

**UNIVERSIDADE FEDERAL DE JUIZ DE FORA**

***CAMPUS* GOVERNADOR VALADARES**

**CURSO DE DIREITO**

**PATRICK BERÇAN MONECCHI**

**PROCESSO PENAL NA ERA DIGITAL:**

**Uma análise de caso acerca da Controvérsia sobre a Autorização Judicial para  
Congelamento de Dados Telemáticos**

**Governador Valadares**

**2024**

**PATRICK BERÇAN MONECCHI**

**PROCESSO PENAL NA ERA DIGITAL:**  
**Uma análise de caso acerca da Controvérsia sobre a Autorização Judicial para**  
**Congelamento de Dados Telemáticos**

Artigo apresentado à Faculdade de Direito da Universidade Federal de Juiz de Fora Campus Governador Valadares, como requisito parcial para obtenção do grau de Bacharel. Na área de concentração Direito sob orientação do Prof. Dr. Daniel Nascimento Duarte.

**Governador Valadares**  
**2024**  
**PATRICK BERÇAN MONECCHI**

## **FOLHA DE APROVAÇÃO**

**PATRICK BERÇAN MONECCHI**

### **PROCESSO PENAL NA ERA DIGITAL:**

Uma análise de caso acerca da Controvérsia sobre a Autorização Judicial para Congelamento de Dados Telemáticos

Artigo apresentado à Faculdade de Direito da Universidade Federal de Juiz de Fora, Campus Governador Valadares, como requisito parcial para obtenção do grau de Bacharel. Na área de concentração Direito submetida à Banca Examinadora composta pelos membros:

---

Orientador: Prof. Dr. Daniel Nascimento Duarte

Universidade Federal de Juiz de Fora – UFJF/GV

---

Prof. Dr. João Guilherme Leal Roorda

Universidade Federal de Juiz de Fora – UFJF/GV

---

Prof. Dr. Guilherme Saraiva Brandão

Universidade Federal de Juiz de Fora – UFJF/GV

---

Ana Bárbara Canedo Oliveira

Ministério Público de Minas Gerais – MPMG

PARECER DA BANCA ( ) APROVADO ( ) REPROVADO

Governador Valadares, de de 2024.

## RESUMO

O presente trabalho tem como objetivo analisar a necessidade de autorização judicial para o congelamento de dados telemáticos no processo penal, com enfoque na aplicação do art. 13, §2º, e art. 15, §2º, ambos do Marco Civil da Internet. Adota-se como parâmetro a análise de caso concreto, com destaque para o Habeas Corpus nº 626.983 do STJ e o Habeas Corpus nº 222.141 do STF, que apresentam posicionamentos divergentes entre as duas cortes. A pesquisa, de caráter qualitativo e crítico, utiliza-se de fontes legais, doutrinárias e jurisprudenciais para investigar a pertinência da exigência de autorização judicial no congelamento de dados, com ênfase nos direitos fundamentais envolvidos. Conclui-se pela importância da reflexão sobre o equilíbrio entre a celeridade investigativa e a proteção dos direitos à privacidade e ao sigilo de comunicações no contexto do processo penal digital.

Palavras-chave: Processo penal, congelamento de dados telemáticos, autorização judicial, Marco Civil da Internet.

## SUMÁRIO

<b>Introdução.....</b>	<b>5</b>
<b>Capítulo 1: Sociedade em Rede e Processo Penal.....</b>	<b>5</b>
<b>1.1 A Sociedade em Rede e a Era da Informação.....</b>	<b>5</b>
<b>1.2 O Processo Penal na Era Digital.....</b>	<b>8</b>
<b>1.3 O Uso do Poder Disruptivo no Processo Penal.....</b>	<b>10</b>
<b>1.4 O Marco Civil da Internet.....</b>	<b>13</b>
<b>Capítulo 2: Necessidade ou desnecessidade de autorização judicial para o congelamento de dados telemáticos.....</b>	<b>14</b>
<b>2.1 O caso em tela .....</b>	<b>14</b>
<b>2.2 A Posição do STJ.....</b>	<b>15</b>
<b>2.3 A Posição do STF.....</b>	<b>17</b>
<b>2.3.1 O Julgamento Monocrático do STF.....</b>	<b>17</b>
<b>2.3.2 O Julgamento da Segunda Turma do STF.....</b>	<b>19</b>
<b>Capítulo 3: O Conflito de ideias.....</b>	<b>21</b>
<b>3.1 Divergência de Posicionamentos.....</b>	<b>21</b>
<b>3.2 Críticas.....</b>	<b>21</b>
<b>3.3 Os Dias Atuais e Futuros.....</b>	<b>24</b>
<b>Conclusão.....</b>	<b>25</b>

## **INTRODUÇÃO**

Este trabalho tem como objetivo discutir a necessidade ou não de autorização judicial para o congelamento de dados telemáticos no contexto do processo penal brasileiro, com base na Lei do Marco Civil da Internet – MCI. A era digital trouxe novos desafios para o processo penal, especialmente no que diz respeito à coleta e preservação de provas telemáticas, como e-mails, mensagens de texto e dados de geolocalização. O congelamento de tais dados, sem autorização judicial prévia, é um tema controverso, que envolve o conflito entre a celeridade investigativa e a proteção de direitos fundamentais, como a privacidade e o sigilo de comunicações. A análise deste tema é essencial para compreender os desdobramentos e os desafios jurídicos na sociedade digital, em que as fronteiras entre a privacidade e a eficiência estatal tornam-se cada vez mais tênues.

A metodologia empregada neste trabalho consiste em uma análise jurisprudencial detalhada de um caso concreto envolvendo divergências entre o Superior Tribunal de Justiça (STJ) e o Supremo Tribunal Federal (STF). A investigação centra-se em julgamentos importantes de dois *Habeas Corpus*, ambos do estado do Paraná. Através da análise dessas decisões, será possível examinar os principais argumentos apresentados por ambas as cortes, bem como as implicações práticas de cada posicionamento na condução das investigações criminais no ambiente digital.

Ao longo deste estudo, serão examinados os impactos dessas decisões na prática do processo penal e na proteção dos direitos dos investigados. Além de destacar os pontos de divergência entre as duas cortes, também serão propostas soluções para conciliar a eficiência investigativa com a proteção dos direitos fundamentais. O objetivo final é contribuir para uma compreensão mais profunda do tema e fomentar o debate sobre as melhores práticas na preservação de provas telemáticas no contexto jurídico atual.

## **CAPÍTULO 1: SOCIEDADE EM REDE E PROCESSO PENAL**

### **1.1 A Sociedade em Rede e a Era da Informação**

A grande revolução em nossa maneira de viver e comunicar nas últimas décadas tem sido possibilitada em grande parte pelo avanço das tecnologias. O crescente impacto e acesso às tecnologias digitais, como a internet, telefones celulares e redes sociais, transformou radicalmente não apenas a maneira como a comunicação é realizada, mas também a maneira

como o trabalho é feito, como consumimos, nos relacionamos e a maneira como experimentamos o mundo ao nosso redor. Essa revolução tecnológica basicamente mudou todos os elementos da rotina diária dos seres humanos e abriu um novo mundo de oportunidades, bem como de perigos, tanto para o próprio ser, quanto para as sociedades de maneira geral.

A Internet foi originalmente concebida como uma rede de comunicação e um sistema de troca de informações entre cientistas e instituições acadêmicas. No entanto, assim que a tecnologia se espalhou, ela imediatamente transcendeu sua aplicação primária, tornando-se a força onipresente que permeia todas as esferas da sociedade. A internet, juntamente com outras inovações tecnológicas, transformou o globo em uma enorme aldeia, na qual as barreiras geográficas se tornaram praticamente irrelevantes e onde a informação é transmitida instantaneamente para qualquer parte do mundo.

A internet modificou profundamente as dinâmicas sociais, econômicas, políticas e teve grande impacto no mundo jurídico. Esse fenômeno de alteração de estruturas fundamentais da sociedade é estudado por Manuel Castells, que o definiu como a “Sociedade em Rede”<sup>1</sup>.

Na sua definição de Sociedade em Rede, Castells diz que ela é uma nova forma de organização social em que a união das comunicações digitais em formato de uma enorme rede são o núcleo das interações humanas. Isso se difere das sociedades anteriores, em que era organizada burocraticamente em ambientes físicos e hierárquicos, sendo que a Sociedade em Rede é caracterizada pela flexibilidade, descentralização e conexão global. Nesse ponto, a informação passou a ser um fluxo contínuo que atravessa fronteiras geográficas e culturais, trazendo influência a todos os aspectos da nossa vida.

Essa nova organização social tem profundas implicações na maneira como interagimos e como as instituições operam. No contexto das interações pessoais, as redes sociais permitem que indivíduos de diferentes partes do mundo se conectem instantaneamente, compartilhando ideias, experiências e opiniões em tempo real. No entanto, essa conectividade global também cria novos desafios, como a disseminação de desinformação, a erosão da privacidade e o surgimento de novas formas de controle social.

Tais pontos são observados na medida em que empresas estritamente digitais, como a *Google*, *Facebook*, *Amazon*, dentre outras multibilionárias, comandam o mercado global nos pontos em que elas foram criadas. *Google* como principal ferramenta de pesquisa e

---

<sup>1</sup> Manuel Castells, *A Sociedade em Rede* (São Paulo: Paz e Terra, 2018).

disseminação de informações, *Facebook* como a principal rede social mundial, *Amazon* como a empresa on-line de maiores vendas de bens de consumo, por exemplo.

Essas empresas compartilham as informações obtidas por elas não de forma crua, mas processadas e disseminadas com outras empresas, que fomentam a formação da denominada Sociedade de Rede, na era em que Castells denominou de “capitalismo informacional”. Tal período é descrito por ele como sendo o período em que o capitalismo emergiu com o aparecimento das tecnologias de informação e comunicação.

Ao contrário do antigo capitalismo, em que a riqueza era gerada principalmente pela produção industrial ou agrícola, o capitalismo informacional baseia-se na produção e manipulação de conhecimento e informação, fazendo com que a informação se torne o principal recurso econômico, assim como a capacidade de processar, armazenar e distribuir informações se torna crucial para a criação de valor e poder no mundo contemporâneo.

Nesse sentido, empresas como as supracitadas são capazes de alterar significativamente as dinâmicas econômicas e sociais, influenciando comportamentos de consumo, padrões culturais e até processos políticos. O poder dessas corporações vai além do domínio econômico; elas detêm controle sobre vastas quantidades de dados pessoais, que são utilizados para personalizar serviços, direcionar publicidade e até moldar a opinião pública, como analisa Castells. Ao controlar os fluxos de informação e moldar as interações digitais, essas empresas exercem um poder imenso sobre a sociedade, capaz de redefinir normas, influenciar legislações e, em última instância, alterar o próprio tecido social, criando uma nova realidade onde as fronteiras entre o público e o privado, o local e o global, se tornam cada vez mais nebulosas.

Esse poder crescente das corporações digitais também desafia as estruturas jurídicas tradicionais, que precisam se adaptar rapidamente a esse novo cenário.

A regulamentação do uso de dados, a proteção da privacidade e a garantia de direitos fundamentais, como a liberdade de expressão e o devido processo legal, tornam-se algumas das questões na Sociedade em Rede, que foi exposta por Castells ainda no ano de 1999, enquanto a internet engatinhava, gerando discussões complexas hodiernamente.

As legislações que outrora eram suficientes para regular a vida em sociedades físicas, baseadas em fronteiras territoriais claras, hoje se mostram inadequadas para lidar com o fluxo constante e transnacional de informações. Isso exige do Estado um esforço contínuo de adaptação de suas leis, além da cooperação internacional para enfrentar os desafios impostos pela globalização digital. Ao mesmo tempo, a crescente dependência da sociedade em relação às grandes plataformas digitais cria um novo tipo de vulnerabilidade, em que o poder de



decisão de poucas empresas pode impactar diretamente os direitos e liberdades individuais de milhões de pessoas ao redor do mundo.

## **1.2 O Processo Penal na Era Digital**

A ascensão da era digital trouxe consigo uma série de desafios e oportunidades para o sistema jurídico, especialmente no âmbito do processo penal. O avanço das tecnologias de comunicação e o surgimento das redes digitais remodelaram a maneira como as investigações criminais são conduzidas, como as provas são coletadas e como os julgamentos são realizados. A digitalização da sociedade não apenas facilitou o acesso à informação e à comunicação em tempo real, mas também transformou a própria natureza das evidências utilizadas no processo penal.

Tradicionalmente, o processo penal baseava-se em provas físicas e testemunhais, como documentos escritos, depoimentos orais e objetos materiais. No entanto, com o advento da era digital, novas formas de prova surgiram, como registros eletrônicos, e-mails, mensagens de texto, dados de geolocalização e interações em redes sociais. Esses dados telemáticos, por sua natureza digital, são efêmeros e podem ser rapidamente alterados ou destruídos, o que levanta questões significativas sobre sua preservação e autenticidade. Além disso, a facilidade com que as informações podem ser disseminadas na era digital também cria desafios em termos de jurisdição e aplicabilidade das leis.

Crimes como fraude eletrônica, crimes cibernéticos e a disseminação de conteúdo ilegal ocorrem frequentemente em um ambiente transnacional, onde os perpetradores, as vítimas e os servidores que hospedam os dados estão localizados em diferentes países. Isso requer uma cooperação internacional robusta e a adaptação das normas processuais para lidar com a natureza global desses crimes. A crescente complexidade dos casos criminais na era digital destaca a necessidade de uma colaboração mais estreita entre as autoridades de diferentes países, além de uma atualização contínua das leis para que estas acompanhem o ritmo das inovações tecnológicas.

Outro aspecto crucial do processo penal na era digital é o impacto das novas tecnologias na privacidade e nos direitos individuais. A capacidade de monitorar e coletar dados em larga escala, muitas vezes sem o conhecimento ou o consentimento dos indivíduos, coloca em risco direitos fundamentais, como o direito à privacidade e o sigilo de comunicações.

Portanto, a necessidade de equilibrar a eficácia das investigações criminais com a proteção dos direitos dos cidadãos é uma das principais questões que o sistema de justiça enfrenta atualmente, exigindo uma revisão constante das práticas investigativas e das normas legais, mesmo que por entendimentos jurisprudenciais, como será discutido.

Nesse contexto histórico, o Direito, que era a ferramenta máxima de força impositiva e coercitiva que o Estado detinha, acaba perdendo força com a chegada do capitalismo informacional, dando involuntariamente espaço à Internet, que a cada dia ganha mais força e mais poder pelas suas ferramentas mais tecnológicas e superiores às ferramentas do Direito.

No mesmo sentido, os autores Daniel Nascimento Duarte e Antônio Santoro, no artigo “Gestão Diferencial dos Ilegalismos no Processo Penal na Era da Sociedade Digital” abordam que:

“O surgimento sempre forjado dessa formação de conhecimento permitiu e precedeu momentos pontuais nos caminhos meticulosos do controle social. Atualmente, com a evolução tecnológica, há um afastamento das instâncias jurídicas no que toca ao conhecimento científico de cariz digital o que tem provocado, em grau de consequência, certos desafios para se repetir o controle social seguro tal qual nos tempos das instituições tradicionais de vigilância.”<sup>2</sup>

Portanto, há uma dificuldade do Estado de equiparar ou superar a força da Internet de forma pacífica e sem infringir direitos fundamentais. Essa complexidade se manifesta em vários aspectos. Primeiramente, a Internet é uma plataforma altamente descentralizada e de alcance global, o que dificulta o controle estatal sobre as informações e as interações que ocorrem em seu âmbito. Tentativas de regulamentar ou monitorar atividades online frequentemente esbarram em questões relacionadas à liberdade de expressão, privacidade e o direito à informação, que são pilares dos direitos humanos.

Além disso, a rapidez com que as informações se disseminam na rede torna o controle estatal ainda mais desafiador. Qualquer medida restritiva imposta pelo Estado pode ser facilmente contornada por meio de ferramentas tecnológicas como VPNs (redes privadas virtuais), criptografia e navegadores anônimos, dificultando ainda mais a aplicação efetiva das leis no ambiente digital.

Isso cria um dilema para o Estado, que precisa proteger a segurança pública e a ordem jurídica sem sacrificar as liberdades individuais e, principalmente, os direitos fundamentais, como aquele presente no artigo 5º, inciso XII, da Constituição Federal: *“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*

---

<sup>2</sup> Duarte e Santoro, “Gestão Diferencial dos Ilegalismos no Processo Penal na Era da Sociedade Digital (São Paulo: Ed. RT, 2021) p. 25.

que a lei estabelecer para fins de investigação criminal ou instrução processual penal.”, e o inciso LXXIX: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”, que são os pontos-chave da discussão deste texto.

Outro ponto de dificuldade reside no fato de que a Internet é um espaço de inovação constante, com novas tecnologias e plataformas surgindo a todo momento. A legislação, por sua natureza, é mais lenta e reativa, o que significa que muitas vezes as normas jurídicas não conseguem acompanhar o ritmo das mudanças tecnológicas. Isso pode levar a situações em que as leis se tornam obsoletas ou inadequadas para regular as novas realidades digitais face à diminuição do poder inquisitório estatal.

Dessa forma, qualquer tentativa de intervenção estatal na Internet pode gerar uma reação negativa da sociedade civil e de organizações internacionais, que veem tais ações como uma forma de censura ou de controle autoritário. Essa resistência pode minar a legitimidade das ações do Estado e provocar um conflito entre a necessidade de regulamentação e a proteção das liberdades fundamentais, complicando ainda mais a tarefa de encontrar um equilíbrio entre segurança e liberdade no ambiente digital.

### **1.3 O Uso do Poder Disruptivo no Processo Penal**

O poder disruptivo no processo penal refere-se à capacidade de inovações tecnológicas e metodológicas de modificar as práticas tradicionais de investigação, coleta de provas e julgamento dentro do sistema de justiça criminal, a fim de tornar páreo com o poder que a Internet vem ganhando. De outro modo, é o Estado inovando em suas armas para que elas não se tornem obsoletas se comparadas às da Internet.

O avanço de tecnologias como inteligência artificial, *big data*, vigilância digital e *blockchain* estão provocando transformações significativas no processo penal, forçando uma reavaliação das práticas e das normas jurídicas tradicionais. Essas inovações, ao mesmo tempo em que introduzem novas possibilidades para as investigações criminais, como a análise preditiva de comportamentos e a conservação de provas digitais, também levantam preocupações importantes sobre a garantia dos direitos fundamentais. Entre as questões mais sensíveis estão a proteção da privacidade, o respeito ao devido processo legal e a manutenção da equidade na administração da justiça.

Dito isso, o poder disruptivo no processo penal não só redefine as capacidades do Estado na investigação e punição de crimes, mas também impõe a necessidade de um equilíbrio cuidadoso entre inovação tecnológica e a preservação dos princípios essenciais de

justiça e direitos fundamentais, que poderá vir, muitas das vezes, através de um desafio de limiar tênue.

Assim, como explicam Duarte e Santoro, o Poder Judiciário tenta equilibrar a relação de controle que outrora era indiscutivelmente superior ao controle da Internet, mas que hoje nem tanto. Ora, se o Estado, neste período, é incapaz de sequer compreender as milhares de novas tecnologias que surgem da Internet rapidamente, ele parte para o caminho mais fácil de controle, aqueles métodos já conhecidos e tradicionais de exalar poder, que geram uma característica ainda mais impositiva, coercitiva e inquisitiva do Estado.

Já que, se não posso com eles, e também não posso me juntar a eles, vou superar esse jogo de poder através dos meios clássicos e imperativos. Dessa forma, os ilegalismos no processo penal<sup>3</sup> apontados pelos autores tornam-se cada vez mais evidentes ao passo que surgem mais evoluções tecnológicas em velocidade incompatível com a velocidade de raciocínio e resposta estatal.

Vêm acontecendo diversos fatos em que o Direito não tem armas suficientes para lidar com o tamanho da Internet, fazendo com que o Poder Judiciário utilize de forças coercitivas extremas para conter as irregularidades. O exemplo mais hodierno é o caso da rede social X (antigo Twitter)<sup>4</sup>.

O X foi completamente banido do território brasileiro, por meio de determinação judicial às empresas provedoras de Internet, obrigando-as a bloquearem os endereços dos sites do X (x.com; etc.), fazendo com que nenhum usuário possa acessar essa rede social, nem mesmo por aplicativo em smartphones, tablets, smart tvs, etc.

O X, comprado pelo bilionário Elon Musk na metade de 2022, foi palco de discursos de ódio e propagação de *fake news* de cunho eleitoral. Tais ações foram intensificadas após os atos antidemocráticos de 8 de janeiro de 2023, em que Elon Musk descumpriu as ordens judiciais do STF de restringir os perfis de usuários que disseminavam discursos de ódio, *fake news* e instigavam os atos antidemocráticos.

Após tantos descumprimentos de decisões judiciais, unido ao fato de que Elon Musk retirou a sua sede do X no Brasil e deixou sem representante legal, o Ministro Presidente do

---

<sup>3</sup> “Conjuntura de microrrelações de poder protagonizadas cooperativamente pelos atores ligados à uma persecução penal a partir de cotidiano exercício de decisões políticas que são permitidas por um saber que se exterioriza na construção de sentido da normatividade processual penal que se exterioriza na construção de sentido da normatividade processual penal direcionada ao caso”(Duarte e Santoro, Gestão Diferencial, p. 40).

<sup>4</sup> BATAIER, Caroline. Do Twitter ao fim do X: entenda os capítulos que levaram à decisão de derrubar a rede social no Brasil. Brasil de Fato, 30 ago. 2024. Disponível em: <https://www.brasildefato.com.br/2024/08/30/do-twitter-ao-fim-do-x-entenda-os-capitulos-que-levaram-a-decisao-de-derrubar-a-rede-social-no-brasil>. Acesso em: 27 ago. 2024.

STF Alexandre de Moraes ordenou que a rede social seja banida por completo do território nacional.

Essa medida é um exemplo claro de como o Direito está perdendo seu caráter regulatório face ao avanço da Internet, sendo obrigado a usar medidas bem mais restritivas para superar as forças digitais.

Portanto, essa estratégia é reativa e, na maioria dos casos, ineficaz, pois não pode superar a evolução da tecnologia e, em alguns cenários, até viola direitos humanos básicos, como o direito à privacidade e à liberdade.

Um dos exemplos que o Estado está usando o poder disruptivo no processo penal para se equiparar à força da Internet é a implementação dos Núcleos da Justiça 4.0<sup>5</sup>, que promete utilizar novas tecnologias para favorecer a população, inclusive com o uso de inteligências artificiais. Esse sistema possibilita um trabalho comunicativo, cooperativo e em rede com o Sistema Judiciário Brasileiro, exatamente a mesma ideia propagada por Castells, na medida em que a Sociedade em Rede passa a ser impulsionada por criações do Judiciário.

Ainda, o Marco Civil da Internet, Lei promulgada em 2014, trouxe diversas regulações, que, à época, foram duramente criticadas pela população. Tais críticas giravam principalmente em torno da percepção de que a lei poderia limitar a liberdade de expressão, aumentar a censura na internet e criar obstáculos para a inovação tecnológica no Brasil.

Muitos usuários temiam que as regulamentações impostas pelo Marco Civil pudessem resultar em uma vigilância excessiva por parte do Estado e das empresas, comprometendo a privacidade dos cidadãos e a neutralidade da rede, como criticado amplamente à época por internautas e autores como Antônio Nogueira<sup>6</sup>, que explora as reações da sociedade civil à promulgação do Marco Civil da Internet, revelando os medos iniciais sobre as possíveis consequências negativas da lei ainda no ano de 2015, destacando a diminuição da privacidade e sigilo.

Tais críticas fazem referência ao receio que o cidadão brasileiro tem contra o poder estatal, que cresce cada vez mais para se igualar ao poder da internet. Sendo assim, o Marco Civil da Internet representou não apenas uma tentativa de regular o uso da internet, mas também se tornou um símbolo do embate entre o avanço tecnológico e a desconfiança popular frente ao aumento do controle estatal. Alguns desses medos foram, no entanto, com o tempo até agora amenizados pela aplicação efetiva da Lei, que consolidou ainda mais a neutralidade

---

<sup>5</sup> Os Núcleos de Justiça 4.0: inovação disruptiva no Poder Judiciário brasileiro.

<sup>6</sup> O Marco Civil da Internet e as Reações da Sociedade Civil: Entre o Temor e a Esperança.

da rede, bem como trouxe avanços substanciais na responsabilização dos provedores de serviços de Internet.

#### **1.4 O Marco Civil da Internet**

A Lei 12.965/14, que ganhou o nome de Marco Civil da Internet, foi o pontapé inicial da regulação estatal sobre a Internet, que gerou deveres às empresas provedoras de internet, mas, ao mesmo tempo, enorme responsabilidade para a interpretação de seus dispositivos. Eis o que diz o Artigo 13, da Lei nº 12.965/14:

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.

§ 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.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

No Brasil, a aplicação do Marco Civil da Internet e a interpretação de seu artigo 13, § 2º, que trata da preservação e acesso a dados telemáticos, refletem os desafios que foram estampados. O grande debate deste texto é sobre a necessidade ou não de autorização judicial para o congelamento de provas digitais, que é um exemplo de como a era digital exige uma reinterpretção das normas jurídicas existentes.

Enquanto o STJ e o STF apresentam entendimentos divergentes sobre a necessidade de autorização judicial, a discussão revela a complexidade de adaptar o processo penal a uma realidade em que a informação é fluida e global, na qual os limites entre privacidade e segurança se tornam cada vez mais difusos e a Internet vem ganhando cada vez mais força impositiva que o Direito, que acaba por ter que recorrer a inovações jurídicas e, às vezes, sobrepor direitos fundamentais na tentativa de se tornar uma força maior que a internet.

Tal discussão ganha mais importância no cenário jurídico atual, porquanto, embora haja o desentendimento das turmas, a questão não foi julgada pelo Plenário do Supremo.

## **CAPÍTULO 2: NECESSIDADE OU DESNECESSIDADE DE AUTORIZAÇÃO JUDICIAL PARA O CONGELAMENTO DE DADOS TELEMÁTICOS**

### **2.1 O caso em tela**

O que motivou a discussão deste texto é a investigação da empresa INFOSOLO INFORMÁTICA S.A, que supostamente teria indevidamente se beneficiado em milhões de reais de irregularidades no processo do Edital de Credenciamento nº 001/2018 do Detran do Estado do Paraná. O teor das investigações contém crimes como organização criminosa, falsidade ideológica, abuso de poder econômico e delitos previstos na Lei nº 8.666/93.

O Ministério Público do Estado do Paraná (MPPR), com atuação do GAECO (Grupo de Atuação Especial de Repressão ao Crime Organizado), requereu ao Diretor da APPLE Computer Brasil e ao GOOGLE DO BRASIL a identificação das contas dos investigados – sócios da empresa – e a subsequente preservação de dados e IMEI coletados a partir das contas de usuários vinculados, tais como dados cadastrais, histórico de pesquisa, o conteúdo de *e-mails* e *Imessages*, fotos, contatos e histórico de localização, desde 1/6/2017.

Tal pedido foi impetrado às empresas de internet dia 22/11/2019 e, na sequência, o MPPR requereu a quebra de sigilo de tais dados telemáticos em 29/11/2019, sendo deferido brevemente em 3/12/2019 pelo Juízo de primeiro grau.

Os argumentos utilizados pelo MPPR tanto para o pedido de preservação dos dados às empresas, quanto para o requerimento da quebra de sigilo judicial, são que os sócios da empresa INFOSOLO INFORMÁTICA S.A. ordenaram as imediatas transferências dos valores ilícitos para contas particulares e de suas holdings, impossibilitando a recuperação de ativos. Além disso, utilizaram interpostas pessoas para apresentar denúncias contra empresas concorrentes, atacar pessoas do Poder Executivo e responsáveis pelo DETRAN/PR. Ademais, intimidaram testemunha ouvida pelo Ministério Público. Em arremate, possuem vínculos com países estrangeiros e dispõem de jatos particulares, configurando concreta possibilidade de fuga. Aduziram, ainda, que há elementos que indicam destruição de provas após a primeira busca e apreensão e vínculo de vários dos denunciados com o Poder Político local.

Os investigados, então, requereram que seja decretada a nulidade das provas obtidas através dessa quebra de sigilo de dados telemáticos, tendo em vista que o MPPR atropelou

princípio da jurisdicionalidade ao requerer aos provedores de internet a preservação do conteúdo de comunicações telemáticas, sem autorização judicial.

Ou seja, os impetrantes não questionaram a legitimidade da quebra de sigilo dos dados telemáticos deferida pelo Juízo de primeiro grau, mas sim o congelamento desses dados a requerimento do MPPR diretamente feito às empresas provedoras de internet, sem passar pelo âmbito judicial.

Tal argumento é baseado no impedimento do controle da peticionária (Raquel Amaral Cardoso, sócia da INFOSOLO INFORMÁTICA S.A.) sobre suas informações, em afronta ao direito à privacidade.

Então, o Tribunal estadual decidiu rejeitar o pedido de nulidade das provas, argumentando que, como nenhum direito é absoluto por si só, limitações podem ser aplicadas, tomando conhecimento do bem comunitário ou coletivo juntamente com outros direitos individuais protegidos pela Constituição e, neste caso, tem como ponto de inflexão as garantias humanas intrínsecas de liberdade, uma vez que não operam como proteção à prática de condutas ilícitas. Quando há confronto entre dois ou mais direitos ou garantias fundamentais, a harmonia deve ser concedida pelo intérprete entre os interesses jurídicos em conflito, de modo a permitir a compatibilidade e equilibrá-los sem sacrificar completamente uns em relação aos outros.

Desse modo, o congelamento dos dados telemáticos é “verdadeira medida cautelar” que infringe os direitos de privacidade e intimidade ao extrapolar os limites da legislação de proteção geral de dados e do Marco Civil da Internet ou não? O polo passivo do caso impetrou *Habeas Corpus* para sanar tal problema.

## **2.2 A Posição do STJ**

O Superior Tribunal de Justiça – STJ –, ao analisar o *Habeas Corpus* N° 626.983 - PR<sup>7</sup>, por unanimidade, concordou com os argumentos do Tribunal Estadual do Paraná no sentido de que o MPPR em nada ultrapassou os limites de privacidade e intimidade ao requisitar diretamente às empresas provedoras de Internet – *Google e Apple* – que segurassem e congelassem por tempo superior aos previstos na Lei n° 12.965/2014, porquanto estão previstos em lei os pedidos impetrados pelo MPPR.

---

<sup>7</sup> STJ – Superior Tribunal de Justiça. HC 626.983, PR, Rel. Min. Olindo Menezes, julgado em 22 fev. 2022, Diário de Justiça Eletrônico, 25 fev. 2022. Disponível em: <http://www.stj.jus.br>. Acesso em: 30 jul. 2024.



A sexta turma do STJ argumenta que é de extrema importância a preservação de tais dados pela volatilidade deles, que podem ser destruídos ou alterados a qualquer instante pelos donatários. E, pelos argumentos de que nenhuma liberdade é absoluta, o Ministro Relator Olindo Menezes bate na tecla que a Autoridade Policial e o Ministério Público, pelos seus caracteres investigativos, podem requerer aos provedores de Internet a preservação cautelar de registros de acessos à internet e registros de aplicações de internet, conforme a letra da Lei especificada nos artigos 13, § 2º, e artigo 15, §2º<sup>8</sup>, ambos da Lei nº 12.965/14.

Ou seja, quem requer alguma, pode tê-la deferida ou não, e, nessa situação, mesmo com o uso do termo “cauteladamente” dito e a solicitação judicial de acesso no prazo de 60 dias contados do pedido administrativo, tanto o administrador do sistema autônomo quanto o provedor da aplicação de internet teriam que responder à polícia, autoridade administrativa ou Ministério Público a sua demanda, garantindo que os registros sejam guardados por maior prazo.

Dessa forma, o Ministro Olindo Menezes diz que o pedido de congelamento feito pelo MPPR não precisa necessariamente de autorização judicial para ser atendido pelo provedor de Internet, fazendo deste o ponto nodal da discussão.

Um ponto de destaque na argumentação da ré é que o que está descrito no artigo 13, § 2º e artigo 15, § 2º do Marco Civil da Internet permite a autoridade policial, administrativa ou o Ministério Público a preservação de “registros de conexão” e “registros de acesso a aplicações” e que tais termos estão explicados no próprio MCI, em seu artigo 5º: “Para os efeitos desta Lei, considera-se (...):

VI - registro de conexão: 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;

VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.(...)”

Nesse sentido, a ré sustenta que os dados que foram requisitados pelo MPPR para serem congelados ultrapassam os limites da Lei, já que os dados que foram guardados são diversos daqueles taxados nos artigos supracitados, como *e-mails*, dados de geolocalização, histórico de pesquisa, dados cadastrais, entre outros.

---

<sup>8</sup> Art. 15: O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.(...) §2º:A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no *caput*, observado o disposto nos §§ 3º e 4º do art. 13.

Dessa forma, a parte ré teve seus direitos de privacidade infringidos e acesso aos próprios dados negados, pela medida restritiva imposta pelo MPPR para que as empresas provedoras de internet congelassem tais dados.

O Ministro Olindo Menezes expõe seus contra argumentos dizendo que a medida imposta foi de extrema importância no caso em tela, já que as informações congeladas são muito voláteis – justamente por serem completamente digitais – e que os outros investigados poderiam trocar informações de cunho relevante no deslinde das investigações.

Ademais, o Ministro mostra a explicação de Victor Auilo Haikal, especialista em Direito Digital e Segurança da Informação sobre o termo “aplicações da internet”, que são: *“Os serviços oferecidos na grande rede. Portais de conteúdo, plataformas de mídias sociais, microblogs, comunicadores instantâneos, e-mails, blogs e tantas outras modalidades de disponibilização de facilidades na rede estão enquadrados nessa categoria.”*<sup>9</sup>

Todos os Ministros votaram com o Relator e, em sequência, o Ministro Sebastião Reis Júnior acrescentou que melhor decisão tangencia os órgãos de persecução penal e o Ministério Público. Por isso, os dispositivos do artigo 13, § 2º e artigo 15, § 2º do Marco Civil da Internet são de rol exemplificativo, porquanto presente a hipótese de interpretação extensiva.

Destarte, o STJ deu razão ao MPPR, traduzindo justamente um exemplo de uso do poder disruptivo que é necessário ser aplicado no presente caso devido às suas peculiaridades, como a forma que as informações 100% digitais podem se propagar, serem modificadas e serem excluídas em apenas alguns cliques.

Fez-se necessário o uso de tal força para se fazer mais potente que as tecnologias atuais e tornar mais eficiente o acesso aos dados, tendo em vista que, normalmente, são de difícil realização em ambientes eletrônicos.

## **2.3 A Posição do STF**

É neste ponto que começam os argumentos e decisões contrários aos anteriores, como será evidenciado.

### **2.3.1 O Julgamento Monocrático do STF**

---

<sup>9</sup> HAIKAL, V. A. Da significação jurídica dos conceitos integrantes do art. 5º: internet, terminal(...). *Marco civil da internet*. (1. ed. São Paulo: Atlas, 2014), p. 315-345.

O Ministro Relator do STF Ricardo Lewandowski, ao julgar o *Habeas Corpus*<sup>10</sup> impetrado pela ré após a ordem denegada do STJ, manifestou-se de forma completamente contrária à corte inferior, na forma de decisão monocrática.

O Ministro Ricardo Lewandowski argumentou utilizando os princípios fundamentais contidos no art 5º, inciso XII, da CF, que protege os sigilos das comunicações em fluxo, como troca de dados e mensagens e o inciso X do mesmo artigo sobre direito à privacidade.

Segundo o Ministro, o pedido do MPPR do congelamento dos dados telemáticos, ou seja, a indisponibilidade dos próprios dados da ré, são imprescindíveis de autorização judicial, pois viola os direitos constitucionais supracitados.

Ainda, Lewandowski levou à risca a interpretação da letra da lei, já que, para que não houvesse a nulidade, o MPPR poderia requisitar o congelamento apenas do 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 (art. 5º, VI, MCI) e os registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP (art. 5º, VIII, MCI), que são justamente os registros de conexão e registros de acesso a aplicações da internet, respectivamente – dados em que seu congelamento pode ser requisitado direto às empresas provedoras de internet, sem autorização judicial.

Dessa forma, observa-se que o MPPR, ao solicitar *e-mails*, dados do *iMessages*, dados de geolocalização, dentre outros, ultrapassou os limites do que o legislador impôs no Marco Civil da Internet, pois, ao serem congelados, impossibilitou que a ré tenha acesso aos próprios dados antes de haver uma autorização judicial, quebrando os princípios fundamentais.

Na mesma linha, o Ministro Edson Fachin, em julgamento do ADPF 403/DF, enfatizou que o princípio à privacidade também é o direito de manter controle sobre suas próprias informações e determinar a forma em que é construída sua imagem pública.<sup>11</sup>

O principal ponto de argumentação de Lewandowski é a falta de previsão legal para atos como os feitos pelo MPPR, levando a uma interpretação ampliativa da Lei exercida pela autoridade policial ou administrativa e pelo Ministério Público. Nesse ponto, o Ministro

---

<sup>10</sup> BRASIL. STF – Supremo Tribunal Federal. HC 222.141, PR, Rel. Min. Ricardo Lewandowski, julgado em 1º dez. 2022, Diário de Justiça Eletrônico, 8 dez. 2022. Disponível em: <http://www.stf.jus.br>. Acesso em: 20 jul. 2024.

<sup>11</sup> BRASIL. STF – Supremo Tribunal Federal. ADPF 403, DF, Rel. Min. Edson Fachin, julgado em 20 mar. 2019, Diário de Justiça Eletrônico, 9 maio 2019. Disponível em: <http://www.stf.jus.br>. Acesso em: 20 jul. 2024.

defende que deve haver um freio nesse comportamento estatal de interferência nos domínios da internet.

Portanto, o Ministério Público do Estado do Paraná não observou a reserva jurisdicional necessária à ordem de indisponibilidade do conteúdo telemático por seu legítimo titular, contrariando no modo acima indicado a Constituição Federal e o Marco Civil da Internet, pois decretou verdadeira medida cautelar ao determinar, por vontade própria, o “congelamento” de todo o conteúdo das comunicações telemáticas de um paciente. Em suma, retirou de seu legítimo titular o direito de dispor do conteúdo de seus dados para quaisquer fins, sem qualquer autorização judicial para tanto.

Por tudo o exposto, monocraticamente, o Ministro do STF Ricardo Lewandowski decidiu por dar razão à parte ré e considerar a nulidade do congelamento dos dados requisitados pelo MPPR sem a devida autorização judicial, bem como todas as provas decorrentes deste ato.

### 2.3.2 O Julgamento da Segunda Turma do STF

O Agravo Regimental no *Habeas Corpus* 222.141<sup>12</sup> foi interposto pelo Ministério Público Federal e o Ministério Público do Paraná contra a decisão do Ministro Ricardo Lewandowski, que declarou nulas as provas obtidas a partir do congelamento de dados telemáticos de uma investigada sem autorização judicial. O MPPR argumentou que o pedido de congelamento era legal, conforme o artigo 13, § 2º do Marco Civil da Internet, que permite o congelamento de dados de conexão sem autorização judicial, desde que o pedido de acesso seja submetido à autorização judicial dentro de 60 dias. No entanto, o pedido do Ministério Público envolvia o congelamento de um conjunto mais amplo de dados, incluindo comunicações privadas, o que, segundo o STF, exigiria prévia autorização judicial.

Então, a decisão colegiada da Segunda Turma do STF, também com o Ministro Relator Ricardo Lewandowski, manteve os mesmos argumentos utilizados na decisão monocrática e, por maioria, a Turma não deu provimento ao recurso ministerial. Votaram com o relator os Ministros Gilmar Mendes e Nunes Marques.

---

<sup>12</sup> BRASIL. STF – Supremo Tribunal Federal. Ag.Reg. no HC 222.141, PR, Rel. Min. Ricardo Lewandowski, julgado em 6 fev. 2024, Diário de Justiça Eletrônico, 8 fev. 2024. Disponível em: <http://www.stf.jus.br>. Acesso em: 30 jul. 2024.

Entretanto, houve discordância entre os Ministros Edson Fachin e André Mendonça, fazendo com que a decisão colegiada ficasse de 3 votos a favor da nulidade das provas e 2 votos contra.

O Ministro André Mendonça, em seu voto, discordando do Relator, disse que o eventual vício contido no processo refere-se a apenas os dados congelados pela Apple, e não pela Google, já que estes últimos foram submetidos diretamente ao crivo judicial. Ainda, defende que não há qualquer limite de prazo para que esses dados sejam guardados pelas empresas provedoras de internet, porquanto o Marco Civil não estipula prazos máximos ou mínimos que devem ser guardados.

Outrossim, sobre o ponto máximo da discussão deste texto, ele aduziu que não enxergou o nexo de causalidade entre o pedido de preservação das provas e a nulidade pretendida, já que esse pedido não se revela como um dos meios de produção de provas e a medida não repercutiu diretamente na instrução do processo e que o pedido extrajudicial não produziu qualquer resultado probatório, fato que foi efetivado apenas após a quebra de sigilo deferida por autorização judicial.

Ademais, a parte ré não se comprometeu a provar que o congelamento dos elementos probatórios interferiu de alguma forma na fabricação das provas.

Portanto, o ponto principal de André Mendonça é que o congelamento feito a pedido extrajudicial do MPPR não teve nexo de causalidade com as provas produzidas no processo, porquanto não foi provado o prejuízo da ré.

O Ministro Edson Fachin concordou com os argumentos de André Mendonça e sustentou que, embora tenha ocorrido o congelamento dos dados telemáticos sem autorização judicial prévia, posteriormente, o acesso a tais informações foi regularizado mediante decisão judicial válida. Em sua visão, essa autorização posterior evitaria a irregularidade na obtenção da prova, uma vez que o conteúdo congelado somente foi obtido com autorização judicial.

O Ministro ressaltou que não houve nexo de causalidade entre o bloqueio inicial e as provas efetivamente produzidas. Segundo ele, a mera irregularidade da falta de autorização naquele momento não ocasionou diretamente a produção das provas utilizadas, uma vez que o acesso era regular mediante decisão do juiz posterior. Ele argumentou ainda que não haveria motivação para excluir esta evidência.

Além disso, Fachin aplicou o princípio da proporcionalidade, considerando que, embora o procedimento inicial possa ser questionável, não houve violação concreta dos direitos da investigada. A preservação dos dados não implicou, por si só, uma invasão à privacidade ou ao conteúdo das comunicações, já que o acesso aos dados foi devidamente

autorizado posteriormente. Por isso, ele concluiu que a nulidade das provas não deveria ser declarada, defendendo a regularidade do procedimento investigativo.

## **CAPÍTULO 3: O CONFLITO DE IDEIAS**

### **3.1 As Divergências**

Vê-se, portanto, que os ministros STJ divergem entre os ministros do STF e, inclusive, estes divergem entre si mesmos sobre o ponto chave da discussão deste texto.

Os argumentos principais estão na forma em que os Ministros enxergam a Lei do Marco Civil da Internet, em que alguns a seguem estritamente, defendendo que irregularidades são causas diretas de nulidade. Outros defendem que onexo de causalidade, no caso em tela, não foi evidenciado entre os dados congelados e as provas produzidas. Ainda, destaca-se um argumento importante do Ministro do STJ Sebastião Reis Júnior de que o rol contido no artigo 13, § 2º, e artigo 15, §2º, ambos da Lei nº 12.965/14, são de caráter exemplificativo.

Enquanto uns defendem o poder persecutório no ambiente cibernético, que é muito novo e tecnológico em comparação ao nosso Direito, outros defendem a aplicabilidade dos direitos fundamentais em desfavor dos órgãos de persecução.

### **3.2 As Críticas**

Diante de todo o cenário exposto, são percebidas enormes falhas no sistema do Direito brasileiro, tanto judiciário, quanto legislativo. As leis não estão conseguindo acompanhar a evolução da Internet, levando a uma enorme ineficiência estatal para regular adequadamente o ambiente digital e proteger os direitos dos cidadãos.

A velocidade com que as tecnologias avançam e a natureza global da comunicação dobrada pela complexidade dos dados telemáticos são condições que desafiam o arcabouço legal, que em muitos casos está desatualizado e inadequado para problemas como crimes cibernéticos, privacidade de dados ou preservação de evidências digitais. Essa lacuna legislativa cria um ambiente de incerteza que impacta não apenas a aplicação da justiça, mas também na proteção de garantias constitucionais fundamentais como privacidade, liberdade de expressão ou devido processo legal.

Essa morosidade do Direito brasileiro, em que os Ministros das mais altas cortes conseguem sequer formar uma jurisprudência unânime e sólida, revela ainda mais o problema que enfrentamos.

De um lado, está a eficiência estatal em face do avanço da Internet, em que foi evidenciado que o simples congelamento dos dados telemáticos, sem a quebra do sigilo e sem a necessidade de autorização judicial, traria rapidez à autoridade policial e ao Ministério Público nas investigações.

Dessa forma, tal medida enrobusteceria o conjunto probatório com mais rapidez e mais solidez, porquanto os dados digitais são de alta volatilidade e se perderiam num piscar de olhos, caso o investigado saiba que o Ministério Público pediu a autorização judicial para congelá-los, por exemplo, frustrando a persecução penal.

Por outro lado, há a necessidade de levar a letra da Lei (o Marco Civil da Internet) de maneira objetiva. A proteção do direito à privacidade é o ponto fundamental que é discutido, já que o STF defende que a privacidade vai além de ter seus dados sigilosos expostos, é também sobre a garantia de ter livre acesso aos próprios dados e poder alterá-los como bem entender, a fim de construir a imagem pública.

Destarte, o “atropelamento” da Lei feito pelos órgãos de persecução também foi considerado uma ofensa aos direitos fundamentais, pois a quebra de garantias legais para acelerar investigações pode comprometer o equilíbrio entre a eficiência estatal e os direitos individuais. Esse tipo de conduta abre precedentes perigosos, em que o devido processo legal é violado, gerando insegurança jurídica e minando a confiança no sistema de justiça.

Sobre isso, é relevada a morosidade e a incerteza estatal para criar um norte sobre essas matérias.

Diante desse cenário, é fundamental reconhecer que a celeridade e a eficiência nas investigações criminais são imprescindíveis para garantir uma resposta eficaz do Estado frente ao crescimento exponencial dos crimes cibernéticos. O Ministério Público, ao defender a possibilidade de congelamento de dados telemáticos sem autorização judicial prévia, atua em prol de uma maior eficiência na persecução penal, especialmente considerando a volatilidade dos dados digitais. A agilidade para preservar essas informações, que podem ser facilmente manipuladas ou destruídas, é crucial para assegurar que provas essenciais não sejam perdidas, prejudicando o curso da investigação.

Ademais, o argumento de que o congelamento dos dados telemáticos não implica, necessariamente, em quebra de sigilo é relevante. Preservar essas informações sem acessá-las imediatamente não viola, de maneira direta, a privacidade do investigado, mas sim garante

que o conteúdo esteja disponível para eventual análise posterior, quando a autorização judicial for concedida.

No mesmo plano, o direito à privacidade não é um direito absoluto e poderá ser quebrado em autorizações judiciais, quando explicada sua importância para a confecção de provas no processo penal. Ainda, o direito à privacidade é aquele que nos preserva do conhecimento alheio e nos reserva a própria vivência, delimitando o que se mostra e o que se oculta, a critério do dono das informações.

Portanto, ao contrário do que pensa o STF, não há um nexo causal entre a indisponibilização dessas informações e a confecção da vida pública – a forma com que transparecemos as nossas informações –, porquanto os dados ainda continuam privados, sem que viesse a público de qualquer maneira. Em arremate de tal discussão, o direito à privacidade foi quebrado corretamente através da decisão judicial.

Dessa forma, não ficou provado como a disponibilização – ou a indisponibilização, neste caso – dos dados seria capaz de alterar a imagem pública da ré, ou ela mesma alterar sua imagem pública através dos dados que foram congelados. Portanto, foi uma colocação genérica feita pelo STF de que o direito à privacidade também é sobre a disponibilização dos próprios dados, estritamente a fim de formar a imagem pública. Isto não foi provado que foi prejudicado no caso em tela.

Embora o STF tenha um papel crucial na proteção dos direitos fundamentais, é preciso refletir sobre os desafios práticos que essa interpretação mais restritiva e incriteriosa impõe. A realidade dos crimes digitais exige uma adaptação das ferramentas jurídicas, permitindo que o Estado atue de forma mais eficaz, sem que isso represente uma violação desproporcional dos direitos individuais. O cenário atual, em que se observa uma lacuna legislativa e a ausência de consenso jurisprudencial, reforça a necessidade de que o ordenamento jurídico brasileiro se ajuste à velocidade do avanço tecnológico.

É, portanto, coerente defender que, no contexto da persecução penal envolvendo dados telemáticos, a flexibilização<sup>13</sup> da necessidade de autorização judicial para o congelamento de provas se justifica. Não se trata de desrespeitar a privacidade ou o devido processo legal, mas sim de encontrar um equilíbrio que permita ao Estado ser mais eficiente na investigação e punição de crimes que utilizam a Internet como ferramenta.

Enquanto não se formam jurisprudências mais sólidas e seguras do que as apresentadas neste texto (porquanto foram as primeiras sobre este tema), não se pode permitir

---

<sup>13</sup> Os argumentos do Ministro Sebastião Reis Júnior.



que a internet seja “terra sem lei”, como era há não muitos anos atrás, sem qualquer regulação estatal.

Destarte, é inescusável a aplicação da plena jurisdição no ambiente virtual mesmo quando as leis que o regulam sejam nebulosas. Não se pode permitir que as brechas legais – que, sobre esse assunto, são gigantes – sejam aproveitadas por aqueles que utilizam a internet para a prática de ilícitos, prevalecendo a aplicabilidade da lei penal.

Assim, é essencial que o ordenamento jurídico evolua de maneira que permita a coexistência entre a proteção dos direitos fundamentais e a eficiência na atuação do Ministério Público e da Polícia. A criação de normas mais claras e adaptadas à realidade digital, assim como uma maior uniformidade nas decisões judiciais, são passos críticos para garantir que a justiça seja realizada sem comprometer a segurança jurídica e a confiança nas instituições, principalmente.

Mas, enquanto isso não acontece, é crucial que o Ministério Público e a Polícia disponham de plenas ferramentas para agir de forma eficiente, mesmo diante das lacunas legislativas. Limitar os órgãos de persecução penal nos pontos apontados neste texto é permitir que ilícitos aconteçam no campo virtual.

Da mesma forma, a aplicabilidade da lei penal no ambiente digital não pode ser enfraquecida pela ausência de normas completamente consolidadas. Ao contrário, é justamente nesses momentos de indefinição que o Estado deve fornecer aos órgãos de persecução penal os instrumentos necessários para garantir a eficácia das investigações e a proteção da sociedade, e não os tirar.

Portanto, limitar a atuação do Ministério Público e da Polícia devido a uma legislação nebulosa é um retrocesso ao Marco Civil da Internet, Lei que outrora foi duramente criticada, hoje é a principal garantia de seguridade que temos no ambiente virtual.

### **3.2 Os Dias Atuais e Futuros**

O conteúdo deste texto é de extrema importância para a confecção da sociedade jurídica nos dias de hoje, pois tudo que foi fixado e se fixará por meio de jurisprudências das cortes superiores serão parâmetros a serem utilizados para a interpretação das normas vigentes.

Com a matéria paralelamente semelhante à deste texto, discutiu-se recentemente, no dia 11 de setembro de 2024, no Plenário do STF a ADI nº 4906<sup>14</sup>, sobre a desnecessidade de autorização judicial para que a autoridade policial ou o Ministério Público possam ter acesso aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito, contidos no artigo 17-B, da Lei nº 9.613/98<sup>15</sup>.

O Plenário do Supremo, por maioria, deu improcedência à ADI e concluiu que é constitucional que o Ministério Público ou a autoridade policial tenha acesso aos referidos dados, decisão que favorece a persecução penal e aumenta a eficiência estatal no âmbito das investigações.

Dessa forma, vê-se que o Plenário do Supremo deu razão aos órgãos de persecução penal, o que é contraditório com a decisão da 2ª turma do STF em relação ao julgamento do caso principal deste texto.

Ora, se o texto do artigo 17-B, da Lei nº 9.613/98 confere aos órgãos de persecução o livre acesso, sem autorização judicial, dos dados descritos, já que não fere o princípio da privacidade, o simples congelamento de dados também não deveria depender de autorização judicial, ainda mais que o mero congelamento não é sinônimo de quebra do sigilo.

Sendo assim, percebe-se que os debates sobre até onde vai a força estatal contra os artificios digitais estão cada vez mais fumegantes e encaminhados para um futuro de intensos conflitos e adaptações. Entretanto, com os julgamentos recentes do Plenário do Supremo, vemos que o norte que está sendo tomado para a regulação da persecução penal na internet é um caminho que traz ferramentas mais robustas aos órgãos investigativos, ao declarar constitucional as práticas supracitadas.

## CONCLUSÃO

A análise realizada ao longo deste trabalho demonstra que o sistema jurídico brasileiro enfrenta dificuldades para acompanhar o avanço tecnológico, especialmente no que tange à persecução penal de crimes digitais e o acesso a dados telemáticos. A divergência

---

<sup>14</sup> BRASIL. STF – Supremo Tribunal Federal. ADI 4906, Rel. Min. Nunes Marques, julgado em 11 set. 2024, Diário de Justiça Eletrônico, 15 set. 2024. Disponível em: <http://www.stf.jus.br>. Acesso em: 12 set. 2024.

<sup>15</sup> Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito.

entre o STJ e o STF sobre a necessidade de autorização judicial para o congelamento de dados revela a complexidade da questão e a dificuldade de balancear a eficiência investigativa com a proteção de direitos fundamentais.

Embora o Marco Civil da Internet tenha sido um avanço, ele não responde de forma adequada às demandas da era digital. A postura mais flexível do STJ, que permite o congelamento de dados sem autorização judicial, é uma medida que garante maior agilidade às investigações, evitando a perda de provas, enquanto o STF mantém uma defesa mais rigorosa da privacidade. No entanto, é fundamental que o Estado ofereça ao Ministério Público e à Polícia as ferramentas necessárias para agir com eficiência.

Assim, é necessária, o quanto antes, uma evolução legislativa e jurisprudencial sólida que garanta aos órgãos de persecução ferramentas adequadas para as investigações penais, como a atualização do Marco Civil da Internet nos moldes defendidos pelo STJ e utilizando os argumentos do Ministro Sebastião Reis Júnior para configurar o rol de dados que podem ser congelados exemplificativo, e não exaustivo, sem que isso seja considerado uma ofensa dos direitos fundamentais, a fim de garantir a aplicabilidade da lei penal e maior celeridade e eficiência das investigações em um ambiente cada vez mais digital e dinâmico.

Ademais, um remolde, assim como já se encaminha, conforme dito no capítulo anterior, na forma que o judiciário enxerga o direito à privacidade, que, como arguido, não há nexos com o simples congelamento de dados, mas com a disponibilização a outrem desses dados, é necessário para a evolução do Direito no ponto nodal da discussão.

Dessa maneira, com uma jurisprudência forte e consolidada e com uma Lei que tem uma interpretação precisa, sem resquícios de dúvidas ou interpretações distintas, o processo penal na era digital terá maior precisão, garantirá que os órgãos persecutórios realizem o trabalho com maior facilidade e, conseqüentemente, autonomia e velocidade. Assim, as demandas específicas deste caso serão solucionadas e, além disso, servirão de parâmetros para as discussões semelhantes futuras, ao passo que promovem uma justiça mais justa e eficaz, mesmo que esse aumento da força estatal seja contrária às ideias dos autores Duarte e Santoro.

## **REFERÊNCIAS**

ALVES, Natália. Registros no Marco Civil da Internet. JusBrasil, 07 mar. 2019. Disponível em:

<https://www.jusbrasil.com.br/artigos/registros-no-marco-civil-da-internet/699238307>. Acesso em: 29 ago. 2024.

BATAIER, Carolina. Do Twitter ao fim do X: entenda os capítulos que levaram à decisão de derrubar a rede social no Brasil. *Brasil de Fato*, 30 ago. 2024. Disponível em: <https://www.brasildefato.com.br/2024/08/30/do-twitter-ao-fim-do-x-entenda-os-capitulos-que-levaram-a-decisao-de-derrubar-a-rede-social-no-brasil>. Acesso em: 27 ago. 2024.

BRASIL. STF – Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental nº 403, Distrito Federal. Relator: Ministro Edson Fachin. Julgado em: 20 de março de 2019. Diário de Justiça Eletrônico, Brasília, DF, 9 maio 2019. Disponível em: <http://www.stf.jus.br>. Acesso em: 6 set. 2024.

BRASIL. STF – Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 4906. Relator: Ministro Nunes Marques. Julgado em: 11 de setembro de 2024. Diário de Justiça Eletrônico, Brasília, DF, 15 set. 2024. Disponível em: <http://www.stf.jus.br>. Acesso em: 12 set. 2024.

BRASIL. STF – Supremo Tribunal Federal. Habeas Corpus nº 222.141, Paraná. Relator: Ministro Ricardo Lewandowski. Julgado em: 1º de dezembro de 2022. Diário de Justiça Eletrônico, Brasília, DF, 8 dez. 2022. Disponível em: <http://www.stf.jus.br>. Acesso em: 20 jul. 2024.

BRASIL. STF – Supremo Tribunal Federal. Agravo Regimental no Habeas Corpus nº 222.141, Paraná. Relator: Ministro Ricardo Lewandowski. Julgado em: 6 de fevereiro de 2024. Diário de Justiça Eletrônico, Brasília, DF, 8 fev. 2024. Disponível em: <http://www.stf.jus.br>. Acesso em: 30 jul. 2024.

BRASIL. STJ – Superior Tribunal de Justiça. Habeas Corpus nº 626.983, Paraná. Relator: Ministro Olindo Menezes. Julgado em: 22 de fevereiro de 2022. Diário de Justiça Eletrônico, Brasília, DF, 25 fev. 2022. Disponível em: <http://www.stj.jus.br>. Acesso em: 20 jul. 2024.

CASTELLS, Manuel. *A Sociedade em Rede*. 8ª ed. São Paulo: Paz e Terra, 2018.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). Os Núcleos de Justiça 4.0: inovação disruptiva no Poder Judiciário brasileiro. *Portal CNJ*, 28 maio 2021. Disponível em: <https://www.cnj.jus.br/os-nucleos-de-justica-4-0-inovacao-disruptiva-no-poder-judiciario-brasileiro/>. Acesso em: 25 jul. 2024.

DUARTE, Daniel Nascimento; SANTORO, Antonio Eduardo Ramires. Gestão diferencial dos ilegalismos no processo penal na era da sociedade digital. *Revista Brasileira de Ciências Criminais*. vol. 183. ano 29. p. 23-55. São Paulo: Ed. RT, setembro 2021.

HAIKAL, V. A. Da significação jurídica dos conceitos integrantes do art. 5ª: internet, terminal, administrador de sistema autônomo, endereço internet protocol- IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrado no ente nacional responsável pelo registro e distribuição de endereço IP; conexão à internet; registro de conexão; aplicações de internet; e registros de acesso a aplicações de internet. In: LEITE, G. S.; LEMOS, R. (Org.). *Marco civil da internet*. 1. ed. São Paulo: Atlas, 2014. cap. 3, p.315-345.

MENDES, Gilmar. Os limites do acesso a dados pelas autoridades. *IRIB - Instituto de Registro Imobiliário do Brasil*, 27 ago. 2020. Disponível em: <https://www.irib.org.br/noticias/detalhes/gilmar-mendes-os-limites-do-acesso-a-dados-pelas-autoridades>. Acesso em: 2 ago. 2024.

NOGUEIRA, Antonio. O Marco Civil da Internet e as Reações da Sociedade Civil: Entre o Temor e a Esperança. *Revista de Direito e Tecnologia*, São Paulo, v. 3, n. 1, 2015, p. 98-115.