PROCESSO PENAL E O AFASTAMENTO DO SIGILO DE COMUNICAÇÕES ARMAZENADAS: ANÁLISE DO MARCO CIVIL DA INTERNET E DA JURISPRUDÊNCIA DE TRIBUNAIS SUPERIORES

CRIMINAL PROCEDURES AND THE SECRECY BREACH OF STORED COMMUNICATIONS: AN ANALYSIS OF THE BRAZILIAN CIVIL RIGHTS FRAMEWORK FOR THE INTERNET AND THE JURISPRUDENCE OF THE SUPERIOR COURTS

Marta Saad[1]
Universidade de São Paulo, USP, Brasil
martasaad@usp.br

Helena Costa Rossi[2]
Universidade de São Paulo, USP, Brasil
helena.costa.rossi@gmail.com

Pedro Henrique Partata[3]
Universidade de São Paulo, USP, Brasil
pedro.mortoza@usp.br

DOI: https://doi.org/10.5281/zenodo.15660288

Resumo: A obtenção de comunicações eletrônicas armazenadas é meio de obtenção de prova nominado no art. 7º, III, do Marco Civil da Internet (MCI), segundo o qual assegura-se a inviolabilidade do sigilo dessas comunicações, salvo por ordem judicial. Nos termos do art. 10, § 2º do MCI, o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer. Até o momento, no entanto, inexiste lei que preveja o procedimento para a obtenção das comunicações armazenadas, em particular, as hipóteses e a forma de coleta dessas informações. O presente artigo pretende analisar como a ausência de previsão legal tem sido tratada pelos Tribunais Superiores no que diz respeito às autorizações para o acesso a essas comunicações no âmbito de investigações criminais, mediante estudo qualitativo de julgados comumente mencionados como paradigmáticos. Mediante revisão dos julgados, o artigo conclui que houve tímida evolução jurisprudencial que demonstre maior proteção das comunicações armazenadas. De forma específica, constata-se que, ainda que a jurisprudência tenha avançado em direção à exigência de autorização judicial, pouco se evoluiu quanto à necessidade de uma autorização legal suficiente, isto é, que inclua as hipóteses e a forma para a obtenção dessas informações, em atenção ao citado art. 10, § 2º.

Palavras-chave: comunicações eletrônicas armazenadas; Marco Civil da Internet; meios de obtenção de prova atípicos; evolução jurisprudencial.

Abstract: Obtaining stored electronic communications is a means of obtaining evidence referred to in article 7, III, of the Brazilian Civil Rights Framework for the Internet, according to which the inviolability of the secrecy of these communications is ensured, except by court order. Pursuant to article 10, § 2 of the Civil Rights Framework, the content of private communications may only be made available through a court order, in the circumstances and in the manner established by law. To date, however, there is no law that provides for the procedure for obtaining stored communications, in particular, that sets the hypotheses and method for collecting this information. This article aims to analyze how the absence of legal provisions has traditionally been treated by Brazilian higher courts regarding authorizations for access to these communications in the context of criminal investigations, through a qualitative study of judgments commonly mentioned by the doctrine as paradigmatic. By reviewing specific cases, the article concludes that there has been a timid jurisprudential evolution demonstrating concern with the protection of stored communications. Specifically, although jurisprudence has advanced towards the requirement of judicial authorization to obtain stored communications, little progress has been made in terms of accepting the need for sufficient legal authorization, that is, one that includes the hypotheses and the way to obtain this information, in compliance with article 10, § 2 of the same legal provision.

Keywords: stored electronic communications; Civil Rights Framework for the Internet; atypical means of obtaining evidence; jurisprudential evolution.

[1] Professora Doutora de Direito Processual Penal na Faculdade de Direito da USP. Doutora (2007) e Mestre (2002) pela mesma instituição. Advogada. Currículo Lattes: http://lattes.cnpq.br/3199855414351538. ORCID: https://orcid.org/0000-0001-5363-390X.

[2] Mestranda em Direito Processual Penal na Faculdade de Direito da USP. Advogada. Currículo Lattes: http://lattes.cnpq.br/6022530640899053. ORCID: https://orcid.org/0009-0004-3436-9807.

[3] Mestrando em Direito Processual Penal na Faculdade de Direito da USP. Advogado. Currículo Lattes: http://lattes.cnpq.br/9431614773439500. ORCID: https://orcid.org/0009-0008-1318-8950.

1. Introdução: moldura normativa e exposição do problema central

Atualmente, existem dois diplomas que regulamentam o afastamento do sigilo de comunicações: a Lei Federal 9.296/1996, ou Lei de Interceptações Telefônicas e Telemáticas (LIT); e a Lei Federal 12.965/2014, ou Marco Civil da Internet (MCI).

A LIT foi promulgada com a finalidade de regulamentar o art. 5º, XII, da Constituição da República (CR), estabelecendo parâmetros para a admissibilidade e a produção desse meio de obtenção de prova. O MCI, por sua vez, é resultado de longo processo legislativo, com ampla participação da sociedade civil, que objetivou regulamentar o uso da internet no Brasil (**Souza; Lemos**, 2016, p. 11-42).

A obtenção de comunicações armazenadas está condicionada a ordem judicial por força do art. 7º, III, do MCI, que garante "inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial". Segundo o art. 10, § 2º, da mesma lei, o "conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer".

A exigência de ordem judicial para o afastamento do sigilo que recai sobre as comunicações armazenadas decorre, naturalmente, do princípio da reserva de jurisdição para a restrição de direitos fundamentais. No entanto, para além da reserva de jurisdição, o MCI dispõe que a lei estabelecerá hipóteses e formas de obtenção dessas informações.

Até o presente momento, tal previsão ainda não foi disciplinada legalmente. Portanto, a obtenção de comunicações armazenadas constitui meio de obtenção de prova apenas nominado (**Badaró**, 2005, p. 351-362; **Gomes Filho; Badaró**, 2007, p. 175-176; **Dezem**, 2008, p. 154), não possuindo procedimento legal previsto, com hipóteses autorizadoras, rol de crimes investigados, dentre outras especificidades.

Diante da ausência de regulamentação que forneça parâmetros legais, determinações judiciais que autorizam a obtenção dessas informações são proferidas sem balizas claras, o que enseja problemas de diversas ordens, como ausência de segurança jurídica, aplicação analógica de procedimentos previstos para outras finalidades e ausência de limites às ingerências sobre os direitos fundamentais afetados. Não raro, determina-se que seja acessado ou apresentado todo o conteúdo armazenado disponível (**Azeredo**, 2015, p. 227-228; **Maranhão**, 2018, p. 45).

Ainda que a reserva de jurisdição constitua importante barreira de controle, ela não evita a discricionariedade do próprio julgador (**Badaró**, 2021, p. 58), o que reforça a necessidade de que limites sejam estabelecidos por lei (**Moraes**, 2010, p. 315-319). A necessidade de parâmetros legais mínimos decorre, ainda, da inclusão de proteção específica para os dados pessoais no art. 5º, LXXIX, da CR. Tal dispositivo, em especial no âmbito criminal, pende de regulamentação específica[1].

Os julgados analisados a seguir demonstram a existência de relativa evolução na percepção dos Tribunais Superiores, no sentido de que a proteção às comunicações armazenadas (e dados em geral) deve ser garantida mediante controle judicial. Poucas são, porém, as indicações de necessidade de previsão legal que institua requisitos rigorosos, de acordo com a gravidade da intervenção (**Mendes, L.**, 2015).

2. Acesso a comunicações armazenadas na jurisprudência dos Tribunais Superiores

Os julgados analisados a seguir, publicamente disponíveis nos sites do Superior Tribunal de Justiça (STJ) e do Supremo Tribunal Federal (STF), são considerados paradigmáticos, por enfrentarem questões relevantes relacionadas ao acesso a dados[2].

2.1. Superior Tribunal de Justiça

Os primeiros julgados do STJ sobre o acesso a comunicações armazenadas demonstram a compreensão de que dados digitais presentes em dispositivos informáticos não seriam tutelados por qualquer garantia, argumento relativamente compreensível no início dos anos 2000.

Exemplo disso é o entendimento firmado no *Habeas Corpus* (*HC*) 66.368/PA, de 2007, em que se discutia a licitude do acesso ao registro de ligações telefônicas de celulares apreendidos. A defesa sustentava a ilicitude dos elementos obtidos a partir do acesso, no momento da prisão e sem autorização, ao registro de chamadas de aparelhos pertencentes a corréu. O relator, Ministro Gilson Dipp, asseverou que o acesso a tais dados não configuraria "quebra do sigilo telefônico, uma vez que somente foram averiguadas quais teriam sido as últimas ligações feitas, bem como as recebidas" e que, assim, não houve o "conhecimento do conteúdo das conversas".

Quase uma década depois, a Corte reconheceu que o avanço tecnológico provocou mudanças no cenário fático, o que clamaria maior proteção às comunicações armazenadas. Exemplo disso é o quanto decidido no Recurso em *HC* 51.531/RO, de 2016. No caso, a persecução iniciou-se com a prisão em flagrante, oportunidade em que o celular foi apreendido e seu conteúdo foi acessado diretamente, sem decisão judicial.

O Tribunal reconheceu a ilicitude do acesso ao conteúdo sem autorização, revelando uma mudança histórica na concepção a respeito do grau de proteção conferido às informações armazenadas. O relator, Ministro Néfi Cordeiro, argumentou que "no acesso aos dados do aparelho, tem-se devassa de dados particulares, com violação à intimidade do agente" e que, "embora possível o acesso, necessária é a prévia autorização judicial devidamente motivada". O relator relacionou a mudança de concepção à evolução tecnológica, afirmando que "o celular deixou de ser apenas um instrumento de conversação pela voz".

O STJ manteve esse mesmo entendimento de reserva de jurisdição no Recurso em *HC* 99.735/SC, de 2018. Nesse caso, todavia, a Corte deixou claro que a decisão judicial prévia não seria, por si só, suficiente. Na origem, a polícia havia obtido autorização judicial para apreender o celular e, então, efetuar o espelhamento do WhatsApp no computador da delegacia. Após a autorização, o celular foi apreendido em busca pessoal e posteriormente devolvido, sem que o investigado tivesse conhecimento da medida. Dessa forma, foi possível obter os diálogos em tempo real.

Ao julgar o recurso, a Ministra Laurita Vaz relembrou que a leitura do *QR code*, utilizado para habilitar o espelhamento, somente pode ser feita pelo próprio usuário e que, se houvesse a habilitação da função "mantenha-me conectado", a sincronização das mensagens ocorreria de forma automática e indefinida. Rememorou ser possível o acesso a todas as conversas (mensagens e mídias anexadas) já efetuadas, independentemente da antiguidade, bem como o acompanhamento de todas as conversas posteriores.

A relatora asseverou que, como é possível a utilização simultânea do celular e do computador espelhado, torna-se possível o envio de novas mensagens e a exclusão de antigas. Ainda, como a eventual exclusão não deixa vestígios, esses dados não poderiam ser recuperados para fins probatórios.

Diante dessa dinâmica, a relatora entendeu ser inviável qualquer analogia com a interceptação, a fim de fundamentar a autorização da medida. Em primeiro lugar, argumentou que, na interceptação, o investigador é mero observador, ao passo que, no espelhamento,

torna-se participante do ato comunicacional. A Ministra também reconheceu que, ao contrário da interceptação, que tem por objeto o acesso às conversas realizadas após a autorização, o espelhamento do WhatsApp viabiliza a obtenção ampla e irrestrita de toda e qualquer comunicação, passada ou futura. Para ela, "não há, todavia, ao menos por agora, previsão legal de um tal meio de obtenção de prova híbrido".

A decisão, no entanto, não representou a pacificação da questão na Corte. Em julgados posteriores, houve o reconhecimento da licitude da técnica de espelhamento. No julgamento do Agravo Regimental no Agravo em Recurso Especial 2.309.888/MG, a Quinta Turma fundamentou a utilização dessa técnica nos permissivos relativos às interceptações e ao agente infiltrado virtual (Lei 12.850/2013), afirmando ser a medida "equivalente à modalidade de infiltração do agente" e "meio extraordinário, mas válido, de obtenção de prova".

Nesses casos, o colegiado entendeu que bastaria autorização judicial que realizasse o exame de proporcionalidade no caso concreto. Ainda, afastou a argumentação relativa à possibilidade de manipulação das informações, fundamentando tal compreensão na fé pública conferida aos atos oficiais praticados por agentes de persecução.

2.2. Supremo Tribunal Federal

No âmbito do STF, também houve gradual reconhecimento e ampliação da proteção conferida às comunicações armazenadas, por meio da exigência de autorização judicial.

No *HC* 91.867/PA3, de 2012, o STF ratificou o entendimento do STJ, vigente à época, no sentido de que o histórico de chamadas não se confundiria com a comunicação, e reconheceu a licitude da prova por entender que o acesso a tais dados não estaria condicionado a autorização prévia. Na oportunidade, a Corte reafirmou o entendimento firmado no Recurso Extraordinário 418.416/SC[4], e equiparou o acesso ao registro de chamada à mera apreensão de um pedaço de papel, o que permitiria a aplicação analógica dos arts. 6º e 240, do Código de Processo Penal.

Quase uma década depois, em 2020, o Ministro Gilmar Mendes reviu seu posicionamento no julgamento do *HC* 168.052/SP. No caso, discutia-se a licitude de provas obtidas mediante verificação de mensagens de WhatsApp por autoridades policiais sem autorização judicial. No caso, após informação anônima, os policiais se dirigiram à residência do indivíduo, onde apreenderam seu celular e acessaram o aplicativo de mensagens, verificando conteúdo que indicaria traficância. Em seguida, ingressaram no domicílio, alegando que o acesso lhes foi facultado pelo sujeito, e no local foram encontradas drogas, armas e munições.

Ao julgar o *HC*, o Ministro Gilmar Mendes registrou que "a modificação das circunstâncias fáticas e jurídicas, a promulgação de leis posteriores e o significativo desenvolvimento das tecnologias da comunicação" exigem solução distinta, estando-se "diante de típico caso de mutação constitucional". Também ressaltou que o art. 7º, III, do MCI, condiciona o acesso às comunicações armazenadas à ordem judicial e concluiu que a verificação das mensagens não poderia ter ocorrido sem prévia ordem judicial.

Ainda que o acórdão tenha consolidado entendimento acerca da necessidade de ordem judicial para o afastamento do sigilo de comunicações armazenadas, a discussão não se limitou a reafirmar a lei (art. 7º, III, do MCI). A questão, em verdade, lançou luzes para a necessidade de se atualizar a proteção aos dados comunicacionais, ressaltando que "quanto mais grave for a intervenção, maiores devem ser os requisitos" e "mais específica deve ser a lei que prevê tal interferência" (**Mendes, L.**, 2015).

3. Conclusão

Ainda que o avanço tecnológico das últimas décadas tenha influenciado a jurisprudência a demonstrar gradual preocupação com a proteção às comunicações armazenadas, pouco se evoluiu quanto ao reconhecimento da necessidade de autorização legal específica para o deferimento e a execução de meios de obtenção de prova digitais[5].

Pela análise dos julgados selecionados, constata-se que se passou a exigir prévia decisão judicial para a obtenção de comunicações armazenadas, ainda que em situações de flagrante, como forma necessária e suficiente para garantir os devidos limites à ingerência sobre os direitos fundamentais.

A determinação constante no art. 10, § 2°, do MCI, no sentido que haveria de ser promulgada lei que previsse hipóteses e formas de acesso ao conteúdo das comunicações privadas, não pode ser esquecida. É a lei, e não o casuísmo prático, que, em temas probatórios, prevê hipóteses e forma de obtenção e serve como salvaguarda de direitos e como limite necessário às atividades estatais.

Informações adicionais e declarações dos autores (integridade científica)

Declaração de conflito de interesses: os autores confirmam que não há conflitos de interesses na condução desta pesquisa e na redação deste artigo. **Declaração de autoria:** todos e somente os pesquisadores que cumprem os requisitos de autoria deste artigo são listados como autores; todos os coautores são totalmente responsáveis por este trabalho em sua totalidade. **Declaração de originalidade:** os autores garantiram que o texto aqui publicado não foi publicado anteriormente em nenhum outro recurso e que futuras republicações somente ocorrerão com a indicação expressa da referência desta publicação original; eles também atestam que não há plágio de terceiros ou autoplágio.

Como citar (ABNT Brasil)

SAAD, Marta; ROSSI, Helena Costa; PARTATA, Pedro Henrique. Processo penal e o afastamento do sigilo de comunicações armazenadas: análise do Marco Civil da Internet e da jurisprudência de tribunais superiores. **Boletim IBCCRIM**, São Paulo, v. 33, n. 392, p. 21-24, 2025. DOI: 10.5281/zenodo.15660288. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/2014. Acesso em: 1 jul. 2025.

Notas

[1] A esse respeito, nota-se que a doutrina tem evoluído no sentido de sugerir critérios específicos a serem previstos em lei, com o intuito de suprir a necessidade de um modelo de regulação com balizas mínimas para o acesso a dados, o que se entende salutar. Sobre o tema: citam-se: Bacigalupo (2002, p. 198-199), G. Mendes e Pinheiro (2015, p. 250) e Malan (2021, p. 115-116).

[2] Alguns desses acórdãos também foram analisados em diferentes estudos doutrinários relacionados ao tema, a exemplo de Zilli (2018, p. 72-75), Smanio (2022, p. 218-219), Ponce e Queiroz (2021, 605-621).

[3] O *HC* 91.867 foi impetrado no STF contra a denegação da ordem no *HC* 66.368, pelo STJ, analisado acima.

[4] O RE 418.416 é apontado como *leading case* da origem da interpretação de que a proteção constitucional do art. 5º, XII, da CR, recairia somente sobre a comunicação de dados. Nesse sentido, Ponce e Queiroz (2021, p. 605-621).

[5] Como já tivemos oportunidade de escrever em Saad, Rossi e Partata (2024).

Referências

AZEREDO, João Fábio. Sigilo das comunicações eletrônicas diante do Marco Civil da Internet. *In*: DE LUCCA, Newton (org.). *Direito & Internet*. São Paulo: Quartier Latin, 2015. v. III, t. II. p. 211-232.

BACIGALUPO, Enrique. *Justicia Penal y Derechos Fundamentales*. Madrid: Marcial Pons, 2002.

BADARÓ, Gustavo Henrique. Provas atípicas e provas anômalas: inadmissibilidade da substituição da prova testemunhal pela juntada e declarações escritas de quem poderia ser testemunha. *In*: YARSHELL; Flávio Luiz; MORAES, Maurício Zanoide (org.). *Estudos em homenagem à professora Ada Pellegrini Grinover*. São Paulo: DPJ, 2005. p. 351-362.

BADARÓ, Gustavo. O debate constitucional sobre privacidade, intimidade e proteção de dados no Brasil. *In*: BRITO CRUZ, Francisco; SIMÃO, Bárbara (org.). *Direitos fundamentais e processo penal na era digital*: doutrina e prática em debate. São Paulo: InternetLab, 2021. v. 4. p. 50-69. Disponível em: https://congresso.internetlab.org.br/wp-content/uploads/2021/08/InternetLab04_Miolo.pdf. Acesso em: 30 jan. 2025.

DEZEM, Guilherme Madeira. *Da prova penal*: tipo processual, provas típicas e atípicas (atualizado de acordo com as Leis 11.689/08 e 11.719/08). Campinas: Millenium, 2008.

GOMES FILHO, Antônio Magalhães; BADARÓ, Gustavo. Prova e sucedâneos de prova no processo penal brasileiro. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 65, p. 175-208, 2007.

MALAN, Diogo. Métodos ocultos, devido processo e o enfrentamento à criminalidade organizada. *In*: CRUZ, Francisco Brito; SIMÃO, Bárbara (org.). *Direitos fundamentais e processo penal na era digital*: doutrina e prática em debate. São Paulo: InternetLab. 2021. v. 4. p. 106-117. Disponível em: https://congresso.internetlab.org.br/wp-content/uploads/2021/08/InternetLab04_Miolo.pdf. Acesso em: 30 jan. 2025.

MARANHÃO, Juliano. O que é dado não é comunicado? *In*: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (org.). *Direitos fundamentais e processo penal na era digital*: doutrina e prática em debate. São Paulo: InternetLab, 2018. v. 1. p. 42-55. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2018/08/DIGITAL_InternetLAB_DUPLA.pdf. Acesso em: 30 jan. 2025.

MENDES, Gilmar Ferreira; PINHEIRO, Jurandi Borges. Interceptações e privacidade: novas tecnologias e a Constituição. *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (org.). *Direito, inovação e tecnologia*. São Paulo: Saraiva, 2015. v. 1. p. 231-250.

MENDES, Laura Schertel Ferreira. Uso de softwares espiões pela polícia: prática legal? *Jota*, 4 jun. 2015. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policia-pratica-legal-04062015. Acesso em: 30 jan. 2025.

MORAES, Maurício Zanoide de. *Presunção de inocência no processo penal brasileiro*: análise de sua estrutura normativa para a elaboração legislativa e para a decisão judicial. Rio de Janeiro: Lumen Juris, 2010.

PONCE, Paula Pedigoni; QUEIROZ, Rafael Mafei Rabelo. Sigilo de dados e proteção de dados pessoais na jurisprudência do STF: síntese da trajetória de um direito fundamental. *In*: MARANHÃO, Juliano Souza de Albuquerque; BARBOSA, Samuel Rodrigues (org.). *O fim da dogmática jurídica?* Estudos em homenagem aos 80 anos do professor Tercio Sampaio Ferraz Junior. Belo Horizonte, São Paulo: D'Plácido, 2021. p. 605-621.

SAAD, Marta; ROSSI, Helena Costa; PARTATA, Pedro Henrique. A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. *Revista Brasileira de Direito Processual Penal*, São Paulo, v. 10, n. 3, e1071, 2024. https://doi.org/10.22197/rbdpp.v10i3.1071

SMANIO, Gianluca Martins. *Vigilância policial em meio digital*: entre o garantismo e a eficiência. Curitiba: Juruá, 2022.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco civil da internet*: construção e aplicação. Juiz de Fora: Editar, 2016.

ZILLI, Marcos. A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade. *In*: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (org.). *Direitos fundamentais e processo penal na era digital*: doutrina e prática em debate. São Paulo: InternetlLab, 2018. v. 1. p. 64-99. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2018/08/DIGITAL_InternetLAB_DUPLA.pdf. Acesso em: 30 jan. 2025.

Recebimento: 20.02.2025. Aprovação: 20.05.2025. Última versão dos autores: 28.05.2025.