ao tempo necessário para alcançar seus objetivos.[126]

A Ministra Rosa Weber, relatora do processo da ADI 6387/DF, entendeu que a MP nº 954/2020 não se fundou em interesse público legítimo para o compartilhamento de dados pessoais, nos moldes em que foi editada. Faltava definição apropriada sobre o uso e a finalidade dos dados coletados, desrespeitando

---

[125] SUPREMO TRIBUNAL FEDERAL. **ADI 6387/2020 MC-REF/DF**.
[126] Ibid.

a garantia do devido processo legal e a necessidade de medidas proporcionais e adequadas. Além disso, a MP não oferecia mecanismos técnicos ou administrativos suficientes para proteger dados pessoais contra acessos não autorizados, contra vazamentos acidentais ou contra utilização indevida, comprometendo a segurança e o sigilo dos dados compartilhados. A conservação dos dados pessoais por 30 dias após o fim da emergência em saúde pública foi considerada excessiva e desnecessária para a finalidade declarada. A ausência de vigência da LGPD, no entendimento da relatora, agravou a falta de garantias de tratamento adequado e seguro dos dados compartilhados. Inclusive. essa tese foi reafirmada pela maioria dos Ministros no julgamento de outra ação, a ADI 6649/DF, que tratou do compartilhamento dos dados pessoais entre os órgãos públicos. [127]

Após esses julgados, também houve avanço na conformação constitucional da proteção de dados pessoais, com a incorporação da Emenda Constitucional (EC) n. 115, de 10 de fevereiro de 2022, que incluiu a proteção de dados pessoais no rol dos direitos e das garantias fundamentais. O marco constitucional foi instituído após a edição da legislação infraconstitucional, qual seja, o MCI e a LGPD. Contudo, ele não deixou de contribuir para o desenvolvimento da temática no Brasil.

Segundo reflete Ingo Sarlet, antes dessa emenda, ainda que se pudesse, em termos práticos,

> reconhecer a proteção de dados como um direito fundamental implícito, daí extraindo todas as consequências atinentes à tal condição, [...] sua positivação formal [...] carrega consigo uma carga positiva adicional, ou seja, agrega (ou, ao menos, assim o deveria) valor positivo substancial em relação ao atual estado da arte no Brasil.[128]

A contraintuitiva inserção constitucional tardia da proteção de dados no rol de garantias fundamentais denota o cenário de assimilação do tema pela legislação brasileira que, embora caminhe a passos relativamente largos nos últimos anos pós-pandemia, ainda enfrenta muitos desafios.

A referida emenda constitucional estabelece, em seu artigo 5º, LXXIX, que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".[129]

---

[127] SUPREMO TRIBUNAL FEDERAL. **ADI 6387/2020 MC-REF/DF.**
[128] SARLET, Ingo Wolfgang. A EC 115/22 e a proteção de dados pessoais como direito fundamental I. **Revista Consultor Jurídico**, v. 11, 2022, Disponível em: https://www.conjur.com.br. Acesso em: 10 de out. de 2024.
[129] Emenda Constitucional n.º 115/2022.

Essa inovação legislativa insere-se na tendência global de fortalecimento da autodeterminação informativa, colocando o Brasil em consonância com as diretrizes estabelecidas pelo pioneiro GDPR da União Europeia, já referido. Essa lei, em seu momento primevo, 2016, foi escrita sob a influência o conceito de autodeterminação informativa originado três décadas antes.

Em especial no âmbito da segurança pública e da persecução penal, a consolidação da proteção de dados assume especial relevo. Isso porque, com a inserção dessa garantia na ordem constitucional, supre-se uma lacuna quanto ao tema, já que, como consignado, a legislação infraconstitucional especializada, a LGPD, não contempla os setores da segurança nacional, segurança pública, investigação criminal.

Especialmente quanto a esse ponto, explica Ingo Wolfgang Sarlet que "com o reconhecimento do referido direito fundamental, passa a inexistir uma 'zona livre' de proteção dos dados pessoais na ordem jurídica brasileira."[130] Mas, ao se observar a redação literal do dispositivo inserido pela EC n.º 115/22, nota-se que o texto não traz a consolidação da autodeterminação informativa expressamente.

Então, qual seria o sentido de se atrelar esse importante conceito a uma alteração constitucional que perdeu a oportunidade de incluir tal garantia de maneira expressa na Carta Magna?

Pois bem. A autodeterminação informativa, na sua essência mais primordial, é um fruto comum dos corolários do princípio da dignidade da pessoa humana e do direito à privacidade, cuja interpretação integrada direciona ao reconhecimento do direito de livre desenvolvimento da personalidade.

Convém destacar que, de forma semelhante à Constituição Brasileira, a Lei Fundamental Alemã não consigna expressamente a autodeterminação informativa ao longo de seu texto. Todavia, no julgamento do caso do Recenseamento, isso não impediu a criação do conceito a partir de garantias já estabelecidas em seu texto.

A similaridade entre elas é tanta que o conceito apareceu, de forma ilustre, em decisão de caso também acerca do recenseamento da população, consoante destacado alhures. Semelhante ao entendimento fundante da autodeterminação informativa na Alemanha, viu-se, também no Brasil, que a interpretação conjugada das garantias sobreditas, em respeito à coerência do sistema, leva à inevitável

[130] Ibid.

limitação de ações estatais que possam tolher o núcleo fundamental da vida privada e, consequentemente, o livre desenvolvimento da personalidade dos cidadãos.

Diante disso, a inclusão da proteção de dados no catálogo constitucional brasileiro representa um importante avanço da legislação e da assimilação - ainda que oriunda de um histórico de precedentes similares - da autodeterminação informativa e é algo a ser considerado na questão do congelamento extrajudicial de dados.

No caso do HC 222.141/DF, a autodeterminação informativa, mencionada nas razões do acórdão, desempenha um papel essencial na integração das interpretações da legislação pátria e da Convenção de Budapeste. Enfrenta a complexa lacuna principiológica que emerge do conflito entre a proteção da privacidade e o interesse público na condução de investigações criminais, desencadeando uma tensão que põe em debate valores igualmente relevantes. Exige que se determine, no caso concreto, qual direito deve prevalecer diante das peculiaridades apresentadas.

De fato, o congelamento extrajudicial de dados, como bem ressalta Vladimir Aras, não se confunde com o acesso direto das autoridades aos dados em questão. Entretanto, a proteção contra o acesso às comunicações privadas, como mencionado, foi idealizada em um contexto em que a única ameaça concebível a esse bem jurídico era o acesso direto a essas informações. À época, sequer se cogitava a possibilidade de que o todo ou grande parte do conteúdo das comunicações pudesse ser preservado sem que o investigado tivesse ciência ou conhecimento do ato.

Atualmente, todavia, essa possibilidade tornou-se uma realidade concreta, tornando anacrônica uma garantia que, embora tenha o inalterado espírito de proteger a vida privada contra os abusos estatais, não mais é suficiente para tanto e tem seu alcance limitado pelos avanços tecnológicos. Tal limitação deve-se ao fato de que o constituinte originário, compreensivelmente, não poderia prever o impacto dessas transformações tecnológicas nem como elas poderiam desafiar e, por vezes, restringir as garantias originalmente concebidas.

Alçada à condição de princípio fundamental no contexto da sociedade da informação, a autodeterminação informativa representa um instrumento jurídico essencial para equilibrar as relações entre o indivíduo e o poder estatal, especialmente no que tange à proteção de dados pessoais. Sua concepção inicial, firmada pelo Tribunal Constitucional Alemão no citado caso emblemático BVerfGE 65, trouxe à tona uma perspectiva dinâmica da privacidade, fundada no direito geral de personalidade.

Esse, nos moldes atuais, abrange o controle individual sobre as informações pessoais e o combate a riscos decorrentes de seu processamento inadequado. O julgamento do HC 222.141/DF reafirmou esse arcabouço teórico e normativo, consolidando a autodeterminação informativa como uma garantia indispensável na era digital.

A decisão evidencia que, embora o congelamento de dados não implique necessariamente o acesso imediato ao conteúdo, ele subtrai do titular o domínio sobre suas informações, violando os princípios da dignidade humana e da privacidade. Assim, ao declarar inconstitucional a prática de congelamento extrajudicial de dados fora dos moldes do MCI, o STF não apenas assegura a proteção dos direitos individuais, como reforça a necessidade de rigor no cumprimento das normas que regem o tema.

Nesse ponto, é essencial destacar que a autodeterminação informativa, embora basilar, não tem caráter absoluto. A própria decisão alemã no caso do BVerfGE 65 e, simetricamente, o julgamento do HC 222.141/DF pelo STF reconhecem que esse direito deve ser ponderado à luz de outros interesses legítimos, como a segurança pública e a investigação criminal.

Contudo, tais restrições devem observar limites rigorosos, sob pena de esvaziar o próprio núcleo essencial das garantias fundamentais. A reserva de jurisdição, em relação ao congelamento dos dados de conteúdo, figura como condição indispensável para qualquer medida restritiva dessa espécie de dados, dado o potencial de ferir garantias constitucionais.

Ademais, a decisão do STF não deixa dúvidas quanto à necessidade de distinção entre os registros de conexão, cuja preservação extrajudicial é permitida pelo MCI, e o conteúdo das comunicações privadas, que possui maior grau de proteção na ordem constitucional vigente. Essa sistemática, ancorada no MCI, harmoniza a proteção da privacidade – entendida como núcleo essencial do desenvolvimento da personalidade – com o legítimo interesse público na condução de investigações criminais.

Não se trata, portanto, de utilizar o princípio da autodeterminação informativa como trunfo para obstruir toda e qualquer investigação que vise ao congelamento extrajudicial de dados. O que se busca é reafirmar que tais medidas devem ser aplicadas de acordo com os limites estabelecidos pela legislação pátria, ou seja, exclusivamente sobre dados cadastrais e registros de conexão.

Considerando a relevância dos bens jurídicos envolvidos, quando houver necessidade de congelamento das comunicações privadas, a medida deve ser submetida ao crivo judicial, garantindo que sua aplicação esteja em conformidade com os princípios da proporcionalidade e da legalidade e, sobretudo, com a proteção dos direitos fundamentais.

O julgamento deixa claro que, para além do acesso, a possibilidade desmedida do congelamento de dados sem amparo judicial compromete a autodeterminação informativa, ao retirar do cidadão o controle efetivo sobre suas informações, subvertendo a lógica protetiva da legislação.

Assim, a autodeterminação informativa, ao ser reconhecida e aplicada na práxis jurisprudencial brasileira, revela-se um instrumento necessário para conter os avanços tecnológicos que podem se tornar ameaças às liberdades individuais. Longe de ser uma abstração teórica, esse princípio é a concretização do compromisso constitucional com a dignidade humana e com a privacidade, protegendo os cidadãos contra intervenções arbitrárias do Estado, especialmente sob o trunfo de utilização das informações em primazia do interesse público quanto de atores privados. O HC 222.141/DF oportuniza a aplicação desse princípio também ao âmbito da persecução penal, não apenas para resguardar os valores democráticos, mas para estabelecer um marco de modernidade jurídica adequado aos desafios de uma sociedade conectada.

3.2 Nível escalonado de proteção de dados na legislação brasileira e disposições da Convenção de Budapeste: discussão sobre viabilidades e limites do congelamento extrajudicial de dados

Como dito na introdução, as leituras realizadas quando da seleção do material coletado para a pesquisa e aprofundadas durante esta escrita propiciaram subsídios que me permitiram desenvolver argumentos sobre seu objeto de análise. Ainda que incipientes, esses argumentos podem ser considerados positivos, se observados como ponto de vista pessoal, resultado concreto do exercício desta monografia.

Com base na análise do arcabouço normativo brasileiro, conclui-se que, em contraposição à tese defendida pelos adeptos da admissibilidade irrestrita da preservação extrajudicial de dados, a chamada "medida precautelar" referente aos dados de conteúdo não deve ser admitida de forma ampla. Pelo contrário, sua

aplicação deve ser estritamente delimitada pelos limites expressamente previstos na legislação vigente, conforme se decidiu no âmbito do HC 222.141/DF.

Como abordado no Capítulo I, ao tratar da legislação pertinente à discussão, o MCI, ao permitir o congelamento extrajudicial de dados, estabelece uma estrutura escalonada, restringindo a medida exclusivamente aos registros de conexão e de aplicações de internet, de modo que os dados de conteúdo não são incluídos no escopo da medida. Em contrapartida, a Convenção de Budapeste apresenta uma previsão significativamente mais ampla, ao permitir que a medida alcance os chamados "dados informáticos", uma denominação genérica que engloba qualquer tipo de informação passível de processamento por computador.

Na discussão inaugurada pelo HC 222.141/DF, duas nuances centrais merecem análise: a primeira é a extrajudicialidade da medida, ou seja, o fato de que o acesso aos dados pessoais ocorreu sem uma decisão judicial formal. Essa característica impõe um desafio, pois exclui a possibilidade de uma apreciação caso a caso da aplicação da medida, o que aumenta o risco de violação aos direitos fundamentais. É que não se pode desconsiderar a possibilidade de requisição do congelamento extrajudicial pelo MP de forma desmedida, sem qualquer justificativa, fazendo-o inclusive para fins abusivos ou dissociados do interesse público.

Essas questões criam um questionamento significativo sobre até que ponto é possível justificar medidas extrajudiciais que envolvam o congelamento ou a preservação de dados sensíveis sem violar garantias fundamentais. O problema pode ser mais bem compreendido sob uma perspectiva lógico-argumentativa, inspirada na estrutura lógica aristotélica.

A propósito, sobre a validade das premissas, a análise do congelamento extrajudicial de dados no Brasil não enseja grandes discussões, uma vez que elas são estabelecidas pelo ordenamento jurídico pátrio, especialmente o MCI. Esse Marco consagra uma lógica escalonada de proteção de dados, diferenciando níveis de sensibilidade, a qual é calcada nas bases constitucionais de proteção às comunicações privadas. Com base na estrutura aristotélica, aplica-se o seguinte raciocínio lógico ao tema:

> **Premissa Maior:** no contexto da persecução criminal, **dados cadastrais** podem ser **acessados sem autorização judicial**, pois possuem um menor grau de proteção de privacidade, conforme regulamentado pelo MCI. **Registros de conexão podem ser congelados sem ordem judicial**, mas

só podem ser obtidos mediante autorização judicial, pois possuem grau intermediário de proteção.

Premissa Menor : dados de comunicação, que incluem conteúdo de mensagens e outras informações pessoais sensíveis, **só podem ser acessados mediante autorização judicial**, dado o alto grau de proteção da privacidade, conforme o art. 5º da CF, a Lei 9.296/1996 e o MCI.

Conclusão: se os dados de comunicação só podem ser acessados com autorização judicial devido à sua sensibilidade, então o congelamento desses dados deve igualmente seguir um padrão rigoroso de proteção, demandando justificativa robusta e controle judicial para assegurar que a medida não viole os princípios de privacidade estabelecidos pelo MCI e demais leis pertinentes.

À primeira vista, a estruturação do problema em premissas lógicas pode soar fria e excessivamente voltada ao positivismo clássico formal, o qual é divorciado de qualquer consequencialismo. Porém, essa organização, aqui, cumpre um papel meramente analítico da sistemática brasileira, a partir dos dispositivos analisados capítulos anteriores. A utilização da fórmula lógica é só uma ferramenta para se extrair, de maneira mais exata, o que já está expresso no ordenamento.

A interação lógica entre as premissas é irrefutável. A ideia de que o congelamento de dados não se confunde com o acesso propriamente dito carece de força argumentativa para afastar a conclusão inequívoca de que a preservação extrajudicial de dados de conteúdo é inadmissível no sistema persecutório penal brasileiro.

De fato, congelamento extrajudicial não é a mesma coisa que acesso aos dados. Entretanto, os princípios que protegem o sigilo dos dados telemáticos são os mesmos que incidem sobre o congelamento extrajudicial de dados, acrescidos à autodeterminação informativa, *topoi* que ocupa espaço de relevância na regulação de dados e privacidade no atual mundo ocidental.

Quanto ao ponto, é verdade que os dados cadastrais e de conexão, por serem considerados de menor sensibilidade, têm um tratamento menos rigoroso, permitindo o congelamento extrajudicial sem grandes entraves. No entanto não há, no MCI, qualquer menção de que dados de conteúdo comunicacional estejam insertos no escopo da medida.

Se houvesse, é certo que se trataria de uma previsão desprovida de sentido dentro da estrutura escalonada de dados; algo que subverteria sua própria lógica, pois qualquer ingerência que possa restringir as garantias relativas às comunicações privadas só está em conformidade com o ordenamento caso autorizada judicialmente.

Nessa conjuntura, não há como simplesmente ignorar toda essa subdivisão bem consolidada no ordenamento, para que se permita a preservação extrajudicial de dados comunicacionais, ainda que a medida seja utilizada com nobres finalidades sociais. Uma concessão nesse sentido abrirá precedentes para desencadear uma potencial vigilância estatal em níveis descomunais, embora revestida de diligência não lesiva aos direitos e às garantias fundamentais.

Antes de eclodir a discussão no STF, por ocasião do julgamento do HC 222.141/DF, o tema foi abordado em 2017 no artigo “Conservação e acesso a dados públicos e privados para fins penais: a normativa legal brasileira examinada desde a perspectiva da jurisprudência do Tribunal de Justiça da Comunidade Europeia”, de autoria de André Machado Maya[131].

Ao analisar o artigo 17 da Lei 12.850/2013, que estabeleceu para as empresas operadoras a obrigação de conservação de registros telefônicos por cinco anos, abrangendo os números de origem e destino das chamadas, o autor destacou que tal obrigação não foi estendida às comunicações eletrônicas, revelando uma abordagem normativa ainda fragmentada frente aos avanços tecnológicos. Antes dessa inovação, o ordenamento jurídico brasileiro limitava-se à regulamentação da interceptação telefônica pela Lei 9.296/1996, sem prever obrigações de conservação cautelar de quaisquer dados nem delimitação temporal para os dados registrais.[132]

Fazendo um recorte restritivo às comunicações telefônicas, Maya salientou que até mesmo a implementação da conservação dos meros registros telefônicos, que se limitam aos dados de origem e de destino, sem avançar sobre o conteúdo propriamente dito, deve observar uma articulação constitucional sistemática. É que os dados conservados refletem aspectos íntimos dos indivíduos, como os padrões de interação e preferências pessoais, mesmo quando não revelam o conteúdo das comunicações. O autor afirma, a título de exemplo, que registros de chamadas para

---

[131] MAYA, André Machado. Conservação e acesso a dados públicos e privados para fins penais: a normativa legal brasileira examinada desde a perspectiva da jurisprudência do Tribunal de Justiça da Comunidade Europeia. **Revista Brasileira de Ciências Criminais**, n. 138, 2017, p. 5-8.
[132] Ibid., p. 10 – 15.

casas de câmbio, de prostituição ou até mesmo para médicos psiquiatras, por si sós, refletem, inequivocamente, aspectos da intimidade pessoal, mesmo que não se acesse o conteúdo das comunicações.[133]

Comparando essa sistemática com o cenário europeu, Maya ressalta que o Tribunal de Justiça da Comunidade Europeia estabelece que a legitimidade de normas similares, que impõe o dever geral de conservação de dados, depende da instituição conjunta de critérios como proporcionalidade, necessidade, autorização por órgão jurisdicional ou entidade independente e delimitação temporal e objetiva da medida. Esses são requisitos também dispostos na Lei 9.296/1996, segundo a qual a interceptação telefônica deve ser precedida de prévia investigação criminal e da demonstração da estrita necessidade da medida.[134]

No âmbito da União Europeia, o debate sobre a conservação e o acesso a dados de comunicações tem se desenvolvido em torno da tensão entre a segurança pública e a proteção dos direitos fundamentais, como privacidade e intimidade. Maya destaca que a Diretiva 2002/58/CE estabeleceu a necessidade de medidas legislativas para regulamentar a proteção dos dados pessoais e a confidencialidade das comunicações eletrônicas; propôs um equilíbrio entre esses direitos e as exigências de segurança pública. A diretiva previa a eliminação ou anonimização dos dados após sua utilização, restringindo a conservação ao estritamente necessário para fins de transmissão ou investigações legítimas.[135]

No entanto, os atentados terroristas no início dos anos 2000 impulsionaram a adoção de medidas mais rigorosas, como a Diretiva 2006/24/CE, que impôs a obrigação geral de conservação de dados de comunicação por períodos de seis meses a dois anos. Essa norma ampliou de forma significativa as possibilidades de controle estatal, autorizando a retenção de dados de localização, de origem, de destino, de tipo e de duração das comunicações, independentemente de suspeitas criminais específicas.

Maya ressalta que a invalidade dessa Diretiva foi declarada pelo Tribunal de Justiça da União Europeia nos casos C-293/12 e C-594/12[136], ambos resultantes da contestação promovida pela *Digital Rights Ireland* (DRI), uma organização

---

[133] Ibid., p. 10-15.
[134] Ibid., p. 10-15.
[135] Ibid., p. 10-15.
[136] TRIBUNAL DE JUSTIÇA DA COMUNIDADE EUROPEIA. **Processos C-293/12 e C-594/12**. Disponível em: [https://curia.europa.eu/juris/liste.jsf?&num=C-293/12]." Acesso em 26 dez de 2024.

dedicada à defesa da privacidade. A ação questionou a legalidade de medidas legislativas que exigiam a retenção de dados relacionados a comunicações eletrônicas, com fundamento na violação dos direitos à privacidade e à proteção de dados pessoais, previstos nos artigos 7º e 8º da Carta dos Direitos Fundamentais da União Europeia.

Especificamente, a contestação foi contrária à Diretiva de Retenção de Dados e Parte 7 do *Criminal Justice (Terrorist Offenses) Act 2005*, que obrigavam provedores de serviços de comunicações a armazenar dados de tráfego e de localização por um período determinado. O objetivo era prevenir, detectar, investigar e processar crimes, além de garantir a segurança do Estado.[137]

O tribunal enfatizou que a obrigação geral de conservação de dados, sem delimitações claras quanto ao alcance subjetivo, geográfico e temporal, comprometia a proporcionalidade e permitia uma intrusão excessiva na vida privada dos indivíduos. Portanto, reconheceu sua incompatibilidade frente à Carta de Direitos Fundamentais da União Europeia.[138]

Maya destaca que, posteriormente, com a decisão dos casos C-293/12 e C-594/12, outros dois, denominados C-203/15 e C-698/15,[139] chegaram à Corte da União Europeia. No primeiro caso, o provedor de serviços de comunicações eletrônicas *Tele2 Sverige* informou à *Post-ochTelestyrelsen* (PTS) que não mais cumpria os requisitos da legislação nacional sobre retenção e manutenção dos dados pelo período de até seis meses. Portanto, a partir de 14 de abril de 2014, a empresa pararia de reter dados de comunicações eletrônicas e apagaria os dados retidos antes dessa data. A PTS discordou do argumento da Tele2 e entrou com uma ação no Tribunal Administrativo de Estocolmo.[140]

Já no caso C 698/15, o Sr. Watson, o Sr. Brice e o Sr. Lewis contestaram a Seção 1 da Lei de Retenção de Dados e Poderes Investigativos de 2014, considerando sua incompatibilidade com os artigos 7 e 8 da Carta e artigo 8 da Convenção Europeia dos Direitos do Homem (CEDH).

---

137 Ibid.
138 Ibid.
139 TRIBUNAL DE JUSTIÇA DA COMUNIDADE EUROPEIA. Processos C-203/15 e C-698/15.
140 TRIBUNAL DE JUSTIÇA DA COMUNIDADE EUROPEIA. Processos C-203/15.

O Tribunal Superior de Justiça da Inglaterra e do País de Gales concluiu que a lei nacional de retenção de dados não era compatível com as leis da União Europeia (EU).

No julgamento conjunto dos casos, o tribunal reafirmou que a conservação de dados só é legítima quando acompanhada de garantias rigorosas, como: limitação a infrações graves, controle prévio por autoridades independentes e previsão de medidas que assegurem a segurança dos dados armazenados. Maya concluiu que o modelo europeu evoluiu para uma abordagem mais equilibrada, priorizando a proporcionalidade e a proteção dos direitos fundamentais, ao tempo em que reconheceu a necessidade de instrumentos eficazes para a persecução penal.[141]

Nesse sentido, com fundamento nesses julgados e fazendo analogia com o ordenamento brasileiro, esse autor defende que é imprescindível a interpretação do artigo 17 da Lei 12.85/2013 estar em harmonia com a Constituição Federal, especialmente o artigo 5º, XII, que protege o sigilo das comunicações, e a respectiva regulamentação trazida na Lei 9.296/1996. Deve-se exigir a reserva de jurisdição para a preservação de dados relativos às comunicações privadas.[142]

Particularmente, considera-se que ermbora o dispositivo se aplique apenas às comunicações telefônicas e não se estenda às comunicações realizadas no ambiente eletrônico da rede mundial de computadores, a reflexão trazida pelo autor, ainda em 2017, é relevante por representar uma das primeiras análises que tangenciam o tema vertido no HC 222.141/DF; ele o aborda, ainda que de forma superficial.

Ademais, nas circunstâncias descritas no texto de Maya, a conservação extrajudicial analisada se mostra análoga ao congelamento das comunicações digitais, considerando que o grau de interferência na privacidade é igualmente significativo. Ressalte-se que no caso da conservação de dados digitais, a invasão se revela mais intensa e abrangente, já que incide sobre o conteúdo da comunicação e não apenas sobre as informações de origem e de destino.

Essas ponderações iniciais de Maya são muito relevantes para se compreender as razões pela qual a preservação de dados referentes às

---

[141] MAYA, André Machado. Conservação e acesso a dados públicos e privados para fins penais: a normativa legal brasileira examinada desde a perspectiva da jurisprudência do Tribunal de Justiça da Comunidade Europeia. **Revista Brasileira de Ciências Criminais,** n. 138, 2017, p. 15.
[142] Ibid., p. 16.

comunicações privadas, sejam elas telefônicas ou digitais, não pode ocorrer sem ordem judicial fundamentada especificamente para esse fim. Isso porque não há outra maneira, ao menos na atual disposição de instituições no ordenamento, que possa resguardar o cumprimento dos requisitos mínimos de razoabilidade para tamanha flexibilização da privacidade.

Já em seu texto, Vladimir Aras critica a decisão do STF no HC 222.141/DF, ao defender a admissibilidade da preservação extrajudicial de dados de conteúdo. Ele arremata sua argumentação valendo-se das disposições constantes na recém incorporada Convenção de Budapeste. Argumenta que, a despeito das estruturas de diferenciação dos dados e do fato de que o MCI permite a incidência da medida apenas ao limitado rol dos dados cadastrais e de conexão, o artigo 16 dessa Convenção - aprovada em rito que lhe confere status de norma infraconstitucional - tem prevalência sobre todas as disposições originalmente pátrias que incidem diretamente sobre a questão. São elas: os artigos do MCI que dispõem sistematicamente sobre a medida, em função da superveniência temporal do tratado sobre a legislação nacional.

Não é necessário muito esforço para se notar que o argumento, semelhante ao intento de suavizar o congelamento, sob a afirmação de que ele se difere do acesso efetivo e, portanto, não seria lesivo à autodeterminação informativa e à privacidade, não se sustenta sob quaisquer luzes.

É necessário resolver a questão hermenêutica entre a Convenção de Budapeste e o MCI, sobretudo ao se considerar a maneira pela qual os níveis de proteção de dados são estruturados e aplicados, visando assegurar uma interpretação que harmonize as disposições legais em conflito.

Ao defender a medida de congelamento extrajudicial de dados, Vladimir Aras afirma que o Brasil, ao se tornar signatário da Convenção de Budapeste, assumiu o compromisso de cumprir o artigo 16 do MCI; logo, deve admitir que a medida recaia tanto sobre dados cadastrais e de conexão, quanto sobre dados de conteúdo.

Ocorre que, como já se expôs, o ordenamento brasileiro não permite o acesso de dados de conteúdo por meio de requisição extrajudicial, como previsto em diversos dispositivos legais.

Também restou claro que, ao contrário do que fora aventado pelos defensores da medida, o congelamento extrajudicial não possui ínfimo grau de invasividade a ponto de permitir que se ignore toda a estrutura legal que garante a

proteção à privacidade e, mais contemporaneamente, assegura a autodeterminação informativa.

O congelamento extrajudicial de todas as espécies de dados de conteúdo não colhe melhor sorte a partir da análise integral da própria Convenção de Budapeste; o referido tratado não prevê a aplicação desmedida da preservação extrajudicial de dados. Já da leitura de seu artigo 15 , destaca-se a seguinte previsão:

> Article 15 – Conditions and safeguards:
>
> 1 - Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
>
> 2 - **Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.**
>
> 3 -**To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties**.[143] g.n.

Da leitura dos referidos artigos, é visível que o tratado condiciona a aplicabilidade de suas disposições processuais à conformidade com o ordenamento pátrio dos signatários, mais especificamente, com “as condições e salvaguardas previstas em sua legislação interna”, desde que alinhadas aos dispositivos internacionais de proteção aos Direitos Humanos. Ainda: o diploma dispõe expressamente que pode ser acrescido, às medidas, o crivo judicial, caso exista motivação que justifique tal avaliação prévia.

---

[143] COUNCIL OF EUROPE. **Convenção de Budapeste.** Artigo 15 – Condições e Salvaguardas. 1- Cada Parte deve assegurar que o estabelecimento, a implementação e a aplicação dos poderes e procedimentos previstos nesta Seção estejam sujeitos a condições e salvaguardas previstas em sua legislação nacional, que deverão fornecer proteção adequada aos direitos e liberdades humanas, incluindo os direitos decorrentes das obrigações assumidas sob a Convenção Europeia de Direitos Humanos de 1950, o Pacto Internacional de Direitos Civis e Políticos das Nações Unidas de 1966 e outros instrumentos internacionais aplicáveis de direitos humanos, incorporando o princípio da proporcionalidade. 2 - Tais condições e salvaguardas deverão, conforme apropriado à natureza do procedimento ou poder em questão, incluir, entre outros, supervisão judicial ou independente, justificativas para sua aplicação e limitação do alcance e da duração de tal poder ou procedimento. 3- Na medida em que seja consistente com o interesse público, em particular com a administração adequada da justiça, cada Parte deverá considerar o impacto dos poderes e procedimentos desta seção sobre os direitos, responsabilidades e interesses legítimos de terceiros. Disponível em: https://www.coe.int/ Acesso em: 24 dez. 2024. Tradução livre.

O próprio artigo 16 da Convenção de Budapeste, ao instituir a conservação expedita dos dados, dispõe que “os poderes e procedimentos referidos neste artigo estarão sujeitos aos artigos 14 e 15”. Assim, faz menção expressa ao respeito conferido às salvaguardas dos ordenamentos locais para aplicação da medida.

A conservação expedita de dados, nesse sentido, se revela como uma orientação geral aos países signatários, um sinal do compromisso com a persecução penal voltada especificamente à cibercriminalidade. É uma medida a ser harmonizada com as modalidades de garantia dos direitos fundamentais de cada país e não uma exigência cogente, até mesmo porque a convenção não traz critérios e procedimentos claros para direcionar sua operacionalização. O que se busca, na realidade, é que os dados sejam conservados de forma ágil, dada a volatilidade das provas digitais, dada sua volatilidade como prova digital, garantindo que, no decorrer de uma investigação criminal, as informações essenciais não sejam perdidas, e essa perda comprometa a efetividade da persecução penal.

Ora, não é razoável sobrepor uma recomendação genérica e, em certa proporção, expressamente condicionada aos ordenamentos dos países signatários às leis brasileiras que regulam a salvaguarda dos dados comunicacionais.

A Convenção de Budapeste, como importante instrumento internacional, deve, consoante previsão expressa em seus artigos 14 e 15, ser aplicada de modo a respeitar a autonomia dos sistemas jurídicos nacionais. Não pode prevalecer sobre normas específicas e detalhadas estabelecidas pela legislação brasileira, para garantir a proteção e a privacidade dos dados.

Isso deveria ocorrer especialmente quando elas resguardam de forma adequada as exigências materiais e processuais necessárias à manutenção do compromisso diplomático firmado. É que existe a possibilidade de preservação expedita de dados, desde que respeitado o respectivo grau de sensibilidade (de acordo com o MCI, que permite a incidência da medida sobre os dados cadastrais e de conexão), com o fim comum de combate à cibercriminalidade.

Sob esse viés, é ainda mais visível que as disposições brasileiras cumprem o compromisso internacional firmado, dentro das limitações constitucionalmente consolidadas. O prazo de preservação dos dados na legislação brasileira é significativamente maior que o prazo estabelecido pela Convenção de Budapeste.

Essa Convenção, em seu artigo 16, estabelece que o prazo inicial de congelamento extrajudicial de dados deve ser de até 90 dias, podendo ser prorrogado

se necessário à preservação da investigação. Já o MCI prevê, nos artigos 13, § 2º, e 15, *caput,* respectivamente, prazos de um ano e seis meses para conservação dos registros de conexão e dos registros de acesso a aplicações de internet. Esses prazos podem ainda ser prorrogados por tempo superior não delimitado, caso haja pedido da autoridade policial ou ministerial. Há que se destacar que, até mesmo essas disposições já são alvos de críticas, por possibilitarem potencial vigilância estatal considerada excessiva[144].

Veja-se que a lei brasileira privilegia a conservação de dados para o alcance das nobres finalidades buscadas pela persecução penal. O que não ocorre é a flexibilização de direitos constitucionalmente previstos, quais sejam: a privacidade e, recentemente, a autodeterminação informativa, conceito modernizador do alcance da privacidade na realidade digital. Logo, é de ver que a legislação brasileira preza pela efetividade da investigação criminal, mas sem violar a garantia de sigilo das comunicações e a autodeterminação informativa, princípios que, como dito alhures, foram consolidados na sistemática nacional com base na dignidade humana.

E justamente por ferir garantias constitucionais é que o congelamento de dados de conteúdo comunicacional se destaca sem ordem judicial prévia. Além de ser incompatível com a legislação infralegal, deve também ser considerado inconstitucional.

Como exposto no tópico anterior, é equivocado concluir que a Convenção de Budapeste impõe o congelamento de dados de conteúdo de forma extrajudicial. E ainda que trouxesse essa exigência, mesmo com a finalidade louvável de repressão de crimes, as disposições não poderiam ser absorvidas por serem contrárias às garantias constitucionais da privacidade e da dignidade humana. Essas, atualmente, desdobram-se na autodeterminação informativa, consolidada no ordenamento brasileiro.

A garantia de inviolabilidade da correspondência, ressalvada apenas a possibilidade de interceptação por ordem judicial, devidamente fundamentada, assegura que as comunicações privadas estejam protegidas contra interferências indevidas, especialmente de entes estatais. Por isso, os dispositivos do MCI, que

---

[144] ALVES, Ana Abigail Costa Vasconcelos; MUNIZ, Antônio Walber Matias; CIDRÃO, Taís Vasconcelos. A oportuna e necessária aplicação do direito internacional nos ciberespaços: uma avaliação sobre a Convenção de Budapeste. **FOMERCO – Fórum Universitário Mercosul**, v. 1, n. 44, 2023. p. 8.

permitem o congelamento extrajudicial, restringem-se a dados cadastrais e a registros de conexão, categorias cujo sigilo admite maior flexibilidade. Já as comunicações privadas, em virtude de sua inviolabilidade constitucional, prevista no artigo 5º, inciso XII da Carta, só podem sofrer ingerências externas por meio de decisão judicial fundamentada, resguardando-se, assim, a dignidade e a privacidade dos indivíduos.

Diante disso, para compreender como a “conservação expedita” de dados se situa hierarquicamente em relação ao disposto no MCI, é fundamental localizar a Convenção de Budapeste na hierarquia normativa brasileira e discutir as implicações de sua aplicação no contexto interno.

Para tal, primeiramente é necessário lembrar que a Constituição Federal estabelece diferentes níveis de reconhecimento para os tratados internacionais, com base em sua natureza jurídica e no processo de incorporação ao ordenamento. Tratados que versam sobre direitos humanos podem adquirir status constitucional, caso sejam aprovados pelo Congresso Nacional em dois turnos, por três quintos dos votos, conforme artigo 5º, § 3º. Tratados de direitos humanos que não seguem esse rito possuem status supralegal, prevalecendo sobre leis ordinárias, mas subordinados à Constituição, como esclarecido no julgamento do RE 466.343/SP pelo STF.[145] Já tratados que não versam sobre direitos humanos são considerados normativamente equivalentes a leis ordinárias, como é o caso da Convenção de Budapeste.

Luiz Flávio Gomes e Valério de Oliveira Mazzuoli enfatizam que os tratados de direitos humanos, mesmo com status supralegal e força suficiente para invalidar normas infraconstitucionais conflitantes, são subordinados à Constituição Federal. Essa posição intermediária reflete o compromisso do Brasil com a proteção internacional dos direitos humanos e sua submissão à ordem constitucional interna.[146]

A Convenção de Budapeste, internalizada no Brasil por meio do Decreto Legislativo nº 37, de 16 de dezembro de 2021 e promulgada pelo Decreto nº 11.491, de 12 de abril de 2023 (como mencionado), por simplesmente não versar diretamente sobre direitos humanos, não foi aprovada pelo rito qualificado exigido para tratados que trazem essa temática). Assim, seu status no ordenamento jurídico brasileiro é legal, sendo equiparado às leis ordinárias, além de subordinado à Constituição.

---

[145] SUPREMO TRIBUNAL FEDERAL. **Recurso Extraordinário n.º 466.343/SP**. Relator Ministro Cezar Peluso. Julgado em 03 de dezembro de 2008.

[146] GOMES, Luiz Flávio; MAZZUOLI, Valerio de Oliveira. Tratados internacionais: valor legal, supralegal, constitucional ou supraconstitucional? **Revista de Direito**, v. XII, n. 15, 2009, p. 9.

Ainda que se entenda que o tratado ostenta caráter supralegal, por versar tangencialmente sobre direitos humanos, já que, de fato, contribui para persecução de graves crimes que atentam contra a pessoa, suas disposições não têm força suficiente para se sobrepor à Constituição Federal e às normas protetivas de direitos humanos que sejam mais benéficas. No caso, a prática de congelamento extrajudicial de dados de conteúdo, em especial comunicações privadas, fere as bases constitucionais e os limites previstos em instrumentos dirigidos aos direitos humanos.

Como exposto, é incontroverso que as comunicações privadas são invioláveis. Desse modo, na estrutura escalonada de proteção de dados, elas possuem sensibilidade máxima. Logo, a autorização para que autoridades requisitem sua preservação diretamente, sem supervisão judicial, viola diretamente o artigo 5º, inciso XII da Constituição, que assegura a inviolabilidade das comunicações privadas.

A inviolabilidade privada, como já se expôs, sofreu transformações com o surgimento das tecnologias que possibilitaram nova dinâmica comunicacional, completamente diferente daquela vivenciada em 1988, quando da idealização originária dessa garantia constitucional. Com a possibilidade de apreensão dos dados comunicacionais armazenados, sem que o titular tenha ciência dessa intervenção em sua esfera privada, surge uma dimensão de risco às garantias constitucionais, tanto da privacidade, quanto da própria dignidade da pessoa humana.

Nesse cenário, a autodeterminação informativa emerge como um princípio modernizador, adaptando a proteção à privacidade às demandas de uma sociedade hiperconectada. Esse direito assegura, aos indivíduos, o controle sobre a coleta, o uso e a disseminação de seus dados pessoais, conciliando a proteção da esfera privada com a fluidez e a interatividade das comunicações contemporâneas. Essas contrastam radicalmente com as realidades tradicionais de comunicação.

Nos moldes contemporâneos, o congelamento extrajudicial de dados comunicacionais, que estão fora do escopo permitido pelo MCI, representa lesão à autodeterminação informativa, um direito que, por força de mutação constitucional, passou a integrar as garantias fundamentais protegidas pela Constituição Federal.

Esse direito, fortemente vinculado à dignidade da pessoa humana, foi reforçado pela EC nº 115, que formalizou a proteção de dados pessoais no rol das garantias constitucionais. Tal avanço consolida a autonomia do indivíduo sobre suas informações, especialmente as que dizem respeito ao núcleo essencial da vida

privada. Evidencia a adaptação do texto constitucional às demandas da sociedade digital, reafirmando o compromisso com a proteção atual à privacidade.

Quanto ao ponto, é importante a referência à aplicação dessa garantia também no âmbito persecutório penal que, apesar de não contemplado pela legislação infraconstitucional, não passou despercebido à práxis jurídica. É o que se observa do que foi decidido pelo STF no bojo da ADI nº 6.529, de relato da Ministra Cármen Lúcia, Tribunal Pleno, julgado em 11/10/2021.[147]

A referida ADI foi julgada durante a vacância da LGPD, oportunidade na qual o STF reafirmou que a proteção de dados pessoais deve ser respeitada mesmo em atividades de inteligência. A decisão limitou o compartilhamento de dados do Sistema Brasileiro de Inteligência (Sisbin) com a Agência Brasileira de Inteligência (Abin) a casos de comprovado interesse público e motivação específica, vedando o compartilhamento com cláusula de reserva de jurisdição sem autorização judicial.

Esta decisão sinaliza uma tendência a aplicar os princípios da LGPD, também consolidados no texto constitucional, em atividades investigatórias e de inteligência, mesmo na ausência de uma legislação específica para esse campo. Em 15 de setembro de 2022, o STF reforçou que o compartilhamento de informações pessoais em atividades de inteligência deve observar a legislação específica e os parâmetros estabelecidos naquela ADI, respeitando os princípios gerais de proteção e direitos dos titulares previstos na LGPD, quando compatíveis com a função estatal.

Dessa forma, apesar de não haver legislação específica para atividades de inteligência, esses princípios devem ser observados pela Abin, especialmente em relação ao uso de *big data analytics* para a produção de inteligência aberta Open Source Intelligence (OSINT). A norma de direito fundamental possui aplicabilidade direta e eficácia plena, significando que a ausência de regulamentação infraconstitucional não pode impedir a aplicação dos princípios da LGPD, permitindo violações de direitos constitucionalmente previstos.

Esse paradigmático julgado revela que, muito embora a LGPD afaste de seu próprio escopo as atividades investigativas e as relativas à segurança pública, aos olhos jurisprudenciais, esse afastamento não deve se sustentar. Há uma clara tendência de se suprir a lacuna regulatória específica deixada pela LGPD, surpreendentemente, com os princípios da mesma LGPD, na qual a autodeterminação

[147] SUPREMO TRIBUNAL FEDERAL. **ADI 6529.**

informativa surge como fruto da dignidade humana e da privacidade, evitando que se violem essas garantias constitucionais.

É evidente que a observância dessas garantias na prática de atividades voltadas à segurança pública constitui um desafio abissal. Este desafio é amplificado pela ausência de legislação que verse, especificamente, sobre a nova realidade digital no âmbito persecutório penal. É incontroverso, contudo, que os limites constitucionais devem ser rigorosamente respeitados, de modo a assegurar a efetividade dos preceitos constitucionais também nesse âmbito, mesmo diante da necessidade de adaptações destinadas a ampliar sua aplicabilidade. A doutrina de Gomes e de Mazzouli reforça que, quando há conflito entre normas internacionais e nacionais, a aplicação do princípio internacional *pro homine* exige que se aplique sempre a norma mais favorável à proteção dos direitos humanos.[148]

Gomes e Mazzuoli explicam que essa técnica de assimilação dos tratados é essencial para preservar a supremacia da Constituição e para garantir que o sistema internacional de direitos humanos não seja utilizado para justificar retrocessos em garantias fundamentais.[149]

Assim, ainda que a Convenção de Budapeste pudesse ser interpretada como autorizando o congelamento extrajudicial, tal interpretação deve ser rejeitada em favor das garantias constitucionais brasileiras. É que o congelamento extrajudicial de dados de conteúdo representa uma ingerência indevida na esfera privada do indivíduo, mitigando, de maneira inaceitável, o poder de gerir suas informações e, portanto, tolhendo a autodeterminação informativa dos cidadãos

Ao se intentar a possibilidade de o usuário gerir dados de conteúdo de maneira apenas aparente, sem que as ações sejam efetivadas no servidores, para possibilitar uma vigilância estatal na vida privada com prazos alargados além dos razoavelmente legais, promove-se uma autodeterminação informativa de algibeira, uma ficção jurídica que serve apenas para sustentar um sistema penal. De modo reflexo, sustenta também um sistema democrático meramente semântico – em alusão à classificação de constituição semântica.[150]

---

[148] GOMES, Luiz Flávio; MAZZUOLI, Valerio de Oliveira. Tratados internacionais: valor legal, supralegal, constitucional ou supraconstitucional? **Revista de Direito**, v. XII, n. 15, 2009, p 12.
[149] Ibid.
[150] LOEWENSTEIN, Karl. **Teoría de la constitución.** Tradução Alfredo Gallego Anabitarte. Barcelona: Editorial Ariel, 1976, p. 57 – 61.

Essa situação representa uma grave distorção dos princípios fundamentais de um Estado de Direito, no qual a proteção da privacidade e a autodeterminação informativa devem ser autênticas e efetivas e não conceitos vazios e manipulados, para justificar práticas que, na essência, violam os direitos e garantias dos indivíduos.

Portanto, a tentativa de justificar o congelamento extrajudicial de dados de conteúdo, com fundamento na Convenção de Budapeste, é insustentável. A prática afronta a supremacia constitucional, comprometendo a proteção integral dos direitos fundamentais diante da nova realidade digital.

CONCLUSÃO

Como visto ao longo deste trabalho, a discussão vertida no HC 222.141/DF revela o embate entre dois pilares do Estado Democrático de Direito: a proteção dos direitos fundamentais, especialmente a privacidade e a autodeterminação informativa, e a eficácia da persecução penal na era digital.

O congelamento extrajudicial de dados, embora concebido como uma medida cautelar, transcende uma simples formalidade processual e adentra o campo da tutela de bens jurídicos fundamentais. É imperativo que sua aplicação seja guiada por critérios estritos de proporcionalidade e razoabilidade.

O estudo das legislações aplicáveis, especialmente o MCI e a Convenção de Budapeste, evidenciou a coexistência de normativos com enfoques distintos e, por vezes, conflitantes. O MCI adota uma abordagem hierarquizada de proteção, respeitando os diferentes graus de sensibilidade dos dados. Dados cadastrais, considerados de menor sensibilidade, podem ser acessados sem reserva de jurisdição, enquanto os dados de conexão e de acesso às aplicações exigem autorização judicial prévia. No topo dessa hierarquia, os dados de conteúdo – compreendidos como as comunicações propriamente ditas – recebem a mais elevada proteção, com inviolabilidade prevista no artigo 5º, XII da Constituição Federal.

A Convenção de Budapeste, por sua vez, amplia o escopo da preservação de informações, embora a expansão da medida seja voltada tão somente a orientar que os países signatários adotem práticas para tutela das provas digitais, sem impor categoricamente a flexibilização de direitos fundamentais consagrados no ordenamento interno.

A tentativa de incluir os dados de conteúdo no escopo de preservação extrajudicial afronta diretamente essa sistemática protetiva, rompendo com a lógica de proporcionalidade.

A decisão da 2ª Turma do STF no HC 222.141/DF, ao declarar nulas as provas obtidas por meio do congelamento extrajudicial de dados de conteúdo sem autorização judicial, representa um marco jurisprudencial na tutela dos direitos fundamentais frente às novas demandas da persecução penal. O voto condutor, ao enfatizar a ausência de previsão legal para a preservação de dados de conteúdo sem intervenção judicial, reafirmou a centralidade da reserva de jurisdição como barreira intransponível contra o arbítrio investigativo, adequando as garantias constitucionais

da vida privada e da dignidade humana à nova realidade por meio da autodeterminação informativa. Tal entendimento, ao harmonizar os princípios constitucionais com as peculiaridades do ambiente digital, reflete o necessário equilíbrio entre celeridade investigativa e proteção dos direitos individuais.

Contudo, a controvérsia analisada neste trabalho também expõe lacunas legislativas e operacionais. A ausência de uma regulamentação específica sobre o tratamento de dados no âmbito penal, especialmente diante das demandas introduzidas pela Convenção de Budapeste, dificulta a conformação de uma sistemática que alie eficiência investigativa à segurança jurídica.

A autodeterminação informativa, como princípio integrador emergente, exige que o indivíduo mantenha o controle sobre o uso de suas informações, mesmo em contextos de investigação criminal. Garante que as práticas estatais se mantenham dentro dos limites constitucionais, e embora supra, principiologicamente, a lacuna referida, a um só tempo demonstra a necessidade de normartização de procedimentos claros para efetivar o alcance das garantias constitucionais às novas demandas da persecução penal no século XXI hiperconectado.

A preservação extrajudicial de dados não deve ser instrumentalizada como um atalho investigativo em detrimento de garantias fundamentais. Ao contrário, seu uso legítimo depende de um modelo normativo, que estabeleça critérios claros e vinculativos, capazes de evitar interpretações expansivas que comprometam o núcleo essencial dos direitos constitucionais. O futuro dessa medida no Brasil depende de uma regulamentação que incorpore as demandas de um ambiente digital cada vez mais dinâmico, sem sacrificar os valores estruturantes do Estado de Direito.

Portanto, conclui-se que o congelamento extrajudicial de dados, como prática cautelar, tem relevância inquestionável na persecução penal contemporânea, mas deve ser aplicado nos termos e nas hipóteses estritas do MCI. Isso, porque esse regramento é harmônico em relação às recomendações da Convenção de Budapeste.

Apenas com o fortalecimento das garantias procedimentais e a observância estrita aos limites impostos pela Constituição, será possível consolidar um modelo investigativo que seja, ao mesmo tempo, eficaz e respeitoso frente à pessoa humana.

O caso do HC 222.141/DF destaca a urgência de soluções claras e céleres que permitam a coexistência equilibrada entre privacidade e segurança pública, resguardando os alicerces do Estado Democrático de Direito.

Por seu turno, a superveniência da Convenção de Budapeste, promulgada no Brasil em 2023, introduziu a figura da preservação expedita, permitindo a conservação de dados de tráfego e de conteúdo sem distinções detalhadas quanto ao impacto na privacidade. Essa ampliação, embora relevante no combate a crimes cibernéticos transnacionais, colide com os dispositivos nacionais ao desconsiderar a hierarquização de proteção e a necessidade de autorização judicial para dados sensíveis. Conforme sustenta Arabi[151], qualquer flexibilização de direitos fundamentais no contexto digital deve ser acompanhada de mecanismos rigorosos de supervisão e de controle, sob pena de comprometer os alicerces democráticos do ordenamento jurídico.

No caso do HC 222.141/DF, o STF reafirmou a inconstitucionalidade do congelamento extrajudicial de dados de conteúdo, destacando que sua aplicação extrapola os limites previstos no MCI e na própria Constituição. A decisão evidenciou que a preservação de dados, ainda que inicialmente precursora, não pode ser instrumentalizada como um atalho para burlar a reserva de jurisdição. A preservação da privacidade não é uma formalidade jurídica, mas um escudo contra o arbítrio do Estado, razão pela qual o núcleo essencial dos direitos fundamentais deve prevalecer mesmo diante das demandas investigativas mais urgentes.

Além disso, explorou-se como a ausência de regulamentação específica para provas digitais no Brasil contribui para a insegurança jurídica, agravada pelo conflito normativo entre o MCI e a Convenção de Budapeste. Nesse contexto, o princípio da autodeterminação informativa emerge como um elemento central, exigindo que o titular mantenha o controle sobre o uso de seus dados. A preservação extrajudicial de dados de conteúdo, ao retirar do indivíduo o poder de gestão sobre suas informações mais íntimas, configura uma afronta direta àquele princípio.

Portanto, entende-se que a admissibilidade do congelamento extrajudicial de dados de conteúdo é incompatível com o ordenamento jurídico brasileiro, tanto por desrespeitar a hierarquia protetiva estabelecida pelo MCI, quanto por violar os direitos fundamentais consagrados na Constituição. Ainda que a Convenção de Budapeste traga instrumentos importantes para a persecução penal, sua aplicação irrestrita no

[151] ARABI, Abhner Youssif Mota. Utilização de dados pessoais no combate ao crime organizado: limites e possibilidades de técnicas especiais de investigação em meio digital. **Revista Judicial Brasileira**, v. 2, n. 1, 2022. p. 39.

Brasil é inadequada, sendo necessário harmonizá-la em relação aos preceitos constitucionais de proporcionalidade e de reserva de jurisdição.

A decisão do STF no HC 222.141/DF não apenas representa um marco na proteção dos direitos fundamentais no ambiente digital, mas também destaca a necessidade urgente de avanços legislativos que contemplem as especificidades das provas digitais. A criação de normas claras e rigorosas, que equilibrem a eficácia investigativa e a preservação da dignidade humana, é imperativa para que o Estado enfrente os desafios da era digital sem comprometer os alicerces democráticos.

A exposição de todos esses pontos demonstra a incompatibilidade do congelamento extrajudicial de dados de conteúdo com o ordenamento jurídico brasileiro, por comprometer pilares essenciais do Estado Democrático de Direito, como a inviolabilidade da privacidade, dignidade humana e autodeterminação informativa.

Conclui-se, assim, que a proteção à privacidade e à autodeterminação informativa, longe de ser um obstáculo à persecução penal, é um baluarte indispensável para assegurar que a eficiência investigativa se desenvolva em conformidade com os valores e princípios do Estado Democrático de Direito.

REFERÊNCIAS

ALVES, Ana Abigail Costa Vasconcelos; MUNIZ, Antônio Walber Matias; CIDRÃO, Taís Vasconcelos. A oportuna e necessária aplicação do direito internacional nos ciberespaços: uma avaliação sobre a Convenção de Budapeste. FOMERCO – Fórum Universitário Mercosul, v. 1, n. 44, 2023. Disponível em: < http://www.congresso2017.fomerco.com.br/resources/anais/8/1507930824_ARQUIVO_FOMERCO%3BAOPORTUNAENECESSARIAAPLICACAODODIREITOINTERNACIONALNOSCIBERESPACOS.pdf>. Acesso em: 24 dez. 2024.

ARABI, Abhner Youssif Mota. Utilização de dados pessoais no combate ao crime organizado: limites e possibilidades de técnicas especiais de investigação em meio digital. **Revista Judicial Brasileira**, v. 2, n. 1, 2022.

ARAS, Vladimir Barros. A título de introdução: segurança pública e investigações criminais na era da proteção de dados. In: ARAS, Vladimir B.; MENDONÇA, Andrey B.; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno F. da; COSTA, Marcos Antônio da S. (Org.) **Proteção de Dados Pessoais e Investigação Criminal**. Ministério Público Federal. Brasília: ANPR, 2020.

ARAS, Vladimir. O congelamento de dados informáticos para fins de prova no processo. **Delictae Revista de Estudos Interdisciplinares sobre o Delito,** v. 8, n. 15, 2023.

BLEDLIN, Felipe. Análise da lei n. 12.654/2012, que prevê a identificação e a investigação criminal genética, à luz dos direitos fundamentais. In: ARAS, Vladimir B.; MENDONÇA, Andrey B.; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno F. da; COSTA, Marcos Antônio da S. (Org.) **Proteção de Dados Pessoais e Investigação Criminal**. Ministério Público Federal. Brasília: ANPR, 2020.

BORTOT, J. F. Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com Base nas Legislações Brasileira e Internacional. Belo Horizonte. **Virtuajus**, v. 2, n. 2, p. 338-362, 8 ago. 2017.

CASTELLS, Manuel. **A sociedade em rede: a era da informação, economia, sociedade e cultura**. 8. ed. São Paulo: Paz e Terra, 2005.

COELHO, Luiza Tângari. A proteção da intimidade na correspondência eletrônica: extensão da tutela da correspondência tradicional. Belo Horizonte. **Revista da Faculdade de Direito de Minas Gerais**, n. 61, p. 355-396, 2012.

COHEN, Julie. What is Privacy For. Nova York. *Harvard Law Review*, vol. 126, 2013.

CONVENÇÃO DE BUDAPESTE sobre Cibercrime. **Convenção sobre o Cibercrime.** Budapest, 23 de novembro de 2001. Disponível em: https://www.coe.int/. Acesso em: 10 jun. 2024.

CORTEZ, Raphaela Jéssica Reinaldo. **Prova digital no processo penal brasileiro: o uso de dados de geolocalização na segurança pública e na investigação**

criminal. Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2023.

COSTA JR., Ivan Jezler. **A busca por um marco processual da internet: requisitos para colheita dos dados armazenados em compartimentos eletrônicos**. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica do Rio Grande do Sul, Programa de Pós-Graduação em Ciências Criminais, Porto Alegre, 2018.

DUARTE, Ana Luísa Vieira. **Análise do encaixe da convenção de Budapeste no ordenamento jurídico brasileiro. 2022. 48 f. Trabalho de Conclusão de Curso (Bacharelado em Direito)** — Universidade de Brasília, Brasília, 2022.

FRAZÃO, Ana. Plataformas digitais, Big Data e riscos para os direitos da personalidade. In: TEPEDINO, Gustavo; MENEZES, Joyceane. (Org.) **Autonomia Privada, Liberdade Existencial e Direitos Fundamentais.** Belo Horizonte: Fórum, 2019.

FRAZÃO, Ana. Direitos básicos dos titulares de dados pessoais. **Revista do Advogado**, São Paulo, AASP, v. 39, n. 144, p. 33-46, dez. 2019. Disponível em: https://www.academia.edu/41202292/Direitos_b%C3%A1sicos_dos_titulares_de_dados_pessoais. Acesso em: 24 dez. 2024.

FREITAS, Elison A.; SILVA, Pedro Henrique Aguiar; SOUZA, Márcio Cabral de. Crimes cibernéticos: desafios da investigação e preservação das provas. **Facit Business and Technology Journal**, v. 1, n. 44, 2023, p. 178-194. Tocantins, 2023.

GOMES, Luiz Flávio; MAZZUOLI, Valerio de Oliveira. Tratados internacionais: valor legal, supralegal, constitucional ou supraconstitucional? **Revista de Direito,** v. 12, n. 15, 2009.

LEITE, George S.; LEMOS, Ronaldo. **Marco Civil Da Internet.** Rio de Janeiro: Atlas, 2014. *E-book.* p.323. Disponível em: https://integrada.minhabiblioteca.com.br/ Acesso em: 16 out. 2024. LEITE, George S.; LEMOS, Ronaldo. Marco Civil Da Internet. Rio de Janeiro: Atlas, 2014. E-book. p.323. Disponível em: https://integrada.minhabiblioteca.com.br/ Acesso em: 16 out. 2024.

LOEWENSTEIN, Karl. **Teoría de la constitución**. Tradução Alfredo Gallego Anabitarte. Barcelona: Editorial Ariel, 1976.

MACHADO, Pedro Antônio de Oliveira. Prefácio. In: ARAS, Vladimir B.; MENDONÇA, Andrey B.; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno F. da; COSTA, Marcos Antônio da S. (Org.) **Proteção de Dados Pessoais e Investigação Criminal**. Ministério Público Federal. Brasília: ANPR, 2020.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Pensar Revista de Ciências Júridicas Universidade de Fortaleza** (Unifor), Fortaleza, v. 25, n. 4, p. 1-18, 2020.

MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **RJLB,** ano, v. 5, p. 781-809, 2019.

PAESE SEGUNDO, Wilson Antonio. Aquisição de provas criminais eletrônicas no Brasil à luz da Convenção de Budapeste, do Cloud Act dos Estados Unidos da América e do Direito da União Europeia. **Galileu. Revista de Direito e Economia,** v. XXII, p. 65, 2022.

PEREIRA, Marcelo Cardoso. **Direito à Intimidade na Internet.** Curitiba: Juruá, 2011.

PONTE, A. Da necessidade de limites ao tratamento e compartilhamento de dados por órgãos de inteligência do Estado à luz da Lei Geral de Proteção de Dados em matéria penal. **Caderno Virtual**, [s.l.], v. 1, n. 54, 2022. Disponível em: https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/6481. Acesso em: 24 dez. 2024.

SARLET, Ingo Wolfgang. A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I. **Revista Consultor Jurídico,** v. 11, 2022.

SCHWAB, Klaus. **The fourth industrial revolution.** 1. ed. New York: Currency, 2017.

SMANIO, Gianluca Martins. A busca reversa por dados de localização na jurisprudência do Superior Tribunal de Justiça: análise crítica do RMS 61.302/RJ. **Revista Brasileira de Ciências Policiais**, v. 12, n. 5, p. 55-57, 2021,

SOLOVE, Daniel J. **Nothing to hide: the false tradeoff between privacy and security**. London: Yale University Press, 2011. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3976770. Acesso em 24 dez. 2024.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. A Convenção de Budapeste e as leis brasileiras. **Anais do 1° Seminário Cibercrime e Cooperação Penal Internacional**, 2009, p. 5. João Pessoa, maio de 2009. Disponível em: https:// www.academia.edu/ Acesso em: 17 out. 2024.

SOUZA, Wesley Wadim Passos Ferreira de. A Convenção de Budapeste e seus reflexos sobre a competência para o processo e julgamento dos crimes cibernéticos no Brasil. **Revista Judicial Brasileira,** v. 3, p. 39-68, 2023.

SUPREMO TRIBUNAL FEDERAL. **Habeas Corpus** n. 222.141/DF.

SUPREMO TRIBUNAL FEDERAL**. STF e proteção de dados pessoais: decisões da Corte marcaram a evolução de um novo direito fundamental**. Disponível em: https://noticias.stf.jus.br/. Acesso em: 24 dez. 2024.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo . **Estudos Avançados**, São Paulo, Brasil, v. 30, n. 86, p. 269–285, 2016. Disponível em: https://www.revistas.usp.br/eav/article/view/115093.. Acesso em: 24 dez. 2024.

TOSCHI, Aline Seabra; LOPES, Herbert Emílio Araújo. **Dados de tróia.** Proteção de dados pessoais e investigação criminal. p. 24. Brasília, 2020. Disponível em: http://www.anpr.org.br/ Acesso em: 24 dez. 2024.

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