A Polícia pode visualizar conversas do WhatsApp em celular apreendido?

Evandro Lincoln Pereira Dias Junior[1]

Piero Leandro Gamper Madalozzo[2]

Resumo

O presente artigo examina normas e garantias legais relacionadas à apreensão, interceptação e invasão de dispositivos eletrônicos, com foco nas implicações para privacidade, investigação policial e utilização de mensagens do WhatsApp como prova. Ou seja, a problemática geral é “A Polícia pode visualizar conversas do WhatsApp em celular apreendido?” O estudo foi realizado para analisar a complexidade jurídica e ética dessas práticas em um contexto digital em constante evolução. A pesquisa abrangeu a legislação brasileira, jurisprudência e tendências atuais, sendo conduzida por meio da revisão de textos legais, análise de casos e consideração de posicionamentos acadêmicos. Os resultados destacam a necessidade de cautela e legalidade na aplicação da lei, respeitando os direitos fundamentais e a privacidade. O estudo evidencia que a obtenção de provas, especialmente a partir do WhatsApp, requer autorização judicial e conformidade com normas éticas. Além disso, são apresentadas técnicas e metodologias da polícia na extração de dados de dispositivos eletrônicos em investigações criminais. Os resultados têm significados amplos, destacando a importância do equilíbrio entre a aplicação da lei e a proteção da privacidade em uma sociedade democrática. A análise de um estudo de caso específico ressalta como violações de direitos fundamentais podem resultar na nulidade de provas, reforçando a relevância do devido processo legal. Em última análise, os resultados apontam para a necessidade contínua de transparência e supervisão rigorosa para manter a confiança pública nas instituições de aplicação da lei.

Palavras-chave: Investigação Criminal; Limitação ao poder do Estado; inviolabilidade das conversas via aplicativos WhatsApp e outros aplicativos de conversa.

INTRODUÇÃO

A utilização de mensagens de aplicativos como o WhatsApp como meio de prova em investigações criminais levanta uma série de desafios jurídicos e éticos em um cenário digital em constante evolução, havendo o seguinte questionamento: A Polícia pode visualizar conversas de WhatsApp? Diante dessa complexidade, a presente pesquisa busca delimitar o tema, explorando normas e garantias legais relacionadas à apreensão, interceptação e invasão de dispositivos eletrônicos, com

[1] Graduando em Direito pela Faculdade do Litoral Paranaense – ISEPE Guaratuba.

[2] Advogado e Especialista em Direito Penal.

um enfoque específico na privacidade dos usuários e nas implicações para a investigação policial.

O tema delimita-se na interseção entre a aplicação da lei, a proteção da privacidade e o uso de mensagens do WhatsApp como prova em processos criminais. Em uma sociedade cada vez mais digital, compreender as normas e limitações legais nesse contexto é crucial para garantir a preservação dos direitos individuais e a eficácia das investigações. A relevância da pesquisa reside na necessidade de estabelecer um equilíbrio adequado entre a busca pela verdade, por meio de provas digitais, e a proteção da privacidade, mantendo a confiança na justiça.

A problemática central gira em torno dos desafios enfrentados pelas autoridades policiais ao acessar informações em dispositivos eletrônicos, especialmente no contexto das mensagens do WhatsApp. A questão ética de conciliar a aplicação da lei com a proteção da privacidade individual, aliada às constantes mudanças tecnológicas, destaca-se como um ponto crucial para análise.

O objetivo geral desta pesquisa é analisar a possibilidade jurídica e os limites do acesso de autoridades policiais às informações contidas em dispositivos eletrônicos apreendidos em investigações criminais, com foco nas mensagens de WhatsApp, considerando as garantias constitucionais de privacidade e inviolabilidade de dados pessoais.

No início da investigação, não estava claro como as constantes mudanças nas tecnologias e nas leis impactavam a capacidade da polícia de acessar informações em dispositivos eletrônicos. A complexidade ética e legal envolvendo a privacidade dos usuários e a obtenção de provas digitais representava uma lacuna no entendimento, motivando a pesquisa para preencher esse vazio de conhecimento.

A pesquisa adotará uma abordagem qualitativa, compreendendo uma revisão sistemática da legislação brasileira, análise de jurisprudências, estudo de casos específicos e revisão da literatura acadêmica.

A metodologia incluirá uma análise detalhada da Lei Geral de Proteção de Dados, bem como a consideração de tendências jurídicas e éticas emergentes. O público-alvo desta pesquisa abrange acadêmicos, profissionais do direito, autoridades policiais e demais interessados na interseção entre tecnologia, direito e ética.

Normas e Garantias Legais para Apreensão, Interceptação e Invasão de Dispositivos Eletrônicos: Um Enfoque nas Provas e Privacidade

A investigação criminal da Polícia possui elementos observacionais da infração penal, como os vestígios, indícios, rastros e evidências. A apreensão, interceptação e invasão de dispositivos eletrônicos fazem parte desse acervo investigatório, possuindo algumas normas a serem respeitadas, para que seja todo o processo seja realizado de maneira regular e com segurança, fazendo com que o cidadão possua garantias legais e que as provas produzidas, sejam feitas com veracidade e legitimidade, para que tenham valor probatório.

Sendo o WhatsApp, um aplicativo que possui ferramentas de fácil manipulação das conversas, no caso, a ferramenta excluir, que não deixa vestígios, seja no aplicativo de celular ou computador e jamais ser recuperada para efeitos de prova em processo penal, como também podendo ser inseridas novas mensagens, deixando assim, qualquer prova produzida por esse meio sendo considerada uma prova incerta, gerando discussões sobre o valor probatório do material apresentado.

Por conta dessas discussões jurídicas, será abordado, na forma que se vê pela frente, algumas normas que dão algum norte a este assunto.

A Constituição Federal (BRASIL, 1988) não tem descrição detalhada relacionada à aplicativos de mensagens de texto em celulares smartphones pelo fato de ser do ano de 1988, em que não se existia esse tipo de dispositivo com tal capacidade, porém, é estabelecido em seu inciso XII, do Art. 5º, o direito à inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, ressalvadas as hipóteses previstas em lei e mediante autorização judicial. Conforme destaca Sartori (2018), o direito à privacidade é um direito fundamental assegurado pela Constituição Federal, e a interceptação de comunicações telefônicas só é permitida em casos excepcionais, devidamente fundamentados.

Não muito tempo após a promulgação da Carta Magna, a Lei Nº 9.296 (BRASIL, 1996), conhecida como Lei de Interceptações Telefônicas, trata sobre as interceptações de comunicações telefônicas de qualquer natureza, para a investigação de crimes. Embora mais voltada para a interceptação telefônica, suas regras podem se aplicar a dispositivos eletrônicos que permitam a comunicação.

Já no Código de Processo Penal (BRASIL, 1941), regula procedimentos criminais e dispõe sobre as medidas cautelares, inclusive a busca e apreensão. Os dispositivos eletrônicos podem ser apreendidos se houver indícios de que eles contenham provas de um crime. De acordo com Araújo (2019), o acesso às conversas de WhatsApp em celulares apreendidos pela polícia pode ser justificado com base no artigo 240 do Código de Processo Penal - CPP, que prevê a possibilidade de interceptação telefônica em casos de investigações criminais. Nesse sentido, a autorização para a quebra do sigilo das comunicações por meio do aplicativo dependerá da existência de indícios concretos da prática de crimes e da autorização judicial.

Avanços e Implicações para Investigação e Apreensão de Dispositivos Eletrônicos

Em 2012, surge a Lei Nº 12.735 (BRASIL, 2012), Lei Carolina Dieckmann, essa lei trata de crimes cibernéticos, como a invasão de dispositivos eletrônicos para obtenção, adulteração ou destruição de dados. Embora não trate diretamente da apreensão, ela aborda aspectos relacionados à investigação de crimes cibernéticos. No mesmo contexto, surge a Lei Nº 12.737 (BRASIL, 2012), que acresce no Código Penal (BRASIL, 1940), o Art. 154-A, que discorre sobre o mesmo sentido que Lei Carolina Dieckmann, também transcorrendo sobre invasão de dispositivos eletrônicos para obtenção, adulteração ou destruição de dados.

A Lei de Combate ao Crime Organizado, Lei Nº 12.850 (BRASIL, 2013), em seu artigo 8º, trata sobre ação controlada em retardar a intervenção policial ou administração que seja relacionada à ação praticada por organização criminosa, para que haja uma formação de provas de modo eficaz e que a medida legal seja acompanhada e observada a todo momento. Note-se que, apesar da obtenção das provas, no parágrafo 3º, o acesso aos autos será restrito ao Juiz, ao Ministério Público e ao Delegado de Polícia até o fim da diligência. No mesmo Diploma, o Artigo 10-A, regula sobre a infiltração de agentes policiais de maneira virtual, para fins de investigações de crimes previstos nesta Lei.

Aprofundando no tema de cyber ataques, em 2014, surgiu o Marco Civil da Internet, Lei Nº 12.965 (BRASIL, 2014), estabelecendo direitos e deveres no uso da internet no Brasil. Em seu artigo 15, prevê a possibilidade de requisição judicial para

acesso a registros de conexão e de acesso a aplicações de internet. Esse dispositivo legal pode fundamentar o acesso às mensagens de WhatsApp por parte das autoridades policiais mediante autorização judicial.

Uma lei a ser mencionada, mesmo não sendo relacionado diretamente ao âmbito criminal, mas pode influenciar nos procedimentos para apreensão de dispositivos eletrônicos quando envolvem agentes públicos é a Lei Nº 13.460 (BRASIL, 2017), que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos. Essa Lei, apesar de curta, é mais utilizada em processos Administrativos, mas em raros casos em que envolvem um fato criminal praticado por um agente público, também há de ser levada em consideração.

Lei Geral de Proteção de Dados (LGPD) para Investigação Policial

Não obstante a esta época, na data de 14 de agosto de 2018, foi sancionada a Lei Nº 13.709 (BRASIL, 2018), conhecida como a Lei Geral de Proteção de Dados Pessoais (LGPD), que regula como os dados pessoais devem ser tratados de forma adequada garantindo a privacidade e a proteção dos indivíduos. Isso inclui as comunicações realizadas através de aplicativos de mensagens como o WhatsApp. As empresas que processam esses dados, como provedores de serviços de telecomunicações e aplicativos de mensagens, precisam cumprir as disposições da LGPD, como obter o consentimento adequado dos usuários, informar sobre a finalidade do processamento e garantir a segurança dos dados.

Quanto ao acesso a essas conversas pelas autoridades, como a polícia, a LGPD também aborda esse assunto. O tratamento de dados pessoais sensíveis, previsto no artigo 11 em seus incisos e parágrafos desse diploma, como informações sobre a vida privada das pessoas, é restrito e deve ser realizado em conformidade com a lei. No entanto, a LGPD também prevê situações em que o tratamento de dados pode ser realizado sem consentimento, como para o cumprimento de uma obrigação legal ou regulatória por parte do controlador dos dados.

Nesse contexto, a polícia e outras autoridades podem obter acesso a dados pessoais, incluindo conversas de aplicativos de mensagens, se houver uma base legal para tal acesso, como no caso de investigações criminais. Geralmente, é

necessária uma ordem judicial para autorizar o acesso a esses dados, garantindo assim que a privacidade e os direitos dos indivíduos sejam protegidos.

Tendências Jurídicas na Utilização de Mensagens do WhatsApp como Prova: Análise da Jurisprudência Brasileira

As decisões judiciais e a jurisprudência também podem embasar o acesso de autoridades policiais às informações contidas em dispositivos eletrônicos. Vital (2019) diz que:

> Conforme a jurisprudência brasileira, são ilegais as provas decorrentes do acesso a mensagens do WhatsApp sem autorização judicial. No entanto, nada impede que, reconhecida essa ilegalidade, o juiz decida de modo fundamentado acerca da perícia, com acesso às informações, que poderão embasar ação penal.

Casos anteriores, envolvendo a obtenção de mensagens de WhatsApp como meio de prova, podem servir de referência para embasar novas decisões judiciais. É importante observar que as decisões e a jurisprudência podem variar de acordo com a interpretação dos magistrados e os princípios e direitos fundamentais envolvidos. Valente (2020, p. 23) afirma que:

> A prova resultado, advinda tão-só de um processo/procedimento de conservação da sua identidade e autenticidade, não pode resumir-se a uma condição de meio retórico, mas assumir-se como entendimento final fundamentado num Direito e num proceder judiciário e policial íntegro, límpido, leal e democrático.

Em alguns recursos e remédios constitucionais, o assunto também acaba sendo discutido, como por exemplo no *Habeas Corpus* nº 617.232/SP (STJ, 2020), em que foi Relator Min. Nefi Cordeiro, na qual foi tratado da ilicitude da obtenção de dados, bem como das conversas de WhatsApp, obtidas pela Polícia em Celular Apreendido por ocasião da Prisão em Flagrante, sem prévia autorização Judicial. A decisão final, foi que o *Habeas Corpus* foi concedido para que fosse declarado nulas todas as provas obtidas, sendo uma delas as conversas obtidas por conta do acesso ao celular do flagranteado sem sua autorização, sendo realizado de modo ilícito.

O TJPR (2019) também compartilha desse entendimento, pois na Apelação Criminal Nº 0000020-67.2019.8.16.0013, a parte apelante sustenta a ilegalidade das conversas via aplicativo “WhatsApp”, porém, no acordão foi reconhecida legalidade

pois houve autorização judicial para tal feito. Ou seja, o entendimento é que sem autorização judicial, as provas das conversas de WhatsApp são passíveis de anulação, mas, a partir do momento que há uma autorização judicial emitida pelo Magistrado, toda prova produzida, das conversas do aplicativo WhatsApp, são legalmente consideradas.

Em outro Recurso em *Habeas Corpus* Nº 99.735/SC (STJ, 2018), que teve como Relatora a Ministra Laurita Vaz, que houve uma tentativa de acesso de maneira Indireta e inusitado ao WhatsApp da parte passiva, pois não houve acesso ao aplicativo por meio do dispositivo eletrônico apreendido, mas sim, um espelhamento do WhatsApp via *QR Code*, no computador, atividade deferida por decisão judicial, tendo sida posteriormente anulada por conta do provimento do recurso impetrado, além da nulidade da prova e dos atos que sobrevieram por conta da decisão.

Pode-se ver que foi uma prova produzida em que o magistrado acabou não verificando se houve a violação a princípios, axiomas, normas ou regras que restariam por viciar a prova obtida.

Mesmo que, fosse alegado que o espelhamento de WhatsApp no computador fosse equiparado a uma interceptação telefônica, no Informativo Nº 640 do Superior Tribunal de Justiça, da Sexta Turma, de mesmo recurso, é retratado que, o espelhamento de WhatsApp pode ser prejudicial para a produção de provas, pelo fato de, haver a possibilidade de exclusão de mensagens e o envio, sendo de fácil manipulação e pelo fato de que o aplicativo utiliza a criptografia *end-to-end,* isto é, as mensagens ficam armazenadas apenas nos dispositivos do remetente e do destinatário, não havendo quaisquer armazenamento dessas mensagens em nenhum servidor.

Pois na interceptação telefônica, que tem efeito *ex nunc*, é realizada apenas depois de uma autorização judicial. Outro exemplo, é o *e-mail*, que tem efeito *ex tunc* (retroativo). Já o WhatsApp, pelos motivos já mencionados, é considerado em termos técnico-jurídicos, como um tipo híbrido de obtenção de prova consistente a um só tempo sendo não possuidor de uma previsão legal, é impossível utilizar de analogia para retratar como uma interceptação telefônica.

O ministro relator Nefi Cordeiro, da 6ª turma do STJ, também partilha de mesmo entendimento, pois, no RHC 133.430, relata que as mensagens obtidas por meio de print screen da tela do WhatsApp Web (espelhamento), devem ser

consideradas Provas ilícitas e portanto, desentranhadas dos autos, pelo fato de o aplicativo ter manipulação das conversas sem gerar vestígios que não possuam maneira de recuperar tais mensagens.

A Importância da Cautela e da Legalidade

Diante dessas questões, é fundamental que o acesso às conversas do WhatsApp em celulares apreendidos pela polícia seja realizado com cautela e observando os preceitos legais e constitucionais. Como ressalta Silva (2019):

> A quebra do sigilo de comunicações telefônicas é uma medida excepcional, que deve ser aplicada somente nos casos em que houver indícios concretos da prática de crimes e com autorização judicial. É importante que sejam resguardados os direitos fundamentais dos cidadãos, como a privacidade, a intimidade e o sigilo das comunicações.

É importante destacar que o acesso às informações em dispositivos eletrônicos, como as mensagens de WhatsApp, deve ocorrer dentro dos limites legais estabelecidos, respeitando os direitos fundamentais, como o direito à privacidade e à inviolabilidade das comunicações. Assim, o acesso geralmente deve ser embasado em decisão judicial específica, garantindo a proporcionalidade e a legalidade da medida. Segundo Martins (2017, p. 235) “O acesso às mensagens do WhatsApp por autoridades policiais pode ser embasado pela obtenção de mandado judicial, que exige a apresentação de evidências convincentes de que as informações são relevantes para uma investigação em curso”.

O fato de no Brasil a investigação criminal ser presidida por uma autoridade com formação jurídica, sendo a polícia judiciária, sendo dirigida por um Delegado de Polícia que tem suas requisições lastreadas por lei e o pelos Promotores representantes do Ministério Público, viabilizando assim, uma instrução probatória consentânea com regras legais, impedindo que uma prova seja produzida de maneira ilegal e prejudique o correto exercício do *juis puniendi* estatal, colocando em risco a própria justiça.

Técnicas e Metodologias da Polícia Brasileira na Extração de Dados de Dispositivos Eletrônicos em Investigações Criminais

Cada vez que existe um novo modelo tecnológico criminosa para práticas de crimes, existe também uma reinvenção por parte das equipes policiais para combaterem tais práticas. Poubel (2015) diz que:

> Para lidar com essa nova realidade criminosa que dificulta bastante rastrear seus movimentos, identificar seus integrantes e obter provas, a tecnologia se apresenta como um dos instrumentos necessários e facilitadores à atuação investigativa policial. Quando se fala em "inteligência", a ideia deve associar a tecnologia à expertise policial.

Porém, nessas reinvenções, o acesso de autoridades policiais brasileiras às informações contidas em dispositivos eletrônicos, incluindo as mensagens de WhatsApp, através das técnicas, metodologias, softwares e equipamentos citados, deve ser feito de forma que seja embasado em fundamentos jurídicos específicos já citados.

A polícia brasileira utiliza diversas técnicas e metodologias para a extração de dados de dispositivos eletrônicos em investigações criminais e alguns deles serão discorridos em frente.

Temos a aquisição física que consiste na cópia integral dos dados armazenados em dispositivos eletrônicos, incluindo sistema operacional, aplicativos e arquivos. Essa abordagem pode ser feita por meio de kits forenses, que possibilitam a extração direta dos dados do dispositivo.

Já na aquisição lógica, são extraídas apenas as informações relevantes para a investigação, como mensagens de texto, registros de chamadas, contatos e arquivos específicos. Essa extração pode ser realizada por meio de softwares especializados que permitem acessar e extrair dados de backups, ou por meio de acesso direto aos sistemas operacionais dos dispositivos.

Em análise de arquivos e metadados, além da extração dos dados, a polícia pode realizar a análise de arquivos e metadados presentes nos dispositivos. Isso inclui informações como data, horário, localização geográfica e outros dados relacionados aos arquivos e atividades realizadas no dispositivo.

Existe também a recuperação de dados deletados, na qual, em algumas situações, é possível recuperar dados que foram excluídos pelos usuários. Essa

técnica envolve a utilização de ferramentas e métodos especializados de recuperação forense para identificar e restaurar os dados removidos.

Celulares Danificados também não fogem da perícia, pois de acordo com Monteiro (2021), assessor de comunicação da Perícia Forense do Estado do Ceará - PEFOCE, explica é uma metodologia nova que está sendo aplicada e muito utilizada nos estados do Ceará, Paraná e Rio Grande do Norte, em que consiste na desmontagem do aparelho celular e acessar diretamente aos dados através da placa do celular, utilizando um método minucioso que exige microssolda e microscópio na análise.

Nas palavras do perito criminal Cristiano Moreira, que faz parte do Núcleo de Perícias Tecnológicas e Apoio Técnico (NPTAT), da Coordenadoria de Perícia Criminal (Copec) da PEFOCE, explica que há o risco de perda de dados, porém, o celular já está danificado e caso se consiga extrair a informação, o benefício da técnica supera o risco.

Além destas técnicas e metodologias citadas, alguns equipamentos e softwares também são utilizados no trabalho de extração de dados do dispositivo. Um exemplo é o Cellebrite. É uma das empresas mais conhecidas no campo da extração forense de dados de dispositivos móveis. Seus equipamentos e softwares, como o UFED (Universal Forensic Extraction Device), têm sido amplamente utilizados pela polícia brasileira.

Existe também o Oxygen Forensic Suite, sendo um software completo de análise forense digital que permite a extração e a análise de dados de dispositivos móveis e computadores. XRY, uma ferramenta utilizada para a extração e análise forense de dados de dispositivos móveis, incluindo celulares e tablets.

Por último, existe a ferramenta FTK Imager que é uma ferramenta gratuita que oferece uma plataforma básica para investigações de evidências digitais, que auxilia na busca de artefatos excluídos nos dispositivos e ainda preserva uma evidência digital para analisá-la posteriormente. Apesar de não ter um mecanismo de pesquisa e automação de busca, ela é muito importante para investigações, pois arquivos excluídos podem mostrar o que aconteceu dentro de um contexto de um caso em que a busca de evidências para solucionar crimes para a atribuição de responsabilidades às pessoas envolvidas podem o ser solicitado por juiz ou um tribunal.

Ética na aplicação da Lei, Princípios Fundamentais e o Direito a privacidade

Quando se trata da polícia visualizar conversas do WhatsApp em um celular apreendido, é importante entender que estarão lidando com uma situação complexa que envolve diversos aspectos éticos. A era digital trouxe consigo desafios e dilemas éticos, pois a necessidade de combater o crime muitas vezes entra em conflito com a proteção da privacidade individual

Por um lado, a polícia, como órgão encarregado de manter a ordem e a segurança pública, pode se beneficiar ao acessar conversas do WhatsApp em um celular apreendido. Isso pode ser crucial na resolução de crimes, na prevenção de atividades ilícitas e no combate ao terrorismo. No entanto, a ética entra em cena quando se questiona a invasão da privacidade dos cidadãos.

E quando se fala de dilemas éticos, não se pode deixar de falar sobre os Princípios Fundamentais da Constituição Federal de 1988. O Artigo 5º da Constituição Federal de 1988, aborda alguns princípios em seus incisos que encaixam de maneiras diferentes, mas ainda assim, fundamentais para a garantia de direito de todos os cidadãos brasileiros.

No inciso X, por exemplo, discorre sobre o Princípio da Intimidade e Privacidade, assegurando a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas. Nesse contexto, a interceptação de comunicações, como as conversas no WhatsApp, sem autorização judicial, pode configurar violação desse princípio.

Já no Inciso XII, Princípio da Inviolabilidade do Sigilo de Comunicações, assegura a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas. O WhatsApp, como meio de comunicação, está incluído nessa proteção.

No Inciso II, aborda sobre o Princípio da Legalidade, que estabelece que "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei". Portanto, a obtenção de informações privadas, como as conversas no WhatsApp, deve ocorrer mediante autorização legal específica, geralmente por meio de mandado judicial.

Os incisos LIV e LV, ainda do Artigo 5º da Constituição Federal de 1988, retrata sobre a Garantia do Devido Processo Legal e da Ampla Defesa. Isso implica

que a obtenção e utilização de provas devem respeitar as garantias individuais, e a parte envolvida deve ter a oportunidade de se defender de maneira adequada.

O Princípio da Proporcionalidade (Princípio implícito, mas fundamental) exige que as medidas adotadas pelo Estado sejam proporcionais à gravidade da situação e necessárias para atingir os objetivos pretendidos. Assim, a invasão da privacidade por meio da visualização de conversas no WhatsApp deve ser proporcional à gravidade da investigação. Tal Princípio também tem efeito regulador nos demais Princípios Constitucionais, com o objetivo de evitar dar muita importância a um princípio específico, em detrimento de outro igualmente importante.

Paulo Vaz (2002), afirma que “Diante da colisão de princípios, é preciso verificar qual dos princípios possui maior peso diante das circunstâncias concretas.” Ele ainda afirma que a proporcionalidade “irá definir os critérios de delimitação da relação meio-fim, assegurando a restrição na exata medida do necessário e evitando excessos. Vai salvar o núcleo essencial do direito tutelado pelo princípio relativizado”

A polícia pode visualizar conversas do WhatsApp em um celular apreendido, mas somente quando isso for feito de maneira ética, legal e com respeito aos direitos e princípios individuais. A transparência e a supervisão rigorosa são essenciais para garantir que qualquer invasão da privacidade seja justificada e limitada. Encontrar esse equilíbrio é fundamental para manter a confiança na justiça e no respeito pelos direitos humanos em uma sociedade democrática.

Respeitar os direitos individuais é basal em uma sociedade democrática. A privacidade é um direito fundamental, e qualquer invasão injustificada pode minar a confiança na aplicação da lei e nas instituições democráticas. Portanto, é vital que o acesso a essas conversas seja realizado com base em mandados judiciais, que estabelecem limites e garantem supervisão. Além disso, a divulgação e o armazenamento responsável das informações coletadas são essenciais para garantir que não haja abusos.

Sobre a polícia visualizar conversas do WhatsApp em um celular apreendido é um dilema ético que exige um equilíbrio sensato entre a necessidade de aplicar a lei e a proteção da privacidade. A transparência, o respeito pelas leis e a supervisão rigorosa são elementos-chave para garantir que a ética seja mantida nesse processo. Encontrar esse equilíbrio é essencial para preservar a justiça e a confiança na aplicação da lei em uma sociedade democrática.

Transparência e Supervisão

A transparência e a supervisão são fundamentais quando se discute a capacidade da polícia de visualizar conversas do WhatsApp em um celular apreendido. No mundo digital de hoje, é essencial que haja mecanismos claros para garantir que a aplicação da lei seja conduzida de maneira justa e ética.

O WhatsApp é uma plataforma de comunicação amplamente utilizada para trocar mensagens pessoais, e o conteúdo dessas conversas frequentemente é considerado privado. Portanto, a transparência é necessária para que o público compreenda as circunstâncias em que a polícia pode acessar essas conversas. Isso geralmente envolve a obtenção de mandados judiciais, que estabelecem as condições e limites para o acesso.

Além da transparência, a supervisão desempenha um papel crítico na garantia de que a aplicação da lei seja conduzida de maneira apropriada. A supervisão poderia ser realizada por órgãos independentes ou autoridades judiciais, e garantir que a polícia siga as leis e regulamentos e evite abusos. Isso é fundamental para manter a confiança do público nas instituições de aplicação da lei.

Atualmente, essa transparência e supervisão é feita pela própria empresa Meta, dona do WhatsApp, que a cada quatro trimestres, lança relatórios sobre atualizações de suas redes sociais, sendo além do WhatsApp, as plataformas Instagram e Facebook, atualizando dados de novas políticas e situações que estão ligadas ao mundo, como a guerra Rússia-Ucrânia e protesto do Irã, combatendo operações de influência por parte da Rússia relacionada a invasão na Ucrânia e protegendo o Direito Individual de cada um poder conectar e compartilhar informações durante esse período de crise.

Estudo de caso

Neste caso do processo 0000440-36.2022.8.16.0088/TJPR, a análise envolve a defesa do réu, que alegou a nulidade das provas obtidas em uma fase inquisitorial do processo criminal. A principal argumentação da defesa é baseada na invasão de domicílio e na apreensão do celular do réu sem autorização legal, o que teria gerado a nulidade das provas derivadas dessas ações.

A defesa também alegou a nulidade do interrogatório em sede policial com base em uma série de argumentos, como desbloqueio do celular da denunciada sem autorização, pressão na delegacia de polícia, falta de presença de um defensor, averiguação prévia das informações no celular apreendido, invasão da residência do réu e a falta de informação sobre o direito a um advogado. A defesa argumentou que esses atos eram ilegais e desrespeitavam a Constituição Federal, além de afirmar que as provas precisavam ser desentranhadas dos autos.

O juiz decidiu que as provas eram nulas com base no artigo 157, §1º, do Código de Processo Penal (CPP). A decisão do juiz implicou na declaração de nulidade das provas decorrentes da prisão ilegal, que incluíam o auto de busca e apreensão, a constatação de mensagens de celular, fotos de uma arma, fotos da tela e áudios do aplicativo WhatsApp e o interrogatório. O juiz fundamentou sua decisão na ilegalidade da prisão e na violação dos direitos do réu durante o processo, o que justificou a exclusão das provas mencionadas.

Essa análise de caso destaca a importância dos direitos fundamentais e da legalidade no processo penal. O juiz considerou que as ações da polícia, desde a invasão de domicílio até a coleta de provas, violaram os direitos do réu e, portanto, as provas derivadas dessas ações foram declaradas nulas. Isso ressalta a relevância do devido processo legal e da proteção dos direitos dos acusados, mesmo em casos de investigação criminal.

CONSIDERAÇÕES FINAIS

No desfecho desta pesquisa, pode-se afirmar que os objetivos delineados foram alcançados, proporcionando uma compreensão mais aprofundada das complexidades jurídicas e éticas associadas à utilização de mensagens do WhatsApp como meio de prova em investigações criminais. Ao longo deste estudo, investigou-se a legislação brasileira pertinente, analisou-se jurisprudências relevantes e examinaram-se tendências jurídicas e éticas emergentes.

Refletindo sobre o que se sabia no início da investigação, a pesquisa foi capaz de preencher lacunas significativas no entendimento, especialmente em relação às implicações da Lei Geral de Proteção de Dados (LGPD) nas investigações policiais e na proteção da privacidade dos usuários. As constantes

mudanças tecnológicas e legais apresentaram desafios consideráveis, mas a análise meticulosa permitiu traçar um panorama mais claro.

Os resultados obtidos destacam a importância de encontrar um equilíbrio delicado entre a busca pela verdade por meio de provas digitais e a proteção dos direitos individuais. A compreensão aprimorada das técnicas e metodologias empregadas pelas autoridades policiais na extração de dados de dispositivos eletrônicos fornece insights valiosos para profissionais do direito e demais interessados.

Ao escrever sobre os resultados do estudo, é evidente que a pesquisa contribui não apenas para o conhecimento acadêmico, mas também para a prática jurídica e para o desenvolvimento de políticas públicas. O entendimento mais profundo das questões éticas e legais envolvendo o uso de mensagens do WhatsApp como prova em processos criminais pode orientar futuras decisões judiciais e aprimorar a legislação vigente.

Em suma, esta pesquisa proporcionou uma visão abrangente das questões pertinentes, oferecendo uma base sólida para discussões futuras e aprimoramentos nas abordagens legais e éticas relacionadas ao uso de mensagens de aplicativos como meio de prova em investigações criminais. O conhecimento adquirido durante esta investigação serve como um legado, enriquecendo o campo jurídico e estimulando novas reflexões sobre a interseção entre tecnologia, privacidade e justiça.

REFERÊNCIAS BIBLIOGRÁFICAS

Academia de Forense Digital. **“Ferramentas para Extração de Dados em Android”**. Disponível em: https://academiadeforensedigital.com.br/ferramentas-para-extracao-de-dados-em-android/. Acesso em: 19 de outubro 2023.

ARCHEGAS, João Victor et al. **Proteção de Dados e Transparência em Moderação de Conteúdo**. Disponível em: https://itsrio.org/wp-content/uploads/2021/07/Protecao-de-Dados-e-Transparencia-em-Moderacao-de-Conteudo.pdf. Acesso em: 18 de outubro de 2023.

AZAD, Usama. **Oxygen Forensic Suite in-depth tutorial**. LinuxHint. Publicado em 2020. Disponível em: https://linuxhint.com/oxygen_forensics_suite_guideline/. Acesso em: 13 setembro 2023.

BRASIL. **Código de Processo Penal**. Rio de Janeiro, RJ, 1942. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 22 agosto 2023.

BRASIL. **Código Penal.** Rio de Janeiro, RJ, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 22 agosto 2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 agosto 2023.

BRASIL. **Lei Nº 9.296, de 24 de julho de 1996.** Brasília, DF, 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 22 agosto 2023.

BRASIL. **Lei Nº 12.735, de 30 de novembro de 2012.** Brasília, DF, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 22 agosto 2023.

BRASIL. **Lei Nº 12.737, de 30 de novembro de 2012.** Brasília, DF, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 22 agosto 2023.

BRASIL. **Lei Nº 12.850, de 2 de agosto de 2013.** Brasília, DF, 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso: 24 de agosto 2023

BRASIL. **Lei Nº 12.965, de 23 de abril de 2014.** Brasília, DF, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 22 agosto 2023.

BRASIL. **Lei Nº 13.460, de 26 de junho de 2017.** Brasília, DF, 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13460.htm. Acesso em: 23 agosto 2023.

BRASIL. **Lei Nº 13.706, de 14 agosto de 2018.** Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 agosto 2023

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. **Habeas Corpus Nº 617.232/SP.** Relator: MINISTRO NEFI CORDEIRO. Julgado em 23/02/2021. Disponível em: https://jurisprudencia.s3.amazonaws.com/STJ/attachments/STJ_HC_617232_95f55.pdf?AWSAccessKeyId=AKIARMMD5JEAO67SMCVA&Expires=1693073157&Signature=FTjtGFnxKDsQLAWzmSXax%2FuGRrs%3D. Acesso em: 23 agosto 2023

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. **RECURSO EM HABEAS CORPUS No 99.735 -SC (2018/0153349-8).** Relatora: MIN. MINISTRA LAURITA VAZ DJ:12/12/2018. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/componente=ATC&s

equencial=88643916&num_registro=201801533498&data=20181212&tipo=5&formato=PDF. Acesso em: 25 agosto 2023.

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. **INFORMATIVO DE JURISPRUDÊNCIA NÚMERO 640**. P. 16-17. Disponível em: https://www.stj.jus.br/publicacaoinstitucional/index.php/informjurisdata/article/view/3887/4113. Acesso em: 28 outubro 2023

BRASIL. TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. **Acordão Nº 0000020-67.2019.8.16.0013.** Disponível em: https://portal.tjpr.jus.br/jurisprudencia/j/4100000017709691/Acórdão-0000020-67.2019.8.16.0013. Acesso em: 28 agosto 2023

BRASIL. TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. **Processo Nº 0000440-36.2022.8.16.0088.** Disponível em: https://consulta.tjpr.jus.br/projudi_consulta/. Acesso em: 20 outubro 2023

FCQ ADVOGADOS. STJ: **É Ilicíta Prova Obtida por Meio de Prints do WhatsApp Web.** Disponível em: https://www.jusbrasil.com.br/noticias/stj-e-ilicita-prova-obtida-por-meio-de-prints-do-whatsapp-web/1233927943. Acesso em: 28 de outubro de 2023.

FERNANDEZ JUNIOR, Enio Duarte. **Brevíssimo Aporte sobre o Direito Fundamental à Privacidade e à Intimidade na Perspectiva do Direito Brasileiro sobre a Proteção de Dados Pessoais.** Disponível em: https://ambitojuridico.com.br/cadernos/direito-civil/brevissimo-aporte-sobre-o-direito-fundamental-a-privacidade-e-a-intimidade-na-perspectiva-do-direito-brasileiro-sobre-a-protecao-de-dados-pessoais/. Acesso em: 17 de outubro de 2023.

GARNIER, Cintia Miele; PADILHA, Tamyris Michele. **Ética, Privacidade e Novas Tecnologias: O Impacto da Lei de Proteção de Dados na Sociedade.** Disponível em: https://www.migalhas.com.br/depeso/311142/etica--privacidade-e-novas-tecnologias--o-impacto-da-lei-de-protecao-de-dados-na-sociedade/. Acesso em: 17 de outubro de 2023.

GUGLIELMO, Camila. **Privacidade e Ética no Mundo Digital**. Disponível em: https://www.aasp.org.br/noticias/privacidade-e-etica-no-mundo-digital/. Acesso em: 18 de outubro de 2023.

LAU, Marcelo; JASPER, Nichols. **FTK Imager: Encontrando arquivos excluídos. Disponível** em: <https://www.devmedia.com.br/ftk-imager-encontrando-arquivos-excluidos/29614 >. Acesso em 19 outubro 2023.

LOPES, Petter. **Mobile Forense: Um Olhar Técnico Sobre Extração de Telefone.** Disponível em: https://periciacomputacional.com/mobile-forense-um-olhar-tecnico-sobre-extracao-de-telefone/. Acesso em: 19 outubro 2023.

MACHADO DE OLIVEIRA, Vinícius. **Hardware Forense**. Academia de Forense Digital, [s.d.]. Disponível em: https://academiadeforensedigital.com.br/hardware-forense/. Acesso em: 16 setembro 2023.

MARTINS, Luiz Gustavo. **O acesso às mensagens do WhatsApp por autoridades policiais: análise à luz dos direitos fundamentais.** Revista Jus Navigandi, Teresina, ano 22, n. 4984, 25 set. 2017. Disponível em: https://jus.com.br/artigos/60792. Acesso em: 25 agosto 2023

MONTEIRO, Francisco. **Peritos em Informática Forense Iniciam Nova Técnica para Extração de Dados em Celulares Quebrados.** Disponível em: https://www.pefoce.ce.gov.br/2021/09/02/peritos-em-informatica-forense-iniciam-nova-tecnica-para-extracao-de-dados-em-celulares-quebrados/. Acesso em: 20 de outubro de 2023.

NÚNCIO, Willian Freitas. "**Cellebrite Reader: Como funciona a ferramenta de análise forense gratuita da Cellebrite**". Academia de Forense Digital, [s.d.]. Disponível em: https://academiadeforensedigital.com.br/cellebrite-reader-ferramenta-gratuita-de-forense-digital/. Acesso em: 16 setembro 2023.

ROSEN, Guy. **Relatórios de Integridade e Transparência - Quarto Trimestre de 2022.** Disponível em: https://about.fb.com/br/news/2023/02/relatorios-de-integridade-e-transparencia-quarto-trimestre-de-2022/. Acesso em: 19 de outubro de 2023.

REIS, Fábio Mendonça dos. "**Forense Computacional: Técnicas para Preservação de Evidências em Coleta e Análise de Artefatos**." Brasil Escola - Monografias, [s.d.]. Disponível em: https://monografias.brasilescola.uol.com.br/computacao/forense-computacional-tecnicas-para-preservacao-evidencias-coleta-analise-artefatos.htm. Acesso em: 13 setembro 2023

SANNINI NETO, F. **Investigação criminal e os dados obtidos de aparelhos de celular apreendidos**. Jusbrasil, 2015. Disponível em: https://www.jusbrasil.com.br/artigos/investigacao-criminal-e-os-dados-obtidos-de-aparelhos-de-celular-apreendidos/198265766. Acesso em: 12 setembro 2023.

SARTORI, R. **A privacidade nas comunicações pelo WhatsApp**. Jusbrasil, 2018. Disponível em: https://robertasartori.jusbrasil.com.br/artigos/581799139/a-privacidade-nas-comunicacoes-pelo-whatsapp. Acesso em: 25 maio 2023.

SILVA, P. P. A. **Polícia pode ter acesso às conversas do WhatsApp em celular apreendido?** Tô de Olho, 2019. Disponível em: https://www.todeolho.net/policia-pode-ter-acesso-as-conversas-do-whatsapp-em-celular-apreendido/. Acesso em: 25 agosto 2023.

VALENTE, Manuel Monteiro Guedes. **Cadeia de Custódia da Prova**. 2. ed, Portugal: Almedina, 2020. Acesso em: 28 agosto 2023

VAZ, Paulo Afonso Brum**. Tutelas de urgência e o princípio da fungibilidade: § 7º, do art. 273 do CPC**. Revista de Processo, São Paulo, v. 32, n. 144, p. 23-37, fev. 2002. Acesso em: 27 outubro 2023

VITAL, Danilo. **Prova ilegal por acesso a celular sem autorização pode ser renovada, diz STJ**. Conjur, 23 fev. 2021. Disponível em: https://www.conjur.com.br/2021-fev-23/prova-ilegal-acesso-celular-renovada-stj?utm_source=dlvr.it&utm_medium=twitter. Acesso em: 25 agosto 2023.