XXXI CONGRESSO NACIONAL DO CONPEDI BRASÍLIA - DF

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO III

CELSO HIROSHI IOCOHAMA

LUIZ GUSTAVO GONÇALVES RIBEIRO

MATHEUS FELIPE DE CASTRO

D597

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO III [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Celso Hiroshi Iocohama, Luiz Gustavo Gonçalves Ribeiro, Matheus Felipe De Castro – Florianópolis: CONPEDI, 2024.

Inclui bibliografia
ISBN: 978-65-5274-054-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: UM OLHAR A PARTIR DA INOVAÇÃO E DAS NOVAS TECNOLOGIAS

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito penal. 3. Processo penal e constituição. XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3: 2024 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXXI CONGRESSO NACIONAL DO CONPEDI BRASÍLIA - DF

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO III

Apresentação

A edição do XXXI CONGRESSO NACIONAL DO CONPEDI – BRASÍLIA nos ofereceu produções cientificas inestimáveis, no âmbito da visão constitucional do Direito Penal e do Processo Penal. Os trabalhos apresentados abordam uma conjuntura de temas e ideias necessárias à reflexão da comunidade cientifica sobre os problemas relacionados ao grupo temático. Dentro desse contexto, no Grupo de Trabalho - DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO III constatou-se qualificadas contribuições para o campo das Ciências Sociais Aplicadas, além de profícuo debate de todos os presentes na sala.

A obra ora apresentada reúne os artigos selecionados através do sistema de dupla revisão cega, de modo a nos permitir certeza de que os temas a seguir apresentados são instigantes e apresentam significativas contribuições para as reflexões dos Programas de Pós-graduação em Direito reunidos no CONPEDI.

São os seguintes, por título e objeto, os trabalhos que compõem o livro:

- “A implementação da delegacia especializada de atendimento à mulher em Viçosa-MG: da law on the books à law in action”, que traz os resultados de uma pesquisa que objetivou identificar o impacto da implantação da Delegacia Especializada de Atendimento à Mulher na proteção à mulher e no combate à violência de gênero e doméstica na Comarca de Viçosa-MG, tomando por corte temporal o intervalo entre os anos de 2019 e 2022. Partindo desse objetivo geral, a pesquisa buscou os seguintes objetivos específicos: a) coletar os dados referentes ao processo de implantação da Delegacia Especializada de Atendimento à Mulher em Viçosa-MG; b) verificar se, desde sua implantação até o corrente ano de 2022, a DEAM em Viçosa-MG foi provida das estruturas física, material e humana necessárias ao desenvolvimento de suas tarefas; c) identificar o perfil e o quantitativo de casos por ela atendidos no intervalo compreendido entre sua implantação no ano de 2019 e dezembro de 2022; d) identificar o perfil e o quantitativo de casos de violência de gênero e doméstica atendidos pela Delegacia de Polícia de Viçosa-MG entre os anos de 2015 e a véspera da implantação da DEAM, para proceder a comparação com o período subsequente; e) verificar se a DEAM em Viçosa tem funcionado dentro dos parâmetros estabelecidos pela Constituição Federal de 1988 e pela Lei n. 11.340/2006 e para além do exercício de mera tarefa de polícia investigativa ou judiciária na promoção e proteção das mulheres vítimas de violência de gênero e doméstica.

- “Homicídio culposo e o arrependimento posterior: uma crítica ao entendimento do STJ e ênfase ao alcance extrapatrimonial do instituto”. O trabalho busca questionar a interpretação dada pelo Superior Tribunal de Justiça à aplicabilidade do instituto do arrependimento posterior ao homicídio culposo. No julgamento do Recurso Especial número 1.561.276/BA, a Corte Cidadã fixou o entendimento de que a causa de diminuição prevista no artigo 16 do Código Penal só incidiria em crimes contra o patrimônio ou com efeitos exclusivamente patrimoniais. Em perspectiva contrária, a pesquisa sustenta que tal interpretação é restritiva e destoa da própria razão de ser do instituto. Entende-se que a reparação do dano na seara penal é uma medida de política criminal, frequentemente estimulada pelo legislador. Deste modo, em atenção aos requisitos expostos no Código Penal, defende-se que a violência no resultado não obstaria a aplicação do instituto, sendo a aplicabilidade aqui sustentada amparada em três principais argumentos. Inicialmente, tem-se que, em uma interpretação sistemática do ordenamento brasileiro, a reparação do dano à vida é possível (e desejável), tendo em conta a ideia de reparação por ato ilícito disposta no Código Civil. Em seguida, destaca-se que a própria razão de ser do instituto do arrependimento posterior, constante na exposição de motivos da Parte Geral do Código, indica que a preocupação se volta sobretudo à vítima (se estendendo aos seus familiares, por consectário lógico). Nessa linha, conclui-se que a interpretação conferida pelo Superior Tribunal de Justiça revela-se contrária aos princípios da legalidade e proporcionalidade, sendo defendida a revisão do entendimento.

- “A função da pena na sociedade Pós-Moderna sob o prisma do paradigma do Estado Democrático de Direito”. O trabalho em questão aborda as teorias retributiva e prevencionista das penas, com foco especial na pena privativa de liberdade e sua função em uma sociedade globalizada e pós-moderna. A teoria retributiva defende que a punição é uma resposta justa ao crime, proporcional à gravidade da infração cometida. Por outro lado, a teoria prevencionista busca evitar futuros crimes por meio da dissuasão, incapacitação do criminoso ou sua reabilitação. Na sociedade pós-moderna, caracterizada por uma interconectividade e complexidade crescentes, o papel da pena privativa de liberdade é amplamente debatido. Embora a retribuição ainda seja vista como crucial para manter a ordem e a justiça social, a prevenção, especialmente com ênfase na reabilitação e reintegração social, ganha destaque. Evidências mostram que penas severas nem sempre resultam em menores taxas de reincidência, o que reforça a necessidade de uma abordagem equilibrada. A globalização apresenta novos desafios e perspectivas, exigindo uma ponderação entre punir e promover uma sociedade mais justa e segura. O artigo conclui que a pena privativa de liberdade, como ferramenta punitiva, deve ser reavaliada à luz dos direitos humanos e das evidências empíricas sobre sua eficácia, destacando a importância de políticas penais que integrem justiça retributiva, prevenção e reintegração social.

- “A atuação do poder público na defesa dos direitos da mulher presidiária”. No trabalho são abordados estudos sobre o estabelecimento penal, função da pena, prisão de mulheres, direitos fundamentais das mulheres, princípio da dignidade da pessoa humana, medidas alternativas da pena, direitos humanos e direitos fundamentais e a violação dos direitos e interesses da mulher presidiária pelo Poder Público. Busca-se a análise das situações prisionais e estatísticas com base de dados em relação ao encarceramento de mulheres no Brasil. Também é abordada a situação de mulheres na situação especial de prisão em tempos de gravidez e a violação de seus direitos enquanto pessoa do sexo feminino.

- “O reconhecimento de pessoas como meio de prova no processo penal: uma análise de erros judiciais”. O texto aborda o reconhecimento de pessoas como meio de prova no processo penal, que apesar de sua importância, é considerada uma prova frágil, pois depende da memória humana, que se demonstrou falha e influenciável, tornando esse meio probatório suscetível a erros. Diante disso, questiona-se: o reconhecimento pessoal ou fotográfico pode ser utilizado como único meio de prova para fundamentar uma condenação no processo penal brasileiro, consequentemente violando o standard de prova além da Dúvida Razoável? Para responder o questionamento feito, foram analisados os procedimentos de reconhecimento no processo penal e os erros judiciais causados por reconhecimentos equivocados, bem como, o posicionamento do STJ em relação à problemática. O trabalho inicia discorrendo acerca da importância desse meio prova, que é amplamente utilizado, mas que pode ser falho, dessa forma, levando a condenações injustas de inocentes. Além disso, foi externado como essa problemática acaba por evidenciar o racismo estrutural e institucional no Brasil. Ao final constatou-se que o reconhecimento deve ser realizado com cautela e de acordo com a previsão legal e não deverá ser utilizado como único meio probatório.

- “Tornozeleiras eletrônicas como instrumento de monitoramento: estigmatização, desafios e implicações para o sistema penal”. No trabalho ora apresentado, o objetivo foi analisar criticamente o uso das tornozeleiras eletrônicas no sistema penal brasileiro, enquanto instrumento de monitoramento de indivíduos em cumprimento de penas alternativas. Inicialmente, discute-se a estigmatização social que recai sobre os usuários desses dispositivos, evidenciando os impactos sociais e as barreiras para a reintegração dos monitorados. Em seguida, aborda-se os desafios inerentes à implementação dessas tecnologias, destacando as falhas operacionais, os custos elevados e as lacunas no arcabouço normativo que regem seu uso. A investigação fundamenta-se em uma revisão bibliográfica abrangente, complementada por análises de casos emblemáticos que ilustram aspectos positivos e negativos da utilização dos dispositivos eletrônicos, frente ao contexto penal e social. Conclui-se que, embora essas ferramentas representem uma inovação importante na mitigação da superlotação carcerária e na promoção de penas alternativas, há reflexos

sensíveis, na relativização da dignidade da pessoa humana dos monitorados, além de uma eficácia limitada pela carga estigmatizante e pelos obstáculos práticos à sua aplicação. O trabalho propõe, portanto, o aperfeiçoamento dessas tecnologias e sua integração com outras estratégias de reintegração social enquanto imperativos para o cumprimento das funções declaradas dos serviços de monitoração eletrônica no país.

- “Divergências entre os posicionamentos de Gunther Jakobs e Manuel Cancio Meliá sobre a teoria do direito penal do inimigo e sua incompatibilidade com o garantismo penal”. No trabalho são abordadas noções sobre a Teoria do Direito Penal do Inimigo, seu surgimento e aplicabilidade, bem como sua incompatibilidade com o garantismo penal de Ferrajoli. Apresenta-se a biografia de Gunther Jakobs e breves considerações abordando as divergências entre o seu posicionamento e o de Claus Roxin em relação à teoria da imputação objetiva, já que se trata de uma temática bastante trabalhada por Gunther Jakobs em suas produções científicas. Também apresenta-se a biografia de Manuel Cancio Meliá e as posições doutrinárias divergentes entre ele e Gunther Jakobs sobre a teoria do direito penal do inimigo.

- “A sociedade de risco e as velocidades do direito penal”. O texto propõe uma análise acerca do fenômeno da Expansão do Direito Penal sob a ótica da teoria desenvolvida por Jesús-María Silva Sánchez, denominada “Velocidades do Direito Penal”, da Teoria Pessoal do Bem Jurídico e o Direito Penal de Intervenção de Winfried Hassemer e da teoria da Sociedade de Risco de Ulrick Beck. O objetivo geral consiste na reflexão sobre as principais características da sociedade do risco investigada por Ulrich Beck e sua relação com o expansionismo penal e as possíveis influências que esse modelo de organização social exerce sobre o Direito Penal. A metodologia utilizada foi a pesquisa bibliográfica e documental a partir de obras relacionadas ao tema, o método jurídico dedutivo, com abordagem qualitativa. Entre as conclusões obtidas por meio deste trabalho, pode-se destacar que a diminuição da criminalidade não está relacionada ao expansionismo penal imoderado, nem ao endurecimento do Direito Penal, mas sim a uma política social igualitária, que deve assegurar que as leis penais respeitem os limites constitucionais, notadamente as garantias constitucionais, tanto na sua criação quanto na sua aplicação. De toda sorte, a insegurança e o medo sentidos pela sociedade devem ser considerados e exigem uma resposta efetiva do Estado, que não será encontrada na reprodução de um Direito Penal meramente simbólico ou no recrudescimento das sanções penais.

- “Direitos humanos e segurança pública: o dilema das saídas temporárias”. O trabalho explora o equilíbrio entre os direitos humanos dos detentos e as preocupações com a segurança pública, no contexto das saídas temporárias previstas na Lei de Execução Penal

brasileira, debatendo também sobre as alterações introduzidas pela Lei nº 14.843, de 11 de abril de 2024. As saídas temporárias, um mecanismo que visa a ressocialização dos apenados, têm gerado debates devido aos casos de reincidência criminal durante esses períodos, levantando questões sobre sua eficácia e impacto na segurança pública. O objetivo da pesquisa é analisar como essas saídas são implementadas, seus efeitos na reintegração social dos presos e as dificuldades que apresentam para a segurança pública. As considerações finais destacam a necessidade de aprimorar as políticas de saídas temporárias por meio de uma aplicação mais rigorosa e um monitoramento eficaz, conforme preconizado pela Lei nº 14.843/2024. Além disso, enfatiza que, embora a ressocialização dos detentos seja um objetivo fim, ela não pode ocorrer em detrimento da segurança pública. A integração de medidas adicionais, como o monitoramento eletrônico e a realização de exames criminológicos, são vistas como passos importantes, mas é igualmente essencial que essas práticas sejam acompanhadas por um suporte contínuo aos detentos, garantindo que a reintegração à sociedade seja efetiva e sustentável.

- “Direitos fundamentais e a criminalização da pobreza: o impacto do direito penal nas populações vulneráveis”. Revela-se que, no Brasil, tem-se visto um aumento expressivo nas taxas de criminalidade nas últimas décadas, acompanhado por políticas de segurança pública que se baseiam cada vez mais na repressão e na militarização. Essas estratégias têm exacerbado as desigualdades sociais e ampliado a marginalização das populações vulneráveis, especialmente nas periferias urbanas. Em vez de resolver as causas estruturais da violência, como a pobreza extrema e a falta de acesso a serviços básicos, essas práticas tendem a perpetuar um ciclo de exclusão e violação dos direitos fundamentais. Diante disso, o objetivo do texto é examinar como o direito penal pode discriminar indiretamente as populações vulneráveis, explorando as políticas de criminalização da pobreza e suas implicações para os direitos fundamentais. A análise revelou que, longe de resolver os problemas de segurança pública, as práticas repressivas contribuem para a ampliação das desigualdades sociais, afetando desproporcionalmente as populações negras e pobres. Além disso, a criminalização da pobreza e a seletividade penal evidenciam que o direito penal, quando instrumentalizado de maneira inadequada, pode violar gravemente os direitos fundamentais, como dignidade humana e o devido processo legal, garantidos pela Constituição e pelos tratados internacionais.

- “Inefetividade do acesso à saúde como fundamento para a aplicação obrigatória da teoria da coculpabilidade”. O trabalho analisa a possibilidade de utilizar a inefetividade dos direitos fundamentais, especialmente o direito à saúde, como base para aplicar a atenuante inominada do artigo 66 do Código Penal em casos de infração penal. A falta de acesso aos direitos fundamentais afeta a autodeterminação do indivíduo, sendo a saúde um elemento crucial para

a vida. A vida é o direito fundamental mais importante e a saúde é essencial para mantê-la. O estudo questiona se a Teoria da Coculpabilidade deve ser aplicada em crimes que visam garantir a saúde como requisito para viabilizar a vida. Um dos objetivos é determinar se a aplicação da teoria da coculpabilidade nesses casos pode ser obrigatória, analisando fundamentos jurídicos internos. O estudo se baseia em pesquisa bibliográfica, legislativa e jurisprudencial. Conclui-se que a saúde é fundamental para a vida e a falta de acesso a ela pode levar indivíduos a cometerem crimes, como o furto famélico e desacato, para preservar a própria vida ou de terceiros. Portanto, em casos específicos, a aplicação da Teoria da Coculpabilidade pode ser juridicamente indicada após análise de critérios objetivos.

- “Constituinte para valer tem que ter direitos da mulher: a Constituição cidadã e os direitos das mulheres”. O trabalho analisa o processo de elaboração da Constituição Brasileira de 1988 focando na constitucionalização dos direitos das mulheres. A partir do marco jurídico e político da Assembleia Nacional Constituinte de 1987-1988, analisa-se como se efetivou a política de combate à violência de gênero, considerando, especialmente, a atuação do movimento feminista e da advocacia. O estudo aborda, brevemente, a evolução legislativa, as conquistas jurídicas e os desafios ainda presentes na luta contra a violência de gênero no Brasil. De igual forma, o texto evidencia como a igualdade jurídica entre os gêneros trouxe impactos desde a Constituição federal de 1988 até os dias atuais, incluindo o arcabouço jurídico que vem se formando para consolidar os direitos femininos e coibir a violência contra as mulheres que, a despeito da evolução social e legislativa, segue em crescimento. As conquistas e os esforços da advocacia, sobretudo a advocacia feminina, e as medidas adotadas pelo Conselho Federal e pelas Seccionais da Ordem dos Advogados do Brasil também são objeto de estudo.

- “Reflexões sobre o direito à saúde das pessoas com deficiência privadas de liberdade sob a ótica do caso Chinchila Sandoval v. Guatemala”. O trabalho revela que, no ano de 2016, a Guatemala foi condenada pela Corte Interamericana de Direitos Humanos, em sentença responsabilizando o Estado por violações institucionalizadas aos direitos à integridade pessoal e à vida, que resultou na morte de María Inés Chinchilla Sandoval, enquanto cumpria pena privativa de liberdade. O trabalho foi desenvolvido a partir da seguinte problemática de pesquisa: sob quais aspectos o caso Chinchilla Sandoval versus Guatemala, no âmbito da Corte-IDH, afigura-se como um standard decisório importante para direcionar a efetivação do direito à saúde para pessoas com deficiência no cárcere? Como hipótese inicial, observa-se que as pessoas com deficiência não têm os direitos observados, sendo consideradas hipervulneráveis. O objetivo geral do trabalho é analisar a efetivação do direito à saúde no cárcere, com base na decisão mencionada. Para alcançar o objetivo geral, os objetivos específicos, que correspondem às seções de desenvolvimento do texto, consistem em: a)

apresentar as peculiaridades do Caso analisado, evidenciando os principais elementos; b) analisar os direitos humanos violados no caso investigado e sua repercussão na situação das pessoas com deficiência encarceradas. Conclui-se pela existência de regramento suficiente para o respeito dos direitos da pessoa com deficiência no cárcere (dimensão programadora), mas ausência de concretude desses direitos (dimensão operacional).

- “Hacking legal ou investigativo/lawful hacking: perspectivas a partir da legislação brasileira”. O texto traz uma análise detalhada das questões relacionadas ao lawful hacking ou hacking legal/investigativo e seu papel no contexto do debate conhecido como Going Dark Problem: complexidade derivada do descompasso temporal entre tecnologia e regulação e atuação em investigação criminal, frente à proteção de dados pessoais no ambiente digital. Portanto, o estudo examina as perspectivas favoráveis e contrárias ao uso de técnicas especiais de investigação, como o hacking legal/investigativo e uso das ferramentas de monitoramento remotamente controladas, explorando a complexidade das implicações legais e éticas associadas a essas práticas. É enfatizado que o uso adequado dessas técnicas pode ser compatível com a proteção dos direitos fundamentais dos cidadãos, desde que sejam observados princípios como transparência, proporcionalidade e auditabilidade. Isso inclui a necessidade de supervisão judicial rigorosa e conformidade estrita com requisitos legais. Destaca-se a importância de debate público contínuo e da participação do Poder Legislativo na regulamentação do hacking legal/investigativo, observando-se a necessidade de cooperação internacional e a conformidade com tratados e convenções, como a Convenção de Budapeste, para abordar o cibercrime em escala global.

- “Pena privativa de liberdade e monitoramento eletrônico: desafios e perspectiva na execução penal”. O texto expõe que a pena privativa de liberdade é um instrumento de punição que não tem sido efetivo no Brasil. Isso se deve, em grande parte, à superlotação carcerária, que resulta em condições precárias e indignas nos presídios. Diante da ineficácia da pena privativa de liberdade, notadamente, em razão da superlotação carcerária no Brasil, pergunta-se: a extensão da aplicabilidade do monitoramento eletrônico pode contribuir para a redução das situações precárias e indignas existentes no sistema carcerário, sem repercussão negativa em sociedade? Para isso, o trabalho objetiva verificar se a extensão da aplicabilidade do monitoramento eletrônico pode ser uma medida positiva, desde que seja utilizada de forma responsável e controlada. A medida pode ajudar a reduzir os problemas do sistema carcerário, sem prejudicar os direitos dos presos. Ao final, constatou-se que a aplicabilidade do monitoramento eletrônico deve ser aplicada de forma justa e proporcional, respeitando os direitos dos presos e evitando qualquer forma de tratamento desumano ou degradante.

- “O preço de se violentar uma mulher: as decisões criminais do TJMG envolvendo reparação por danos causados pela violência doméstica contra a mulher perspectivadas pelo Tema 983 do STJ”. A violência doméstica contra a mulher, durante décadas, foi assunto naturalizado e integrado ao cotidiano familiar e relacional no Brasil: algo corriqueiro e, por vezes, justo no contexto doméstico. Graças às intensas reivindicações feministas, desembarcadas no Brasil a partir das décadas de 70 e 80, essa visão passou a ser questionada e, especialmente, neste Século XXI, a ser afastada, sendo emblemática tipificação e a definição da violência doméstica e familiar contra a mulher pela Lei n. 11.340/2006. E, ao menos no plano jurídico-normativo, ganhou força com a edição da Lei 11.719/2008 e a obrigatoriedade de fixação, na sentença condenatória criminal, do valor mínimo para a reparação civil dos danos causados pela infração e, mais recentemente, pela fixação, no Tema 983 pelo STJ do entendimento de que o dano moral, nesses casos consiste em in re ipsa. Próximos do encerramento desse primeiro quarto de século de tantas mudanças no plano jurídico-normativo, necessário faz verificar o efeito prático alcançado por essas medidas, o que justifica verificar se, a edição dos textos legais acima mencionados e da Tese 983 do STJ foram suficientes para a adequação da compreensão dos danos sofridos pela mulher vítima de violência a partir das perspectivas feministas e a sua consequente conversão em reparações judiciais em valores minimamente compatíveis com sua gravidade. O que fazemos, nesta pesquisa, a partir de uma perspectiva qualitativa e do uso do método bibliográfico-documental, por meio da leitura das decisões do TJMG.

- “Mensagens de aplicativos de mensageria como provas no processo penal: uma análise de decisões do STJ”. O trabalho analisa a utilização de mensagens de aplicativos de mensageria como prova no processo penal, com foco em decisões do Superior Tribunal de Justiça (STJ). O objetivo é analisar a eventual (in)admissibilidade e (in)validade dessas provas, examinando os parâmetros e diretrizes estabelecidos pelo tribunal, realizando uma análise técnica dos pressupostos e afirmações constantes do julgamento do Habeas Corpus n. 99.735/SC e do Agravo Regimental no Habeas Corpus n. 828.054/RN, especialmente sobre pontos tecnológicos. O estudo emprega uma análise bibliográfica e documental, utilizando métodos indutivo-dedutivo para analisar casos concretos e alcançar conclusões. A pesquisa destaca a importância do STJ na uniformização da jurisprudência e aborda as decisões colegiadas mais relevantes, apontando acertos e erros técnicos, como, por exemplo, o desconhecimento sobre os registros de conexão existentes e acessíveis ou o desconhecimento acerca do fenômeno da irrepetibilidade de hash em aparelhos celulares. Conclui-se que é imprescindível a análise técnica das decisões do STJ sobre provas digitais e a difusão de conhecimentos técnicos para melhorar a interpretação e aplicação dessas provas nos processos judiciais.

- “Estupro de vulnerável e gravidez: a dignidade da criança e do adolescente sob a perspectiva da jurisprudência”. O texto busca estudar o crime de estupro de vulnerável com enfoque na jurisprudência do Superior Tribunal de Justiça e na aplicação desta na justiça amapaense nas hipóteses em que a violência sexual resulta gravidez. A pesquisa apresenta a evolução do preceito normativo que tipifica a violência sexual contra a pessoa menor de 14 (catorze) anos, o conceito jurídico de vulnerabilidade e a possibilidade de relativização e, por fim, realiza a análise dos julgados à luz do dever de proteção integral da criança e da adolescente. Propôs-se a interpretação da norma penal em cotejo com os princípios constitucionais basilares que impõem uma postura ativa contra todas as formas de violência, em reforço ao compromisso do Estado brasileiro com as normas internacionais de proteção à infância e à adolescência.

Sendo esses os trabalhos que compõem o livro, afirma-se a certeza de que esta publicação fornece importantes instrumentos para que pesquisadores e aplicadores do Direito enriqueçam ainda mais os seus conhecimentos. Em razão disso, os organizadores desta obra prestam sua homenagem e agradecimento ao Conselho Nacional de Pesquisa e Pós-Graduação em Direito (CONPEDI) e, em especial, a todos os autores que participaram da presente coletânea.

Brasília, primavera de 2024.

Celso Hiroshi Iocohama – Universidade Paranaense – UNIPAR celso@prof.unipar.br

Luiz Gustavo Gonçalves Ribeiro – Dom Helder-Escola Superior lgribeirobh@gmail.com

Matheus Felipe de Castro – Universidade Federal de Santa Catarina matheusfelipedecastro@gmail.com

MENSAGENS DE APLICATIVOS DE MENSAGERIA COMO PROVAS NO PROCESSO PENAL: UMA ANÁLISE DE DECISÕES DO STJ

APP'S MESSAGES AS EVIDENCE IN CRIMINAL PROCEEDINGS: A ANALYSIS OF THE STJ COURT DECISIONS

Fabrício Lamas Borges da Silva
Emerson Wendt

Resumo

O trabalho analisa a utilização de mensagens de aplicativos de mensageria como prova no processo penal, com foco em decisões do Superior Tribunal de Justiça (STJ). O objetivo é analisar a eventual (in)admissibilidade e (in)validade dessas provas, examinando os parâmetros e diretrizes estabelecidos pelo tribunal, realizando uma análise técnica dos pressupostos e afirmações constantes do julgamento do Habeas Corpus n. 99.735/SC e do Agravo Regimental no Habeas Corpus n. 828.054/RN, especialmente sobre pontos tecnológicos. O estudo emprega uma análise bibliográfica e documental, utilizando métodos indutivo-dedutivo para analisar casos concretos e alcançar conclusões. A pesquisa destaca a importância do STJ na uniformização da jurisprudência e aborda as decisões colegiadas mais relevantes, apontando acertos e erros técnicos, como, por exemplo, o desconhecimento sobre os registros de conexão existentes e acessíveis ou o desconhecimento acerca do fenômeno da irrepetibilidade de hash em aparelhos celulares. Conclui-se que é imprescindível a análise técnica das decisões do STJ sobre provas digitais e a difusão de conhecimentos técnicos para melhorar a interpretação e aplicação dessas provas nos processos judiciais.

Palavras-chave: Admissibilidade probatória, Aplicativos de mensageria, Prova digital, Superior tribunal de justiça

Abstract/Resumen/Résumé

This paper analyzes the use of messages from messaging apps as evidence in criminal proceedings, focusing on the decisions of the Superior Tribunal de Justiça (STJ), an Brazilian Superior Court. The objective is to analyze the possible (in)admissibility and (in)validity of this evidence, examining the parameters and guidelines established by the court, carrying out a technical analysis of the assumptions and statements of Habeas Corpus n. 99.735/SC and the Agravo Regimento no Habeas Corpus n. 828.054/RN, especially on technological points. The study employs a bibliographic and documentary analysis, using inductive-deductive methods to analyze concrete cases and reach conclusions. The research highlights the importance of the STJ in standardizing jurisprudence and addresses the most relevant collegiate decisions, pointing out technical successes and erros, such as, for example, the lack of knowledge about existing and accessible connection records or the lack of knowledge about the phenomenon of hash unrepeatability on mobile phones. The conclusion is that it is

essential to technically analyse the STJ's decisions on digital evidence and to disseminate technical knowledge in order to improve the interpretation and application of this evidence in court cases.

Keywords/Palabras-claves/Mots-clés: Digital evidence, Evidentiary admissibility, Messaging apps, Superior tribunal de justiça

1 INTRODUÇÃO

Com o advento do computador ENIAC em 1946, passando pelo surgimento internet atual com o protocolo TCP/IP (Wendt; Jorge, 2021) até a popularização do uso de smartphones e da internet móvel, o ser humano tem vivenciado uma revolução tecnológica sem precedentes, que alterou a forma com os seres humanos realizam quase todas as suas atividades cotidianas[1].

Todavia, pouca coisa mudou tanto como a forma pela qual as pessoas se comunicam com o uso dos aplicativos de mensageria para o envio de mensagens e arquivos. Para se ter ideia, de acordo com o relatório Brasil 2024 Digital (Kemp, 2024), no início do ano de 2024, 93,4% da população brasileira com acesso a smartphones utilizava o aplicativo de mensageria Whatsapp, o mais popular, para troca de mensagens e arquivos, enquanto seus concorrentes Facebook Messenger e Telegram possuíam a expressiva quantidade de uso por, respectivamente, 60,8% e 56,5% dos brasileiros com acesso aos referidos aparelhos.

Assim, pode-se afirmar que a maioria dos brasileiros utiliza os aplicativos de mensageria como forma de comunicação regular.

Além disso, soma-se o fenômeno de migração da parcela da criminalidade do mundo físico para o mundo digital, com quantidade expressiva de crimes cibernéticos[2] e, ainda, o fato de aplicativos de mensageria serem utilizados, por vezes, como meio para a prática de crimes diversos como, por exemplo, ameaças enviadas por meio de mensagens ou estelionatos virtuais. Também, vem sendo comum o uso destes aplicativos como meio de comunicação dos criminosos entre si, especialmente nas associações e organizações criminosas complexas.

Assim, se tornou frequente a coleta e a análise de registros de mensagens de aplicativo de mensageria como meio de prova relacionado à prática de crimes diversos.

Neste cenário, o Superior Tribunal de Justiça - STJ - enquanto órgão jurisdicional responsável pela interpretação da legislação da infraconstitucional brasileira tem se debruçado sobre o tema, dando decisões, por vezes, acerca da (in)admissibilidade e (in)validade das provas

[1] No início dos anos 2000, por exemplo, ninguém – ou quase ninguém - sabia o que era EAD, *homework*, *streamers*, redes sociais, influencers ou aplicativos de mensageria, termos comuns hoje à maioria dos brasileiros. O mundo digital e a internet mudaram a forma como estudamos, trabalhamos, assistimos filmes, ouvimos música, nos relacionamos e adquirimos bens e serviços.

[2] Para se ter ideia, de acordo com o Anuário Brasileiro de Segurança Pública de 2023 (FBSP, 2023), o Brasil registrou em 2023 uma redução de crimes patrimoniais contra instituições financeiras (-21,9%), estabelecimentos comerciais (-15,6%), cargas (-4,4%), residências (-13,3%) e transeuntes (-4,4%), enquanto, por sua vez, os dados apontados pela FirtGuard Labs (Fortinet, 2024) apontaram que no mesmo ano o Brasil teve mais de 103,1 bilhões (cento e três bilhões e cem milhões) de tentativas de ataques cibernéticos contra brasileiros, incluindo ali crimes cibernéticos dos mais variados.

advindas de aplicativos de mensageria, criando parâmetros a serem seguidos e oferecendo diretrizes aos operadores do direito.

Diante disso, questiona-se, como problema que este trabalho buscará responder: quais os parâmetros que o STJ tem adotado sobre a admissibilidade e validade das provas advindas de aplicativos de mensageria e, caso existentes, se baseariam eles em pressupostos e conclusões legais e fáticas corretas?

Responder a esta pergunta é o mote deste artigo que, partindo do método indutivo-dedutivo, analisando casos para se chegar a conclusões, por meio da análise bibliográfica e documental, busca analisar os julgados mais relevantes decididos de forma colegiada pelo Superior Tribunal de Justiça acerca da (in)validade e (in)admissibilidade destas provas.

2 AS DECISÕES DO SUPERIOR TRIBUNAL DE JUSTIÇA NA ANÁLISE DAS PROVAS DE APLICATIVOS DE MENSAGERIA

No desenho constitucional da jurisdição brasileira, o Poder Constituinte de 1988 atribuiu importantes missões ao STJ, sendo aquela corte responsável por julgar *habeas corpus* decididos pelos Tribunais de Justiça dos Estados e Tribunais Regionais Federais, em última ou única instância, e, ainda, por julgar *recurso especial* de decisões que contrariem leis federais ou sejam motivo de interpretação divergente entre tribunais diversos, nos termos do referido artigo 105, incisos II, alínea "a" e III, alínea "b" (Brasil, 1988), o que lhe torna responsável por uniformizar a jurisprudência brasileira sobre diversos temas.

Assim, é inquestionável a importância e o papel do referido tribunal, assim como de suas decisões no desenho processual penal brasileiro, com seus eventuais acertos e desacertos ganhando contornos que se multiplicam em decisões por todo o país.

É o que ocorre no que diz respeito também à utilização de provas advindas de aplicativos de mensageria, cujos parâmetros estabelecidos pelo STJ tendem a ser observados e replicados por operadores do direito do país inteiro, criando balizas para outros atores processuais.

Neste sentido, este trabalho, sem a intenção de esgotar o tema, analisará duas de suas decisões colegiadas, a saber, o Recurso em Habeas Corpus n. 99.735/SC (Brasil, 2018) e o Agravo Regimental no Habeas Corpus n. 828.054/RN (Brasil, 2024).

2.1 O Recurso em Habeas Corpus 99.735/SC – a decisão colegiada pioneira sobre o tema, sua abrangência e seus (des)acertos técnicos

O Recurso em Habeas Corpus n. 99.735 (Brasil, 2018), originário de Santa Catarina, foi a primeira decisão colegiada do STJ a tratar de mensagens de aplicativos de mensageria como prova no processo penal e é utilizado até hoje como paradigma para outras decisões. Segue trechos da ementa, de relatoria da Ministra Laurita Vaz, da 6ª Turma (Brasil, 2018):

> [...]AUTORIZAÇÃO JUDICIAL DE ESPELHAMENTO, VIA **WHATSAPP WEB**, DAS CONVERSAS REALIZADAS PELO INVESTIGADO COM TERCEIROS. ANALOGIA COM O INSTITUTO DA INTERCEPTAÇÃO TELEFÔNICA. IMPOSSIBILIDADE. PRESENÇA DE DISPARIDADES RELEVANTES. **ILEGALIDADE DA MEDIDA**. RECONHECIMENTO DA NULIDADE DA DECISÃO JUDICIAL E DOS ATOS E PROVAS DEPENDENTES. [...]. 4. **Tanto no aplicativo, quanto no navegador, é possível, com total liberdade, o envio de novas mensagens e a exclusão de mensagens antigas (registradas antes do emparelhamento) ou recentes (registradas após), tenham elas sido enviadas pelo usuário, tenham elas sido recebidas de algum contato**. **Eventual exclusão de mensagem enviada (na opção "Apagar somente para Mim") ou de mensagem recebida (em qualquer caso) não deixa absolutamente nenhum vestígio, seja no aplicativo, seja no computador emparelhado**, e, por conseguinte, **não pode jamais ser recuperada para efeitos de prova em processo penal**, **tendo em vista que a própria empresa disponibilizadora do serviço, em razão da tecnologia de encriptação ponta-a-ponta, não armazena em nenhum servidor o conteúdo das conversas dos usuários**. [...], no espelhamento via WhatsApp Web **o investigador de polícia tem a concreta possibilidade de atuar como participante tanto das conversas que vêm a ser realizadas quanto das conversas que já estão registradas no aparelho celular**, [...]. 8. **O fato de eventual exclusão de mensagens enviadas (na modalidade "Apagar para mim") ou recebidas (em qualquer caso) não deixar absolutamente nenhum vestígio nem para o usuário nem para o destinatário, e o fato de tais mensagens excluídas, em razão da criptografia end-to-end, não ficarem armazenadas em nenhum servidor, constituem fundamentos suficientes para a conclusão de que a admissão de tal meio de obtenção de prova implicaria indevida presunção absoluta da legitimidade dos atos dos investigadores, dado que exigir contraposição idônea por parte do investigado seria equivalente a demandar-lhe produção de prova diabólica**. [...] – (destaques nossos).

Em apertada síntese, esta decisão, que cuida exclusivamente do uso de Whatsapp Web para a coleta de evidências digitais, julgou um caso de uma ação penal em que, com autorização judicial, policiais coletaram mensagens por meio de Whatsapp com o uso do aplicativo Whatsapp Web, considerando o STJ que esta prova não deveria ser admitida nos autos.

A decisão não diz quais normas ou regramentos específicos teriam sido eventualmente violados na produção probatória e parece não estar em harmonia com o princípio da liberdade

probatória do processo penal[3]. Ela também é pouco didática do ponto de vista prático, pois diz o que não deveria ter ocorrido sem falar o que poderia ser feito no lugar, de modo que alguém que lê a decisão com a genuína intenção de buscar parâmetros nada retira sobre como agir.

Sem falar que a decisão, ao optar pela vedação de um meio de prova, parece também não estar em melhor sintonia com o princípio da persuasão racional da prova adotado no Brasil, que prevê que uma prova poderá ter maior ou menor valor probatório a depender da confiabilidade dela e de sua análise em conjunto com outros elementos existentes nos autos[4].

A decisão, ademais, tem como pressupostos: 1) que os agentes estatais que coletaram a prova poderiam, em tese, pelo método adotado, alterar os elementos probatórios coletados e que; 2) a possibilidade disso, em tese e independentemente de qualquer elemento em concreto, seria suficiente para tornar esta prova como inadmissível.

Como primeira crítica, nota-se que a decisão não apresenta qualquer dado acadêmico ou empírico que comprove eventual facilidade em se alterar evidências digitais por parte de policiais ou cidadãos comuns[5]. Também não apresenta pelo menos um único caso, no Brasil ou no mundo, em que isso tenha ocorrido.

A realidade é oposta, pois estudos existentes sobre o tema, como o elaborado por Wendt (2023), aplicado a profissionais de delegacias especializadas em crimes cibernéticos do país, demonstram que mesmo em relação a tais profissionais – de áreas especializadas – há dificuldades em se capacitar de forma continuada.

Se não bastasse, outro ponto que demonstra ser equivocado o raciocínio que a mera possibilidade de facilidade de alteração de uma prova digital deveria conduzir ao seu descarte

[3] Neste sentido, dispõe a doutrina que: [...] quanto aos meios de prova, vigora no processo penal ampla liberdade probatória, podendo a parte se valer tanto de meios de prova nominados, quanto de meios inominados. O parágrafo único do art. 155 do CPP reforça essa liberdade probatória quanto aos meios, ao dispor que somente quanto ao estado das pessoas serão observadas as restrições estabelecidas na lei civil. A *contrario sensu*, portanto, desde que o objeto da prova não verse sobre o estado das pessoas, qualquer meio de prova poderá ser utilizado. Obviamente, esses meios de prova devem ter sido obtidos de maneira lícita e com respeito à ética e à moral, haja vista o preceito constitucional que veda a admissibilidade no processo de provas obtidas por meios ilícitos (CF, art. 5º, LVI) (Lima, 2019, 672-674).

[4] Neste sentido, dispõe a doutrina que: "[...] o juiz é livre na formação de seu convencimento, não estando comprometido por qualquer critério de valoração prévia da prova, podendo optar livremente por aquela que lhe parecer mais convincente. Um único testemunho, por exemplo, poderá ser levado em consideração pelo juiz, ainda que em sentido contrário a dois ou mais testemunhos, desde que em consonância com outras provas [...] o livre convencimento motivado é regra de julgamento, a ser utilizada por ocasião da decisão final, quando se fará a valoração de todo o material probatório levado aos autos [...] (Oliveira, 2014, 340-341).

[5] Muito se fala na doutrina processual brasileira sobre uma eventual facilidade em se alterar provas digitais. Não existe pesquisa, contudo, demonstrando a quantidade de pessoas comuns (não formados em áreas de tecnologia) que disponham deste tipo de conhecimento.

ocorre quando levamos esta mesma premissa para as provas mais utilizadas na prática forense, a saber, a prova testemunhal e a prova documental.

É de conhecimento notório que para alterar uma versão uma testemunha não precisa de nada além do que saber se comunicar e ter vontade de mentir. Nem por isso a coleta de depoimentos é inadmissível em ações penais, onde a prova é coletada regularmente e analisada em cotejo com as demais provas existentes nos autos. Aliás, ousa a lógica entender ser mais fácil alterar uma prova digital – o que exige conhecimentos informáticos mínimos – do que alterar um depoimento testemunhal.

A alteração documental, de igual modo, especialmente quanto aos documentos particulares (como instrumentos de procuração particulares, livros escriturais contábeis, agendas), também exige pouca habilidade e ocorre no processo penal com frequência suficiente para o legislador brasileiro ter inserido um incidente específico para tratar sobre o tema, constante no artigo 145 do Código de Processo Penal.

Todavia, a possibilidade de alteração das provas testemunhais ou documentais não gera seu descarte ou invalidade automática, mas sim um valor relativo em cotejo com outros elementos probatórios, conforme o sistema de persuasão racional adotado no Brasil, ignorado pelo STJ quanto a provas advindas de aplicativos de mensageria.

Outro ponto importante do julgado, diz respeito a como sua abrangência tem sido encarada no ordenamento jurídico. Da leitura da ementa e voto, nota-se que a decisão aborda tão somente o uso de *print screen* (fotografia da tela) feito por agente estatal por meio da ferramenta Whatsapp Web, tratando das peculiaridades que esta ferramenta possui.

Apesar de ser bem óbvio, convém lembrar que um *print screen*, enquanto arquivo digital contendo a imagem da tela de dispositivo é só uma das espécies de provas digitais, não sendo todas as espécies de provas digitais abrangidas por esta decisão.

Também há diferença entre *print screen* (gênero), que pode ser relacionado a inúmeros aplicativos ou softwares (como *print screen* de rede social ou de SMS ou mesmo de ligação telefônica realizada) dos *print's screen's* específicos de Whatsapp (subgênero), que pode ser do Whatsapp Web (espécie) feito da tela de um computador, do *print* do Whatsapp App feito no celular que está a mensagem (espécie).

Logo, o julgado não cuida de todo e qualquer *print screen* e não diz ser ilícito o uso de qualquer *print screen* ou mesmo de qualquer *print screen de WhatsApp* (inclusive móvel) como prova no processo penal. Apesar disso, esta decisão já foi utilizada no STJ como fundamento

para entender que a jurisprudência daquele tribunal considera "*print screen*" como uma prova ilícita[6].

Outros pontos relevantes a serem analisados em relação a este julgado são os aparentes equívocos técnicos, mais especificamente existentes nas seguintes afirmações sobre o WhatsApp Web feitos pelo STJ: 1) que é possível "com total liberdade o envio de novas mensagens"; 2) que é possível "com total liberdade a exclusão de mensagens antigas (registradas antes do emparelhamento) ou recentes (registradas após)"; 3) que esta atividade "não deixa absolutamente nenhum vestígio, seja no aplicativo seja no computador emparelhado" e que em decorrência da criptografia o conteúdo não fica armazenado em nenhum servidor (Brasil, 2018).

Em primeiro lugar, convém ressaltar que não há plena liberdade de apagar conteúdo enviado no WhatsApp Web. Detalhando, em uma conversa entre duas pessoas, em relação ao destinatário da mensagem (a outra parte da conversa), somente é possível apagar mensagens enviadas até 2 (dois) dias do acesso, conforme explicita a própria plataforma WhatsApp (2024).

Passado este prazo, não é mais possível apagar as mensagens no outro aparelho, o que nos permite inferir que há equívoco quando o STJ afirma existir "plena liberdade" para apagar mensagens enviadas ou que seria impossível acessar o conteúdo desta mensagem, já que uma mensagem não apagada permaneceria em regra no outro aparelho.

Além disso mesmo que seja apagada dentro deste curto período em que isso é possível (em 2 dias), ainda assim WhatsApp deixará registrado no celular do destinatário uma prova que uma mensagem foi enviada e apagada pelo remetente, nos moldes demonstrados na figura a seguir:

Figura 1: representação visual de mensagem apagada pelo remetente

Fonte: produzida pelos autores[7].

[6] Cita-se, como exemplo, a decisão monocrática o Agravo em Recurso Especial n. 2.441.511, de Relatoria da Ministra Daniela Teixeira (Brasil, 2024), em que ela cita expressamente, que: "a utilização de "prints" de mensagens, mesmo que realizados pela autoridade policial, viola a cadeia de custódia prevista nos artigos 158 e ss. do CPP e é prova ilícita de acordo com os precedentes desta Corte(...)" – destacou-se. Para fundamentar sua decisão, a ministra cita expressamente o HC 99.735/SC.

[7] A presente mensagem foi produzida pelos autores a partir de um recorte de *print screen* de aparelho pessoal.

Passado este período, somente é possível apagar uma mensagem enviada exclusivamente no próprio dispositivo, o que, por óbvio, não interferiria na cópia do registro da mensagem no outro celular envolvido na conversa (o outro aparelho que enviou ou recebeu a mensagem). Assim, não há plena liberdade para apagar mensagens enviadas, existindo limites técnicos e temporais importantes.

Outro ponto técnico relevante é que, apesar de ser possível, via WhatsApp Web, que a pessoa que está acessando o dispositivo envie novas mensagens, há limitações técnicas e temporais, não existindo plena liberdade para o envio de novas mensagens, como mencionado.

Estas novas mensagens enviadas, na hipótese ventilada pelo STJ, possuirão data e horário determinado e salvo no aplicativo, não sendo possível tecnicamente a um agente estatal ou a qualquer pessoa, por exemplo, inserir uma mensagem pretérita no aplicativo Whatsapp via Whatsapp Web, com data pretérita ao acesso realizado, por exemplo.

Isso deveria ser, em uma análise crítica e técnica, cotejado no caso concreto, onde será possível aferir se uma mensagem questionada seria anterior ou posterior ao eventual acesso de agente público à plataforma do Whatsapp Web, não existindo lógica em atribuir mensagens anteriores ao acesso a um policial, já que ele não poderá fazê-lo.

Detalhando, se um agente estatal acessou um dispositivo via Whatsapp Web no dia 1 de fevereiro de 2024, ele até conseguiria em tese enviar uma mensagem nova, mas esta mensagem teria o registro de data e hora específico do envio, tanto visualmente como em metadado registrado no aplicativo.

Neste caso do exemplo, ele não conseguira acrescentar uma mensagem incriminadora como se enviada, *e.g.*, no dia 24 de janeiro de 2024, o que tecnicamente descarta a hipótese de plena liberdade para o envio de mensagens.

No exemplo mencionado, ao se debruçar sobre esta prova quando houver, por exemplo, uma eventual impugnação a uma mensagem, o Poder Judiciário teria plenas condições de solicitar a análise dos dados e metadados da mensagem e, diante disso, excluir eventual prova que houver sido eventualmente criada por terceiro, o qual inclusive deverá responder pelo crime de fraude processual, previsto no artigo 347 do Código Penal (Brasil, 1941).

No mais, ao contrário do que afirma o acórdão, alterações de mensagens deixam registros que podem ser analisados em um caso em concreto.

Neste sentido, é possível conferir quando um dispositivo novo acessou o WhatsApp web de alguma conta, de duas formas distintas.

A primeira delas é por meio dos registros de conexão da plataforma, que registram o IP[8] e o dispositivo acessado pelo prazo mínimo de 6 (seis) meses, conforme determina o Marco Civil da Internet, em seu artigo 15.

Assim, a plataforma armazena obrigatoriamente a informação dos dispositivos que acessaram a conta e o IP utilizado, podendo preservar e fornecer esses dados sempre que houver pedido, mediante autorização judicial.

A segunda possibilidade de registro, menos conhecida, é por meio do relatório de conta que poderá ser obtido pelo proprietário da conta no WhatsApp App. Neste sentido, o WhatsApp disponibiliza em sua plataforma, para qualquer usuário, o relatório de registro de acesso de sua conta, narrando todos os dispositivos que acessaram e o respectivo IP.

Este relatório pode ser solicitado nas configurações do próprio aplicativo, acessando o menu conta e, em seguida, a opção solicitar dados da conta.

Se o usuário seguir estas etapas bastará esperar alguns dias para ter acesso completo ao relatório de sua conta, sendo possível, assim, ter acesso a uma prova técnica que alguém utilizou indevidamente o WhatsApp Web.

Neste relatório, estarão enumerados os dispositivos que acessaram[9], com nome técnico do dispositivo de celular e os endereços de IP relativo a cada dispositivo.

O WhatsApp, assim, documenta e disponibiliza aos usuários os dispositivos e os IP's que acessaram, entregando os registros de acesso. Veja-se um exemplo[10].

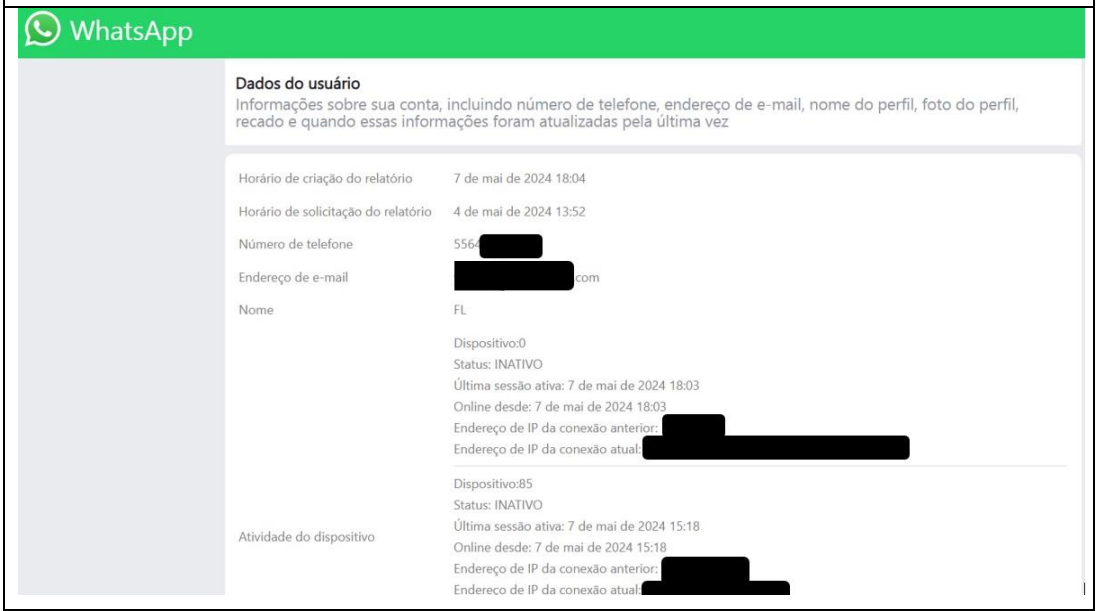
[8] IP ou *Internet Procol* se trata, grosso modo, de um identificador necessário para acesso à internet, por meio do qual é possível identificar dispositivos que fizeram acesso.

[9] O app denomina o dispositivo de celular, gerador da chave de criptografia, como "dispositivo:0" e os demais dispositivos web, em sequência, como "dispositivo:1", "dispositivo:2", criando um código novo a cada dispositivo.

[10] Dados pessoais sensíveis foram anonimizados, nos termos do artigo 11 da Lei Geral de Proteção de Dados.

Quadro 1: imagem do relatório de conta do WhatsApp

Relatório do WhatsApp de acesso à conta



Fonte: produzido pelos autores (2024)[11].

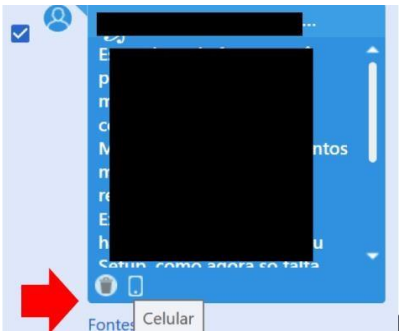
Logo, a possibilidade ventilada pelo julgado de que um agente estatal que poderia inserir mensagens no WhatsApp de terceiros deixaria sim registros, sendo um equívoco técnico a afirmação do STJ que acessos de WhatsApp Web "não deixa absolutamente nenhum vestígio", como afirmou o julgado em estudo.

Se não bastasse, há de se ressaltar que, conforme já mencionamos, dentro dos metadados das próprias mensagens no aparelho, há o registro do dispositivo que enviou de modo que, inclusive, softwares como o UFED, da empresa israelense Cellebrite, conseguem identificar facilmente e automaticamente se uma mensagem foi enviada de um aparelho celular ou de outro dispositivo web.

Veja a seguir uma colagem do UFED:

[11] Imagem extraída do relatório da conta de um autor, solicitados nos moldes descritos no presente artigo.

Quadro 2: exibição de como as conversas aparecem no UFED

Forma que fica a mensagem via WhatsApp Web no UFED	**Forma como fica a mensagem via Celular no UFED**
	

Fonte: produzido pelos autores (2024) [12]

Assim, se alguém inserisse uma mensagem em WhatsApp alheio para incriminar alguém isso deixaria vestígios, tanto de conexão (junto à plataforma WhatsApp ou no relatório acessível ao usuário) como nos metadados da própria mensagem. Logo, a informação do acordão que constituiria uma "prova diabólica", impossível de ser feita, a eventual demonstração que alguém inseriu alguma mensagem em WHATSAPP alheio não condiz com a realidade, sendo uma incorreção técnica.

Outro ponto do julgado que entendemos ter ocorrido uma afirmação técnica equivocada é a de que não haveria registro dessas conversas em decorrência da criptografia de ponta-a-ponta. Isso porque a criptografia do aplicativo WhatsApp impede tão somente a leitura do teor dos conteúdos enviados por agentes externos, mas isso não significa necessariamente que as conversas não ficam armazenadas em nenhum servidor.

Detalhando, apesar das mensagens de WhatsApp serem criptografadas, é possível que os usuários do WhatsApp tenham *backup*[13], por vezes automático, que pode ocorrer no próprio dispositivo, em um computador ou nos servidores da Google (celulares android) ou iCloud

[12] A imagem foi extraída de uma investigação sigilosa em curso em que um dos autores está trabalhando. Possui dados sensíveis que foram anonimizados, nos termos do artigo 11 da Lei Geral de Proteção de Dados. Também, foram tarjados dados que permitam a eventual identificação da conversa, em razão do sigilo da investigação.
[13] Termo da informática designado para cópias de segurança.

(celulares Iphone), dentre outros[14]. Este backup, em regra, armazena conversas despidas de qualquer criptografia[15]

Logo, a informação constante no acordão que as mensagens do WhatsApp não ficam armazenadas em nenhum servidor em decorrência da criptografia também não é uma afirmação totalmente correta e esta situação poderia ser analisada em um caso concreto.

2.2 Agravo Regimental no Habeas Corpus n. 828.054/RN e suas incorreções técnicas

Outra decisão importante para se entender a questão trabalhada neste artigo é o Agravo Regimental no Habeas Corpus n. 828054-RN, de relatoria do Ministro Joel Paciornik, julgado pela 5ª turma do STJ, em 23 de abril de 2024 (Brasil, 2024). Segue trechos da ementa:

> PROCESSUAL PENAL. AGRAVO REGIMENTAL NO HABEAS CORPUS. TRÁFICO DE DROGAS. **APREENSÃO DE CELULAR. EXTRAÇÃO DE DADOS**. **CAPTURA DE TELAS**. **QUEBRA DA CADEIA DE CUSTÓDIA**. **INADMISSIBILIDADE DA PROVA** DIGITAL. AGRAVO REGIMENTAL PROVIDO. 1. O **instituto da cadeia de custódia** visa a garantir que o tratamento dos elementos probatórios, desde sua arrecadação até a análise pela autoridade judicial, seja idôneo e livre de qualquer interferência que possa macular a confiabilidade da prova. 2. Diante da **volatilidade dos dados telemáticos e da maior suscetibilidade a alterações**, **imprescindível se faz a adoção de mecanismos que assegurem a preservação integral dos vestígios probatórios**, **de forma que seja possível a constatação de eventuais alterações, intencionais ou não, dos elementos inicialmente coletados**, demonstrando-se a higidez do caminho percorrido pelo material. 3. **A auditabilidade, a repetibilidade, a reprodutibilidade e a justificabilidade são quatro aspectos essenciais das evidências digitais, os quais buscam ser garantidos pela utilização de metodologias e procedimentos certificados, como, e.g., os recomendados pela ABNT**. 4. A observação do princípio da **mesmidade** visa a assegurar a confiabilidade da prova, **a fim de que seja possível se verificar a correspondência entre aquilo que foi colhido e o que resultou de todo o processo de extração da prova de seu substrato digital**. **Uma forma de se garantir a mesmidade dos elementos digitais é a utilização da técnica de algoritmo hash, a qual deve vir acompanhada da utilização de um software confiável, auditável e amplamente certificado, que**

[14] É este *backup* faz com que usuários tenham suas conversas armazenadas em outros dispositivos e é ele que garante, por exemplo, que a maioria das pessoas tenham todo seu histórico de conversas recuperado ao comprar um novo aparelho telefônico.

[15] Detalhando, uma conversa existente no backup só será criptografada se houver configurações específicas feitas pelo usuário (se seguir os seguintes passos: configurações > conversa > backup de conversas > backup criptografado de ponta a ponta > ativar > criar senha específica). Esta configuração não é sequer fácil de ser feita por usuários comuns. Se feita, ainda assim, a chave de criptografia específica do backup teria sido configurada e criada pelo próprio usuário (eventual vítima de uma incriminação injusta), o que lhe possibilitaria ter acesso à chave que reabriria suas mensagens. Assim, se esta configuração for feita, eventual cidadão incriminado injustamente terá a senha e poderá utilizar o backup para fins de apresentação de contraprova.

> **possibilite o acesso, a interpretação e a extração dos dados do arquivo digital**. [...] – destaques nossos.

Em apertadíssima síntese, a decisão entendeu que na análise dos elementos oriundos de aplicativo de mensageria de um aparelho celular, em um caso concreto, teria ocorrido quebra da cadeia de custódia digital. Assim, o tribunal sugeriu que a análise das provas digitais deveria ser garantida por métodos como os constantes das normas da Associação Brasileira de Normas Técnicas – ABNT. Ainda, sugeriu expressamente a adoção do mecanismo "hash", o qual possibilitaria, de acordo com o STJ, a garantia do princípio da mesmidade na análise[16].

Esta decisão, assim no RHC 99.034/SC, partiu do pressuposto que provas digitais seriam mais suscetíveis a alterações do que provas comuns e que isso poderia justificar, independentemente de qualquer elemento em concreto, sua invalidade, o que discordamos, conforme detalhado no tópico anterior.

A decisão também abordou sobre eventual violação da cadeia de custódia da prova digital. Todavia, não há no Brasil qualquer previsão legal sobre regras específicas para a cadeia de custódia da prova digital[17]. Logo, parece desarrazoado entender que houve uma violação às regras de cadeia de custódia da prova digital em um caso concreto se estas regras, do ponto de vista normativo, nem sequer existem no nosso ordenamento.

Se houvesse tais regras, ainda assim, haveria de se ressaltar que o próprio STJ entende que uma violação da cadeia de custódia, por si só, não necessariamente gera uma nulidade, sendo necessário avaliar uma violação e seus efeitos em concreto[18].

---

[16] Os conceitos de hash e princípio da mesmidade serão detalhados adiante neste artigo.

[17] A legislação sobre cadeia de custódia, nos artigos 158-A ao 158-F do Código de Processo Penal (Brasil, 1941), não traz qualquer dispositivo específico sobre o tema, prevendo somente etapas relacionadas à prova material comum (coleta, preservação, rastreio etc.)

[18] Neste sentido, por exemplo, é o entendimento do HC 653.515-RJ (Brasil, 2023), de relatoria do Ministro Rogério Schietti Cruz: HABEAS CORPUS. [...] **QUEBRA DA CADEIA DE CUSTÓDIA DA PROVA. AUSÊNCIA DE LACRE**. [...] o caso dos autos traz hipótese em que houve uma desconformidade entre o procedimento usado na coleta e no acondicionamento de determinadas substâncias [...] 5. Se é certo que, por um lado, o legislador trouxe, nos arts. 158-A a 158-F do CPP, determinações extremamente detalhadas de como se deve preservar a cadeia de custódia da prova, também é certo que, por outro, **quedou-se silente em relação aos critérios objetivos para definir quando ocorre a quebra da cadeia de custódia e quais as consequências jurídicas**, para o processo penal, dessa quebra ou do descumprimento de um desses dispositivos legais. [...] 7. **Mostra-se mais adequada a posição que sustenta que as irregularidades constantes da cadeia de custódia devem ser sopesadas pelo magistrado com todos os elementos produzidos na instrução, a fim de aferir se a prova é confiável**. [...] – destacou-se

Outro ponto a ser destacado é que o julgamento cita que deveria ser utilizado, como complemento legislativo, no contexto das provas digitais, procedimentos certificados, como as normas da ABNT.

Sobre isso, convém ressaltar que a ausência de legislação específica sobre o tema não parece indicar que o STJ poderia escolher uma norma para ser cumprida, diante da competência constitucional do Supremo Tribunal Federal de cuidar de inconstitucionalidade por omissões legislativas[19]. No mais, ainda que o STJ pudesse escolher uma diretriz para criar regras procedimentais, não parece ser uma conduta racional exigir que isso se aplique a casos anteriores a uma decisão que defina estes parâmetros. Sendo mais claro, não parece lógico exigir que os agentes de força da lei, anos antes de uma decisão, sejam capazes de adivinhar que o STJ considerará exigível como norma suplementar em uma data futura.

Outro ponto a ser ressaltado é que a ABNT cobra valor pecuniário para o acesso às suas diretrizes sobre provas digitais. Logo, tratar as normas da ABNT que cuidam do tema como lei e exigir seu cumprimento significa a adoção de uma norma de acesso restrito, o que viola a exigência de publicidade das normas em vigor[20]. Para se ter ideia, considerando as principais normas das organizações associativas de parâmetro (ABNT e suas associadas ISO e IEC[21]) acerca de evidências digitais, só para se ter acesso a elas, é necessário desembolsar uma quantia que chega a quase R$ 4.000,00 (quatro mil reais)[22].

Superadas estas questões, ainda que consideremos a escolha como legalmente adequada por parte do STJ, questiona-se: a própria ABNT considera suas diretrizes como

[19] Eventual omissão legislativa que gere alguma inconstitucionalidade por violação de direitos, como poderia ocorrer na eventual ausência de normas de cadeia de custódia digital, é tema de competência do Supremo Tribunal Federal, nos termos do artigo art. 102, inciso I, alínea "a" da Constituição da República (Brasil, 1988), em procedimento complexo, aberto e plural, com manifestação da Advocacia-Geral da União e da Procuradoria-Geral da República, possibilidade de ingresso de agentes estatais e privados como *amicus curae* a fim de melhorar a discussão e ciência ao poder omisso para adoção de providências (art. 12-H da Lei n. 9.868/99)

[20] Além da ideia de que toda norma pressupõe publicação é importante também pensar nas dificuldades que pessoas economicamente menos favorecidas teriam para ter acesso às normas para se defenderem.

[21] International Organization for Standardization – Organização Internacional de Normatização – e International Electrotechnical Commission ou Comissão Internacional de Eletrotécnica.

[22] Os preços para não associados, na data de 01/06/2024, para aquisição das normas principais da ABNT sobre provas digitais são: a) ABNT-NBR-ISO /IEC 27037:2013 (Diretrizes para identificação, coleta, aquisição e preservação de evidência digital): R$ 364,20; b) ISO/IEC 27037: 2012 – em inglês (Diretrizes para identificação, coleta, aquisição e preservação de evidência digital – versão original ISO): R$ 1.494,00; c) ISO 21043-2:2018 – em inglês (Ciências forenses – part 2º reconhecimento, registro, coleta transporte e armazenamento de itens): R$ 816,00; d) ISO/IEC 27050-1:2019 – em inglês - (Tecnologia da informação – descoberta eletrônica – part 1 – visão geral e conceitos) R$ 1.161,00. Total das 4 obras: R$ 3835,00. Lembra-se, por fim, que mesmo os associados possuirão acesso restrito à norma da ABNT pelas suas regras atuais (45 minutos por ano).

válidas para organismos estatais? Indica ela, como fez o STJ, a adoção de algum procedimento específico ou softwares certificados?

A resposta é: não. Com a palavra, a própria ABNT, na principal diretriz que ela sobre o tema (2013):

> [...] Esta norma **não ordena o uso de ferramentas ou métodos particulares**. [...]. **Esta norma não trata de metodologias para procedimentos judiciais**, procedimentos disciplinares e outras ações relacionadas ao manuseio de potenciais evidências digitais que estão além do escopo de identificação, coleta, aquisição e preservação de potenciais evidências digitais. A aplicação desta norma requer conformidade com leis, regras e regulamentos nacionais. **É recomendável que ela não substitua exigências legais de qualquer jurisdição**. Em vez disso, ela pode servir de diretriz para qualquer DEFR ou DES em investigações envolvendo potenciais evidências digitais [...] – destacou-se.

Assim, enquanto o STJ entende que as normas da ABNT devem suprir eventual legislação inexistente, a principal norma da ABNT diz expressamente o contrário, que isso não é recomendável. Surge uma contradição na decisão do STJ: seguindo as diretrizes da ABNT como norma, o ordenamento jurídico brasileiro está desobedecendo essas diretrizes.

Outro aspecto relevante do trecho colacionado acima é observar que a ABNT diz expressamente que não recomenda o uso de ferramentas ou métodos específicos enquanto o STJ, por sua vez, dizendo estar se escorando nas normas da ABNT, dispõe expressamente que "*uma forma de se garantir a mesmidade dos elementos digitais é a utilização da técnica de algoritmo hash, a qual deve vir acompanhada da utilização de um software confiável, auditável e amplamente certificado(...)"* (Brasil, 2024).

Quando o STJ afirma em um julgamento envolvendo um aparelho telefônico que deve ser utilizada a "*técnica de algoritmo hash"* (Brasil, 2024) para garantir o princípio da mesmidade há um erro técnico crasso.

Sobre o princípio da mesmidade, explica Badaró (2022, pag. 518):

> A noção de "mesmidade" foi trazida para a doutrina brasileira [...] por Geraldo Prado, que sustenta que a "autenticidade da prova" deve ser auferida pela confrontação da sua obtenção aos "princípios da 'mesmidade' e da 'desconfiança'. A "mesmidade" é a garantia de que a prova valorada em juízo é a mesma colhida ou resultado direto da fonte de prova colhida no local dos fatos.

Em outras palavras, a noção de mesmidade estaria garantida quando existerem elementos que apontem que a prova valorada seria exatamente a mesma colhida no local dos fatos. É uma tradução para o universo processual penal da noção de autenticidade da prova digital[23].

A autenticidade da prova digital, assim, diria respeito à garantia da "a veracidade do emissor e do receptor da informação" (Vecchia, 2020, p. 29). Em outras palavras, a análise de autenticidade busca verificar se é possível garantir a origem de um dado, isto é, de onde ele veio, como ocorreria na informática, por exemplo, na conferência de assinaturas digitais de arquivos, confirmando a origem de um arquivo.

No contexto de dados oriundos dos aplicativos de mensageria, dizer que há autenticidade em um dado significa reconhecer que é possível assegurar a sua origem, isto é, de qual aparelho telefônico ou conta veio o dado.

Uma boa forma de garantir a autenticidade de um arquivo digital de mensageria, por exemplo, é manter a apreensão física de um aparelho celular cumprindo todas as etapas da cadeia de custódia de vestígios físicos e mantê-lo apreendido mesmo após sua extração, permitindo que o possuidor do conteúdo "apreendido digitalmente" no aparelho possa questionar algum conteúdo vindo da extração e conferir sua existência, se for o caso.

Quanto ao código hash, ele, em apertada síntese, se trata de uma sequência alfanumérica gerada após uma aplicação, por meio de softwares, de operações matemáticas e lógicas, gerando um código de alfanumérico tamanho fixo, que, em regra[24], será diferente para cada arquivo, sendo alterado a partir de qualquer mínima modificação (VECCHIA, 2020). Em outras palavras, é um código que se altera a partir de qualquer mínima alteração de um arquivo, mesmo que invisível a olho nu (como a inserção de um espaço em branco em um arquivo).

O código hash não necessariamente garante a autenticidade, sendo mais apto a verificar a integridade de uma prova digital clássica de memória não volátil[25], como um arquivo

[23] A autenticidade é uma das principais características das provas digitais, sendo outras a confiabilidade, a disponibilidade e a integridade (Vecchia, 2020).

[24] Há exceções denominadas colisão de hash, um tema que foge do escopo deste artigo. A probabilidade disso ocorrer é baixa e depende do algoritmo escolhido

[25] Há duas espécies de memória na informática, a volátil e a não volátil. A memória volátil é aquela que requer energia elétrica para manter os dados armazenados. Um exemplo é a denominada memória RAM. Já a memória não volátil é aquela que não depende de energia para armazenamento, se mantendo mesmo quando a energia é desligada (TechTerms, 2024). Um aparelho celular conjuga as duas memórias e ainda possui processos internos automáticos que geram alteração involuntária de alguns arquivos.

(uma planilha ou uma fotografia, *e.g.*) existente em um pen-drive. Mas ele sequer é suficientemente adequado para ser aplicado em todas as provas digitais.

Sendo mais claro, em relação ao espelhamento de aparelhos celulares ou outros dispositivos que possuam memória volátil[26] ou processos automatizados a técnica (escolhida pelo STJ) de análise de mesmidade por (repetição de) código hash não é possível.

Detalhando, é comprovado cientificamente ser impossível extrair, por duas vezes seguidas, o mesmo *código hash* de cópias (mesmo que sequenciais) de aparelhos de memória volátil, como um aparelho celular.

A ressalva sobre a inaplicabilidade do código hash nos casos em que envolva extração de memória volátil é feita pela própria ABNT (ABNT, 2013):

> Convém que um hábil e experiente DEFR seja capaz de realizar todos os processos descritos na documentação e de alcançar os mesmos resultados, sem orientação ou interpretação. **É recomendável que o DEFR esteja atento a possíveis circunstâncias em que não será possível repetir o teste, por exemplo, quando um disco rígido original foi copiado e voltou a ser utilizado ou quando um item envolve memória volátil**. Nestes casos, convém que o DEFR assegure que o processo de aquisição é confiável – destacou-se.

Neste sentido, detalha a doutrina técnica internacional sobre a irrepetibilidade do código hash em extrações de aparelhos celulares diante das características específicas destes aparelhos (Cuomo; D'Agostino; Ianulardo, 2022, em tradução livre):

> Graças aos testes laboratoriais, a existência de múltiplos arquivos frequentemente e continuamente sujeitos a mudanças **geradas pela presença de vários hashes encontrados nas extrações forenses conduzidas em momentos muito curtos (às vezes não ultrapassando 15 minutos) foi comprovada**. [...]. **A esse respeito, identificamos arquivos que têm diferentes códigos hash em duas aquisições físicas, e é precisamente por causa desses arquivos que essas operações não constituem atos perfeitamente repetíveis**. [...] Arquivos de vários tipos, como imagens e textos reproduzindo e-mails, criados ao mesmo tempo que foram extrapolados do arquivo compactado produzido pelo Ufed após a aquisição, razão pela qual, **embora exibindo o mesmo conteúdo, eram diferentes de tempos em tempos, incluindo arquivos de log, que contêm registros de eventos do sistema que ocorreram no dispositivo**. É bastante incomum que testes técnicos de natureza não repetível sejam realizados nesse último tipo de arquivos. Assim, é **verdade que os conteúdos do arquivo de log são diferentes dependendo do momento em que são analisados (portanto, a irrepetibilidade da inspeção)**,

[26] Os aparelhos celulares possuem, além da memória tradicional, a denominada memória volátil, captada integralmente pelo método do processo de extração por aquisição lógica (que captura muito mais que a cópia lógica tradicional, captando aspectos como a integralidade de sua memória RAM volátil e arquivos não alocados – ou arquivos deletados, por exemplo) e também processos automatizados.

Grosso modo, conforme explicam Cuomo, D'Agostino e Ianulardo (2022), há peculiaridades dos sistemas de aparelhos celulares, relativo a processos internos, que ocorrem independentemente de qualquer ação do usuário e que alteraram o código hash, o que se soma ao fato que as cópias mais avançadas exigem processos também impedem uma repetição exata de código hash[27], notadamente por conta de alguns registros internos automatizados (log's[28]) na memória volátil do celular, que faz com que duas extrações seguidas, com minutos de diferença, de um mesmo aparelho celular, mesmo mantendo exatamente o mesmo conteúdo, não tenham um hash igual.

Isso não significa que uma extração não é autêntica, não é íntegra ou tampouco que houve qualquer mínima alteração de conteúdo, mas apenas que a técnica recomendada pelo STJ não é aplicável para este caso, como também detalham outros autores como Dal Checco (2017)[29].

Assim, nota-se que o STJ neste julgado escolheu um método que nem sequer funciona no caso em que julgava, sendo um erro técnico crasso do referido tribunal.

3 CONSIDERAÇÕES FINAIS

Retomando o problema levantado no primeiro capítulo do trabalho, buscando responder a primeira parte dele, a saber, sobre os eventuais parâmetros do STJ acerca da admissibilidade de provas advindas de aplicativos de mensageria, conclui-se que o STJ, em decisões colegiadas, tem adotado o entendimento de que *print screen* advindo especificamente da ferramenta WhatsApp web não pode ser utilizado como prova no processo penal, por algumas características específicas da ferramenta.

[27] No brilhante trabalho (2022), os autores detalham que tanto nos aparelhos celulares com sistema Android quanto nos aparelhos celulares com o sistema iOS, os arquivos do sistema podem variar entre extrações devido a processos internos e temporários. São exemplos de questões técnicas: as limitações de acesso às partições, as necessidades de privilégio de root necessárias para se copiar a memória, as alterações de firmware, a criptografia, a necessidade da técnica de jailbreaking. Todos estes aspectos influenciam a extração do código hash, impedindo a repetição.

[28] Os logs são registros de eventos existentes em sistemas de informática. Eles registram dados como inicialização, desligamento, erros, acesso a banco de dados, tráficos ou tentativas de tráfego em redes, a depender da configuração do software ou aplicativo.

[29] Para melhor detalhamento do ponto, recomenda-se a leitura do artigo Ripetibilità e Irripetibilità Delle Acquisizioni Forensi (2017), referenciado ao final deste artigo.

No mais, como outro parâmetro, o STJ tem entendido que as provas advindas de aplicativos de mensageria precisam respeitar as normas da ABNT sobre a coleta de provas digitais, para garantir o princípio mesmidade, concluindo expressamente que a adoção do mecanismo de código *hash* seria o recomendável a ser adotado.

No mais, em resposta a outra parte do problema levantado pela pesquisa, a saber, se pressupostos e conclusões técnicas das decisões do STJ sobre o tema seriam escorreitas do ponto de vista legal e fático, conclui-se que não são, conforme detalhado no capítulo 2 do trabalho.

Em breve resumo, conforme relatado no item 2.1 deste trabalho, a decisão proferida no Recurso em Habeas Corpus n. 99.735/SC (Brasil, 2018) partiu do pressuposto equivocado de que as provas técnicas são mais fáceis de alterar do que as demais, o que não parece ser o caso em comparação com provas tradicionais. Ela ainda diverge do sistema da persuasão racional adotado no Brasil. No mais, ela adotou afirmações técnicas completamente equivocadas acercas das possibilidades da ferramenta WhatsApp web e da existência dos registros de atividades eventualmente ilícitas por parte de quem coleta as informações ali, bem como pareceu não entender como funciona a criptografia da ferramenta para reafirmar sua decisão, sendo incorreta do ponto de vista legal e fático.

Em situação semelhante, houve equívocos técnicos relevantes no que restou decidido no Agravo Regimental no Habeas Corpus n. 828.054/RN, explicados no item 2.2 deste trabalho. Dentre outros aspectos, a decisão, ao exigir a adoção de normas da ABNT na coleta de provas digitais, desconsiderou complemente questões fáticas como o fato das normas não serem disponibilizadas gratuitamente e o próprio teor das diretrizes da ABNT, que expressamente não recomendam seu uso como metodologia para procedimentos judiciais e que expressamente também diz não indicar seu uso em substituição a exigências legais e tampouco ordenam o uso de métodos específicos, como o STJ fez expressamente se escorando nas diretrizes da associação.

Em relação específica a outro ponto específico da decisão, a saber, do STJ recomendar o uso da técnica de extração de código hash para verificar o princípio da mesmidade em relação a provas obtidas de celular, o STJ fez exigência tecnicamente impossível e inaplicável, conforme comprovado por trabalhos científicos internacionais, ignorando o fenômeno da irrepetibilidade de hash em espelhamentos de aparelhos celulares.

Assim, este trabalho entende ser importante à comunidade jurídica, acadêmica e profissional, que se atentem ao teor das decisões do STJ sobre o tema, para não repetir os mesmos equívocos legais e fáticos.

Por fim, conclui-se ser importante uma melhor e maior difusão de conhecimento técnicos acerca de provas digitais, notadamente as advindas de aplicativos de mensageria, contribuindo com a melhora das discussões a fim de, por consequência, melhorar a qualidade técnica das decisões judiciais tomadas sobre o assunto.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT **NBR ISO/IEC 27003:2013**. Tecnologia da informação - técnicas de segurança - Diretrizes para implementação do sistema de gestão de segurança da informação. RIO DE JANEIRO, 2013.

BADARÓ, Gustavo Henrique. **Processo penal**. 10ªed. São Paulo: Thomson Reuters Brasil, 2022

BRASIL. Superior Tribunal de Justiça. **Acórdão que deu provimento a recurso ao habeas corpus n. 99.735/SC.** Relatora: Ministra Laurita Vaz. 27 de novembro de 2018. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201801533498&dt_publicacao=12/12/2018. Acesso em: 01 jun. 2024.

BRASIL. Superior Tribunal de Justiça. **Acórdão que deu provimento ao habeas corpus n. 653.515-RJ.** Relator: Ministro Rogério Shietti Cruz. 23 de novembro de 2021. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=141279576&tipo=5&nreg=202100831087&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20220201&formato=PDF&salvar=false. Acesso em: 01 jun. 2024

BRASIL. Superior Tribunal de Justiça. **Acórdão que deu provimento a Agravo em Recurso Especial n. 2.441.511.** Relatora: Ministra Daniela Texeira. 09 de fevereiro de 2024. Disponível em: https://processo.stj.jus.br/processo/dj/documento/mediado/?tipo_documento=documento&componente=MON&sequencial=227812959&num_registro=202303093964&data=20240214. Acesso em: 01 jun. 2024.

CUOMO, Raffaele; D'AGOSTINO, Davide; IANULARDO, Mario. Mobile **Forensics: Repeatable and Non-Repeatable Technical Assessments**. Sensors, v. 22, n. 18, p. 7096, 2022. Disponível em: https://doi.org/10.3390/s22187096. Acesso em: 01 jun. 2024.

DAL CHECCO, Paolo. **Ripetibilità e Irripetibilità Delle Acquisizioni Forensi**. Studio d'Informatica Forense. Disponível em: https://www.dalchecco.it/ripetibilita-irripetibilitaacquisizioni-forensi/. Acesso em: 01 jun. 2024.

FORTINET, FortGuard Labs. **Fortinet relata que a América Latina foi alvo de mais de 360 bilhões de tentativas de ataques cibernéticos em 2022.** Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2023/fortiguardlabs-reports-destructive-wiper-malware-increases-over-50-percent. Acesso em: 01 jun. 2024.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **17º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2023. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf. Acesso em: 01 jun. 2024.

FOUROZAN, Behrouz A e FEGAN, Sophia Chung. **Protocolo TCP/IP**. Tradução: João Eduardo Nóbrega Tortelo. 3ª. Ed. Porto Alegre: AMGH, 2010.

KEMP, Simon. **Digital 2023: Brasil**. Datareportal. Disponível em: https://datareportal.com/reports/digital-2023-brazil. Acesso em: 01 jun. 2024.

LIMA, Renato Brasileiro de. **Manual de processo penal**: volume único. 7. ed. Salvador: Ed. JusPodivm, 2019.

OLIVEIRA, Eugênio Pacelli de. **Curso de processo penal I**. 18. ed. São Paulo: Atlas, 2014.

TECHTERMS. **Volatile Memory Definition**. Disponível em: https://techterms.com/definition/volatile_memory. Acesso em: 01 jun. 2024.

VECCHIA, Evandro Dalla. **Perícia Digital. Da Investigação à Análise Forense**. 2ª edição. Campinas: SP - Millennium Editora Ltda, 2019.

WENDT, Emerson. **As expectativas cognitivas e normativas dos atores de investigação policial em face dos crimes cibernéticos**. 2023. Tese (Doutorado em Direito) - Universidade La Salle, Canoas, 2023.

WENDT, Emerson e JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos**. 3ª ed. Rio de Janeiro: Brasport, 2021.

WHATSAPP. **Sobre dispositivos conectados**. Online: 2024. Disponível em: https://faq.whatsapp.com/378279804439436/?helpref=tc_about&cms_platform=android. Acesso em: 01 jun. 2024.