RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

AÇÕES TELEMÁTICAS DESENVOLVIDAS EXCLUSIVAMENTE SOBRE APLICATIVOS DE TROCAS DE MENSAGENS INSTANTÂNEAS

TELEMATIC ACTIONS DEVELOPED EXCLUSIVELY ON INSTANT MESSAGING APPLICATIONS

ACCIONES TELEMÁTICAS DESARROLLADAS EXCLUSIVAMENTE SOBRE APLICACIONES DE MENSAJERÍA INSTANTÁNEA

Phelipe Swiantek de Carvalho[1]

e4124653
https://doi.org/10.47820/recima21.v4i12.4653

PUBLICADO: 12/2023

RESUMO

O artigo em comento visa discorrer sobre a implementação prática de ações de interceptação telemática e quebra de sigilo dos dados telemáticos, desenvolvidas exclusivamente sobre aplicativos de trocas de mensagens instantâneas. Demonstrar quais dados são possíveis extrair, e como utilizá-los para a produção de provas no curso de uma investigação, ou mesmo como ação produtora de conhecimento, no âmbito da Inteligência de Segurança Pública. O conteúdo do presente artigo científico perpassa por conceitos básicos relacionados à matéria, e faz alusão a legislações atinentes às medidas telemáticas desenvolvidas sobre aplicativos de trocas de mensagens instantâneas.

PALAVRAS-CHAVE: Interceptação telemática**.** Quebra de sigilo dos dados telemáticos. Aplicativos de trocas de mensagens instantâneas. Investigação. Inteligência.

ABSTRACT

The paper aims to discuss the practical implementation of telematic interception actions and the breach of secrecy of telematic data, developed exclusively on instant messages apps. It also aims to demonstrate which data can be extract and how to use this data to produce evidence in the course of an investigation, or even as a knowledge-production action within the scope of Public Safety Intelligence. The content of the present paper goes through basic concepts related to the subject and alludes to legislation related to telematic measures developed on instant message applications.

KEYWORDS: *Telematic interception. Breaking confidentiality of telematic data. Instant messaging applications. Investigation. Inteligence.*

RESUMEN

El artículo en discusión tiene como objetivo discutir la implementación práctica de acciones de interceptación telemática y violación del secreto de los datos telemáticos, desarrolladas exclusivamente en aplicaciones de mensajería instantánea. Demostrar qué datos se pueden extraer y cómo usarlos para producir evidencia en el curso de una investigación, o incluso como una acción productora de conocimiento, en el ámbito de la Inteligencia de Seguridad Pública. El contenido de este artículo científico recorre conceptos básicos relacionados con el tema, y alude a la legislación relacionada con las medidas telemáticas desarrolladas sobre las aplicaciones de mensajería instantánea.

PALABRAS CLAVE: *Interceptación telemática. Violación del secreto de los datos telemáticos. Aplicaciones de mensajería instantánea. Investigación. Inteligencia.*

[1] Bacharel em Segurança Pública pela Academia Policial Militar do Guatupê (PMPR). Bacharel em Direito (Universidade Cruzeiro do Sul). Pós-Graduado em Inteligência Policial (Faculdade Campus Elíseos). Pós-Graduado em Segurança Pública (Faculdade Unina). Curso de Inteligência (Diretoria de Inteligência – PMPR). Curso de Gestão da Atividade de Inteligência (ESINT – PMMG). Curso de Entrevista na Atividade de Inteligência (Ministério da Justiça). Curso de Introdução a Atividade de Inteligência (Ministério da Justiça).

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

1 INTRODUÇÃO

O desenvolvimento da rede mundial de computadores e a modernização dos aparelhos celulares, trouxeram consigo a popularização dos aplicativos de trocas de mensagens instantâneas. Segundo Fernandes (2019), o advento citado ensejou na redução do volume de conversas realizadas por ligações comuns, ou seja, sem o uso da internet. A mola propulsora dessa mudança de comportamento ocorreu em 2015, quando os aplicativos de trocas de mensagens desenvolveram uma funcionalidade que permite ao usuário a realização de ligações relativamente gratuitas via internet. Segundo Agrela (2015), em matéria publicada na revista Exame, naquele ano foram sentidas importantes quedas na quantidade de minutos mensais que os brasileiros passavam ao telefone realizando chamada de voz comum. Passado pouco mais de sete anos, houvera ainda mais molas propulsoras que incentivaram o cidadão a utilizar as chamadas via internet, como por exemplo, o desenvolvimento das tecnologias 4G e 5G.

No cenário do desenvolvimento tecnológico, emerge também a mudança do padrão de comunicação das organizações criminosas, as quais, seguindo uma tendência global de mudança de comportamento, passaram a utilizar cada vez menos as ligações tradicionais em detrimento da comunicação via internet. Com o intuito de combater o crime organizado, urge a aplicação de técnicas que sejam suficientemente capazes de fazer frente a referida mudança de comportamento, nesta esteira, o presente artigo científico abordará aspectos técnicos da Interceptação Telemática e da Quebra de sigilo dos dados telemáticos, desenvolvidos exclusivamente sobre aplicativos de trocas de mensagens instantâneas.

2 CONCEITOS BÁSICOS

Antes de aprofundar acerca das questões que dizem a respeito do objeto tema deste artigo científico, se faz necessário conceituar alguns vocábulos e estabelecer algumas diferenças entre termos semelhantes. Neste contexto pragmático inicial, é importante conceituar as atividades de “inteligência de segurança pública”, “inteligência” e “investigação”. O primeiro termo a ser posto em voga, é o de “Inteligência de Segurança Pública”, (ISP), que para a Polícia Militar do Paraná, segundo a Portaria 612/2021, significa:

> Exercício permanente e sistemático de ações especializadas para identificar, avaliar e acompanhar ameaças reais ou potenciais na esfera de Segurança Pública, orientadas para produção e salvaguarda de conhecimentos necessários para subsidiar os tomadores de decisões para o planejamento e execução de uma política de Segurança Pública e das ações voltadas para prever, prevenir, neutralizar e reprimir atos criminosos de qualquer natureza que atentem contra a ordem pública, a incolumidade das pessoas e do patrimônio e do meio ambiente; (PMPR, Portaria nº. 612, 2021, p. 63)

Num segundo momento se faz necessário conceituar a Atividade de Inteligência, que segundo a Agência Brasileira de Inteligência, (ABIN), pode-se definir da seguinte forma:

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

> A atividade de Inteligência é o exercício de ações especializadas para obtenção e análise de dados, produção de conhecimentos e proteção de conhecimentos para o país. Inteligência e Contrainteligência são os dois ramos da atividade. A atividade de Inteligência é fundamental e indispensável à segurança dos Estados, da sociedade e das instituições nacionais. Sua atuação assegura ao poder decisório o conhecimento antecipado e confiável de assuntos relacionados aos interesses nacionais. (Brasil, n. d., Agência Brasileira de Inteligência)

Observamos nestes conceitos iniciais certa semelhança, entretanto, a que se destacar que o fim das duas atividades é a produção de conhecimento, todavia a Atividade de Inteligência é bem mais abrangente, pois engloba as diversas frentes do conhecimento, já a Inteligência de Segurança Pública se mostra como um subgrupo da Inteligência, pois vislumbra produção de conhecimento especificamente no campo da Segurança Pública.

Outro termo importante a ser exposto é o de “Investigação”. Buscas na legislação vigente denotam uma ausência conceitual taxativa da atividade de investigação, todavia neste caso podemos nos socorrer da doutrina, a qual expõe a seguinte definição:

> A investigação criminal no Brasil é um procedimento administrativo para coleção de provas encontradas e elaboradas, na maioria das vezes, pela polícia, que determinam a materialidade e desvendam a autoria de crimes. (Sampaio, 2014)

Por fim, resta diferenciar os termos “Inteligência” e “Investigação”. Conforme definições citadas percebe-se que são atividades distintas, principalmente porque a investigação se mostra uma atividade de natureza reativa, enquanto a inteligência apresenta-se de natureza consultiva/acessória; enquanto a investigação busca identificar autoria e materialidade referente a um delito, naquilo que pode ser tecnicamente comprovado, a inteligência produz e salvaguarda conhecimento, com o fim de assessoramento; enquanto a investigação efetivamente produz provas para instrução processual, a inteligência factualmente produz conhecimento para assessoramento de determinada autoridade tomadora de decisão. Essas são as diferenças básicas referentes aos termos em comento, todavia a dissimilitude não se esgota nos pontos citados.

3 CONCEITOS COMPLEMENTARES

Num segundo momento é necessário trazer à tona a semântica de algumas palavras, pois a compreensão destas locuções são indispensáveis para o entendimento pleno do objeto tema deste artigo científico, o qual gira em torno da interceptação telemática e quebra de sigilo, ou afastamento dos dados telemáticos sobre os aplicativos de trocas de mensagens instantâneas, para tanto iniciar-se-á pela compreensão do termo “telemática”, o qual é definido como conjunto de serviços e técnicas que combinam a utilização de recursos informáticos com os das telecomunicações, (Telemática, 2023).

Em prossecução sobeja estabelecer um significado objetivo para o termo “interceptação telemática”. Podemos inferir da Lei 9296, de 24 de julho de 1996, (Brasil, 1996), que interceptação telemática é o ato de interceptar o fluxo de comunicações telemáticas**,** entretanto a legislação

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

supracitada não é taxativa, neste sentido observa-se a ausência de um conceito técnico para o termo "interceptação telemática". Vislumbrando suprir a lacuna ora citada, apresenta-se uma definição baseada na solução entre o significado da palavra telemática e a referência jurídica contida na Lei 9296/96. Neste caso temos o seguinte conceito de interceptação telemática: Ato de interceptar o fluxo das comunicações, que são baseadas em serviços e técnicas que combinam a utilização de recursos informáticos com os de telecomunicações.

No que diz a respeito da quebra de sigilo, ou afastamento dos dados telemáticos, também se vislumbra uma carência conceitual. A fim de construir um termo razoável acerca da quebra de sigilo dos dados temáticos, pode-se inferir da Lei 12.965/14, Marco Civil da Internet no Brasil, (Brasil, 2014), que a palavra "dados", refere-se a informações de comunicação armazenadas, ou seja, pretéritas. Por fim, novamente se faz necessário citar o significado da palavra "telemática": Conjunto de serviços e técnicas que combinam a utilização de recursos informáticos com os das telecomunicações, (Telemática, 2023). Portanto a quebra de sigilo, ou afastamento dos dados telemáticos pode-se definir como: Ato de acessar os dados armazenados que são baseados em serviços e técnicas que combinam a utilização de recursos informáticos com os de telecomunicações.

4 LEGISLAÇÃO

O presente Artigo não tem por escopo o aprofundamento legal e doutrinário que envolve a interceptação telemática e a quebra de sigilo dos dados telemáticos, mas tão somente apontar as principais normas que dizem a respeito da matéria, a fim de viabilizá-la. Neste contexto a que citar precipuamente a Constituição Federal, Artigo 5º, Inciso XII, onde se vislumbra a flexibilização da inviolabilidade das comunicações:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...)
> XII - É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. (Brasil, 1988).

Adiante cumpre destacar também a Lei 9296/96, que trata sobre a interceptação das comunicações de qualquer natureza, inclusive a telemática. Em primeiro plano, para a implementação da medida, é importante a existência de indícios razoáveis da autoria ou da participação em infração penal. A segunda exigência refere-se à ausência de outro modo para demonstrar o fato apurado, ou seja, se trata de uma medida derradeira. Por fim, é aplicável apenas nos crimes punidos com reclusão.

Sobre o afastamento dos dados telemáticos, cumpre destacar a Lei 12.965/14, Marco Civil da Internet no Brasil, a qual dispõe, no Art. 22, alguns termos imprescindíveis para implementação da quebra de sigilo dos dados telemáticos.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

> Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.
> Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
> I - fundados indícios da ocorrência do ilícito;
> II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
> III - período ao qual se referem os registros.
> (Brasil, 2014).

Por fim resta destacar que o tema não se finda nas leis e nos quesitos supracitadas, a compreensão total do tema é bem mais ampla, e doutrinária, contudo, resta claro a importância de, ao menos, conhecer os pressupostos básicos que viabilizam as ações telemáticas.

5 APLICAÇÃO PRÁTICA

Conforme Resolução do Conselho Nacional de Justiça, 59/2008, Art. 10, após cumpridos os requisitos legalmente previstos para deferimento da medida, o Magistrado fará constar expressamente:

> I – Indicação da Autoridade Requerente;
> II – Os números de Telefones ou nome de usuários, e-mail ou outro indicador no caso de Interceptação de dados;
> III- O prazo de Interceptação;
> IV- A indicação dos titulares dos referidos números;
> V- A expressa vedação de interceptação de outros números não discriminados na decisão;
> VI- Os nomes das Autoridades policiais responsáveis pela investigação e que terão acesso às informações;
> VII- Os nomes dos Funcionários do Cartório, ou Secretaria responsável pela tramitação da medida e expedição dos respectivos Ofícios, podendo reportar-se a portaria do juízo que discipline a rotina cartorária.
> (Brasil, 2008)

Estando a decisão judicial dentro dos parâmetros estipulados pelo CNJ, ela deve ser encaminhada à empresa detentora do aplicativo de trocas de mensagens instantâneas, normalmente acompanhada de um ofício da autoridade responsável pela investigação, por meio dos canais de comunicação da empresa. Na maioria dos casos, as empresas de trocas de mensagens instantâneas detêm um canal exclusivo para autoridades legalmente constituídas enviarem decisões judiciais. Neste ponto, cumpre destacar que os numerais a serem interceptados, ou que sofrerão o afastamento dos dados telemáticos, devem constar na decisão judicial de maneira plenamente assertiva, de modo a seguirem o plano de numeração adotada no Brasil, o qual segue as recomendações da União Internacional de Telecomunicações – UIT, de maneira especial a recomendação E164, (ITU, 2010), com a seguinte composição: [+] [código do país] [DDD sem o zero] [número de telefone].

5.1 Solicitação de preservação de dados

Antes da imersão sobre a aplicabilidade das medidas de interceptação telemática e quebra do sigilo dos dados telemáticos, existe uma medida extrajudicial que pode ser desenvolvida logo no início

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

de uma investigação, sem prejuízo das medidas subsequentes, independentemente do aprofundamento da investigação, que é a solicitação de preservação de dados**.** Essa medida não se correlaciona com a interceptação telemática, uma vez que essa é proativa, ou seja, não abrange dados passados. Embora não aplicável na esfera mencionada, a medida de preservação de dados é convergente com o afastamento dos dados telemáticos, pois serve para resguardar os dados cadastrais, os históricos de conexões IP's, as informações de grupos, e a agenda de contatos do investigado. A solicitação de preservação de dados pode ser requerida de maneira extrajudicial, desburocratizada, apenas com base em uma investigação em curso, (Inquérito Policial Militar, Inquérito Policial comuns, ou um Processo Investigatório Criminal). Geralmente esses dados podem ser preservados por 90 dias, a depender de cada plataforma. A contagem dos dias de preservação ocorre a partir da data de solicitação, e a renovação do pedido fica a critério da mesma autoridade, e deve ser solicitada anteriormente ao vencimento da primeira medida. Por fim, cumpre destacar que a medida extrajudicial é meramente assecuratória, o acesso efetivo aos dados só se dá mediante ordem judicial.

5.2 Interceptação telemática

Interceptação telemática, difere em sua execução da interceptação telefônica, pois no segundo caso a autoridade requisitante pode acompanhar em tempo real todas as interlocuções do ramal interceptado, ao passo que na primeira não existe o acompanhamento em tempo real, mas, tão somente o acompanhamento diário regular, pois as informações são enviadas a cada 24 horas a autoridade requisitante, pelo prazo estipulado na legislação vigente, Lei 9296, de 24 de julho de 1996, Art. 8º-A, § 3º, (Brasil, 1996), ou seja, pelo prazo de 15 dias. Também no primeiro caso não é possível o acesso às interlocuções, pois, segundo as empresas detentoras dos aplicativos de trocas de mensagens instantâneas, a tecnologia de criptografia de ponta-a-ponta, garante que apenas o remetente e o destinatário possam ter acesso ao conteúdo (as mensagens, fotos, vídeos, mensagens de voz, atualizações de status, documentos e chamadas) que é enviado, Segundo as empresas, ninguém além dos interlocutores têm acesso à comunicação, nem mesmo as próprias empresas. A criptografia de ponta a ponta, fica sempre ativada independente da vontade do usuário e não há nenhuma maneira de desativá-la, além disso as empresas alegam que não guardam as mensagens depois de serem entregues ao destinatário, (Whatsapp, 2023).

Apesar do que consta supracitado, existem outras informações dentro da interceptação telemática que, essas sim podem ser disponibilizados para a autoridade requisitante, quais sejam: extratos de comunicação, consistente nas informações de remetente e destinatário; data e hora da comunicação; tipo da comunicação e o registro de acesso da conta alvo se disponível. Destaca-se, mais uma vez, que para essa medida não existem informações pretéritas disponíveis, mas tão somente aquelas contempladas pelo período da interceptação. Por exemplo, caso a autoridade requisitante solicite uma interceptação telemática referente a um mês atrás, esse é um pedido impossível de ser atendido, uma vez que essas informações não são armazenadas pelas empresas, seria a mesma coisa que pedir uma interceptação telefônica referente ao ramal "x", de uma data pretérita, ou seja, impossível

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

de ser cumprido, uma vez que teoricamente não existem trabalhos operacionais para interceptar aquela linha referente ao período almejado.

A interceptação telemática de aplicativos de trocas de mensagens instantâneas é uma medida muitíssimo útil, pois tem a capacidade de fornecer dados que auxiliam na elucidação de delitos. Também é uma medida produtora de conhecimento, que pode auxiliar tecnicamente o tomador de decisão na prevenção de crimes. Suponhamos hipoteticamente que determinado investigado esteja mancomunado com demais membros de uma Organização Criminosa, e na atual conjuntura da investigação estão sendo alvos de interceptação telemática, neste contexto, a primeira prova que pode ser produzida, consiste no estabelecimento dos vínculos entre os investigados, fato devidamente comprovado pelo extrato de conversas diárias. A medida se mostra também eficaz na produção de conhecimento acerca da organização criminosa. Dentro do mesmo exemplo hipotético citado anteriormente, suponhamos que os malfeitores criem um grupo de conversas, dentro da plataforma do aplicativo, a fim de alinhar os detalhes de uma ação criminosa, pois bem, neste caso, quando o terminal interceptado enviar uma mensagem no grupo, constará no extrato de conversas todos os destinatários daquela mensagem, data e hora da mensagem, tamanho da mensagem, formato dela, se áudio ou texto, de modo que, após um trabalho apurado, a polícia poderá apontar todos os suspeitos que possivelmente farão parte, direta e indiretamente da ação, e com base no conhecimento produzido, balizar o policiamento ostensivo para a prevenção da ação, até que a investigação esteja madura o suficiente para ser deflagrada. Noutro exemplo hipotético, mas dessa vez voltado ao tráfico de armas e drogas, certo traficante investigado, em parceria com demais meliantes, engendrou uma forma de envio de entorpecentes de Foz do Iguaçu para Paranaguá, dois extremos do Estado do Paraná. Tal envio consiste na remessa diária de caminhões aparentemente idôneos, com cargas lícitas para o Porto de Paranaguá, entretanto dentro dos caminhões, em fundos falsos, acomoda entorpecentes e armas de fogo. A ação se mostra avançada pois, em alguns casos, nem mesmo o motorista sabe acerca do transporte do ilícito, pois a droga é implantada durante o carregamento, por terceiros, longe da vista do condutor. Considerando que uma investigação complexa pode levar um tempo considerável para ser exposta, algumas medidas de contenção podem ser tomadas a fim de evitar o crescimento e aprimoramento do *modus operandi*[2] desta ORCRIM[3], (Brasil, 2013), neste cenário a interceptação telemática pode ser uma importante ferramenta de contenção, pois, o conhecimento produzido no curso da investigação pode, por meios técnicos, orientar o policiamento ostensivo, a ponto de indicar, com base na fundada suspeita, quais cidadãos devem ser abordados, para que haja a comprovação do delito, e também para conter o envio de drogas e armas. Por fim, mas não menos importante, a que se frisar, que em ações reais as abordagens devem sempre serem direcionadas e dosadas pela investigação a fim de não atrapalhar o curso das diligências.

[2] Modus Operandi – expressão em latim que significa modo de operação.
[3] ORCRIM – Organização Criminosa, Lei 12.850 de 2 de agosto de 2013.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Além dos breves exemplos citados, existem outras infinidades de provas e informações que podem ser produzidas com base na Interceptação Telemática. A referida técnica se mostra ainda mais positiva quando aplicada em concomitância com demais técnicas, como por exemplo a quebra de sigilo dos dados telemáticos de aplicativos de trocas de mensagens instantâneas, a qual será abordada a seguir.

5.3 Quebra de sigilo dos dados telemáticos

A quebra de sigilo dos dados telemáticos é uma medida diferente da interceptação telemática, porém complementar. Considera-se importante ser feita em paralelo com a primeira quinzena da interceptação telemática, pois a referida medida entrega dados relevantíssimos acerca da compreensão dos vínculos dos investigados. O pedido dos dados armazenados podem conter os seguintes quesitos: Dados cadastrais da conta (informações do aparelho e sistema operacional, versão da *App*, data e horário do registro, status de conexão, última conexão com data e hora, nome, endereço de e-mail se disponível, e informações de cliente Web); Foto de perfil; Registros de acesso (IPs) dos últimos 6 meses; Histórico de mudança de números; Grupos (data de criação, descrição, identificador do Grupo ("*group-ID*"), Foto, quantidade de membros e nome do Grupo); e Agenda de contatos.

Informações do aparelho e sistema operacional: a respeito das informações do aparelho e sistema operacional, o requisitante receberá os dados técnicos característicos do aparelho celular que está sendo utilizado para troca de mensagens, como por exemplo:

Quadro 1: Informações do aparelho e sistema operacional

Nome do modelo: Apple iPhone 7
Número do modelo: 15.6.1
Sistema operacional: iPhone

A partir desses dados pode-se produzir uma gama de conhecimentos importantíssimos que delimitam demais ações investigativas ou de produção de conhecimento. Por exemplo, quando uma medida de busca e apreensão está na iminência de ser cumprida, e temos uma ação de quebra de sigilo dos dados telemático precedente a Busca, pode-se produzir um conhecimento básico, destinado a equipe policial que cumprirá a medida, informando detalhadamente todos as características do aparelho a ser buscado, evitando assim diligências desnecessárias e/ou equivocadas. Obviamente existem outras dezenas de aplicações, tanto investigativas como de produção de conhecimento que podem ser extraídas a partir dos dados supracitados.

Versão do *App*[4]: neste ponto da quebra de sigilo dos dados telemáticos, a informação que se pode extrair acerca da versão do *App*, está relacionada às funcionalidades disponíveis, que podem ser utilizadas pelo investigado. As versões mais atuais dos aplicativos de trocas de mensagens

[4] App – Aplicativo.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

instantâneas dispõe de recursos que permitem o acesso a uma mesma conta, de pontos geográficos distintos, e isso implica diretamente na quantidade de suspeitos envolvidos num mesmo delito, e também em outras infinidades de desdobramentos advindos dessa informação.

Data e horário do registro: esse dado fornecido diz a respeito da entrada do investigado na plataforma a partir daquele terminal, informação útil que pode corroborar ou não com demais elementos de convicção.

Status de conexão: acerca do Status da conexão, existem dois estados possíveis, *"on line"* ou *"off line",* ambos dizem a respeito da interatividade daquele dispositivo com a rede mundial de computadores.

Última conexão com data e hora: neste campo tem-se a utilidade, "visto pela última vez", informação sobre o último acesso do usuário ao aplicativo, conhecimento relevante, que somado a demais elementos de convicção podem contribuir com a investigação ou como produção de conhecimento.

Nome: a informação relativa ao nome é opcional ao usuário dos aplicativos de trocas de mensagens instantâneas, portanto não é uma fonte fidedigna, uma vez que o usuário pode não preencher esse campo, pode preencher qualquer nome distinto, ou pode somente colocar um *emoji*[5] no lugar. Portanto a informação relativa ao nome deve ser cautelosamente analisada.

Endereço de *e-mail*: referente ao endereço de *e-mail*, este também é outro ponto de preenchimento facultativo aos usuários de aplicativos de trocas de mensagens instantâneas. A funcionalidade dos *e-mails* para os usuários, serve para terem um meio de recuperação da conta. Se a informação estiver disponível, deve-se somar ao trabalho em curso.

Foto do Perfil**:** a foto do perfil é um elemento de convicção que pode contribuir para a investigação. Atualmente os sites de pesquisas disponibilizam ferramentas de buscas reversas a partir de imagens.

> A busca reversa de imagens é uma técnica computadorizada que envolve a recuperação de imagens a partir de seu conteúdo. É um tipo de "consulta de imagem através de um exemplo" na qual, dependendo do contexto de cores, formas, texturas, metadados ou quaisquer outras informações derivadas da imagem, são obtidos resultados de grandes bases de dados de imagem com imagens digitais (González, 2016).

A operacionalização da técnica de busca reversa é simples: Deve-se salvar parte da imagem investigada ou ela toda em algum arquivo disponível. No site de buscas como por exemplo o Google, deve-se clicar no ícone "câmera fotográfica" existente na parte superior direita do navegador, depois disso o site vai pedir para que o operador faça o upload da imagem a ser analisada. Por fim, o próprio buscador vai garimpar na rede mundial de computadores por imagens semelhantes, links que contenham a imagem, ou mesmo a própria imagem em tamanhos distintos. A Técnica citada é auxiliadora e pode contribuir com a identificação do local onde determinada imagem foi capturada.

[5] *Emoji* – Pictograma ou ideograma que transmite a ideia de uma palavra ou frase, (Padilha, 2023).

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Deve-se levar em consideração que o sistema aceita qualquer imagem, portanto essa fonte de dados deve ser cautelosamente analisada, pois pode ter sido inserida com intuito criminoso, vislumbrando despistar investigações em curso, pelo que reitero a importância de aliar este dado com demais elementos de convicção, a fim de se chegar a um veredito assertivo acerca do perfil do usuário.

Ademais, as análises das fotos de perfil podem servir como base para identificação de pessoas por meio do reconhecimento biométrico, utilizando bases de dados distintas. Por fim, mas ainda na questão da foto de perfil, existem algumas hipóteses que podem contribuir pouco com a investigação, as quais giram em torno da ausência da foto de perfil, ou a colocação de uma imagem aleatória.

Registros de acesso (IPs) dos últimos 6 meses: os dados relacionados ao endereço IP, são dos mais valiosos entregues pela quebra de sigilo dos dados telemáticos dos aplicativos de trocas de mensagens instantâneas, mas o que é um endereço IP?

> Endereço IP significa “endereço do Protocolo de Internet”. O Protocolo de Internet é um conjunto de regras para comunicação pela internet para envio de e-mail, streaming de vídeo ou conexão a um site. Um endereço IP identifica uma rede ou dispositivo na internet. (Patrizio, 2019).

Todo dispositivo conectado à internet tem um endereço IP capaz de identificar o dispositivo e a rede que ele está utilizando para se comunicar. Neste contexto, a operacionalização do uso desses dados para uma investigação ou como fonte de produção de conhecimento, se faz com auxílio de sites denominados localizadores de IP. Nestes sites, geralmente, existe um campo para a submissão do IP. O resultado da busca vai informar o provedor da internet, ou seja, qual empresa disponibilizou a internet que o investigado utilizou. Sabendo quem é o provedor de internet, em posse dos dados de IP, data e hora da conexão, é possível que o provedor forneça os dados cadastrais do cliente detentor do ponto de internet, e a localização. Portanto, as informações relacionadas ao IP podem apontar localidades de organizações criminosas, e identificar pessoas, principalmente aquelas que acreditam estar ocultas por detrás da tela de um eletrônico. Finalmente, salienta-se a necessidade de autorização judicial para desenvolvimento da ação.

Histórico de mudança de números**:** é comum que os aplicativos de trocas de mensagens instantâneas permitam ao usuário a troca de número, mantendo os mesmos dados cadastrais, e preservando as conversas individuais e em grupo do usuário, fato consumado por meio de uma migração dos dados para o novo número. Também é comum que cidadãos em cometimento de delitos realizem a troca de número a fim de desbaratar ações investigativas em curso, portanto o histórico de mudança de números se mostra eficaz para a produção de provas que demandem comprovações de rastreabilidade, ou mesmo como fonte produtora de conhecimento.

Grupos: as informações relativas aos grupos de trocas de mensagens que o investigado/usuário participa, estão ligadas de modo intrínseco ao delito que tal investigado possa estar cometendo.

A data da criação dos grupos: O dado relativo à data de criação dos grupos aos quais o investigado participa também é disponibilizado, a informação pode ser, quando em consonância com

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

demais elementos de convicção, um excelente indicativo a respeito do período que o alvo está realizando determinada prática criminosa.

A descrição do grupo: o espaço serve para os administradores daquele grupo colocarem informações de interesse comum a todos os participantes. Suponhamos hipoteticamente que uma quebra de sigilo telemático revelou a existência de um grupo de trocas de mensagens instantâneas, onde seus membros sabidamente são faccionados a uma determinada organização criminosa, e consta na descrição do grupo, por exemplo, os dados bancários de terceiros, que servem para depósitos proveniente de lucros de ações criminosas; pode conter também orientações de conduta, e/ou mensagens subliminares, enfim, a depender da descrição do grupo, provas poderão ser produzidos acerca das entranhas da criminalidade.

Identificador do grupo: Outro dado disponível referente aos grupos do investigado é o Identificador do grupo, se trata de uma sequência alfa numérica exclusiva, é a identidade formal do grupo, portanto, trata-se de um dado que servirá como balizador de pedidos complementares futuros que o requerente fizer a plataforma de troca de mensagens acerca daquele grupo.

Foto de capa: a foto de capa dos grupos que o investigado participa também é acessível, se trata de um elemento que na maioria das vezes demanda uma análise técnica acerca da representação da imagem com o objetivo do grupo. Por vezes, ocorre que em análises das fotos dos grupos de organizações criminosas, as imagens não correspondem com o objetivo do grupo, justamente com o propósito de ludibriar investigações, pelo que uma análise minuciosa, em consonância com demais indicativos qualificarão o dado.

A quantidade de membros existente no grupo: tal informação constará no rol de informações atinentes ao grupo que o investigado participa, todavia, os dados dos membros desses grupos não. Neste ponto se faz importantíssimo mencionar que no pedido inicial de quebra de sigilo dos dados telemáticos, o requerente deve solicitar também a autorização para o fornecimento de dados dos membros dos grupos que vierem a ser indicados formalmente, pela autoridade responsável do caso. Deste modo aquele grupo que for considerado suspeito poderá ser analisado em minúcias, sem burocracias, de modo a otimizar o tempo do analista e do Poder Judiciário.

Nome do grupo: constará disponível o nome de cada grupo, é um elemento que pode estar associado a foto do grupo, e assim como aquele dado, este deve ser tratado cautelosamente, pois em ações criminosas esses elementos se mostram avesso ou desconexo ao intuito do grupo. Exemplificando hipoteticamente: Em um grupo criado para a prática do tráfico de drogas, dificilmente será nomeado com palavras que remetem aos entorpecentes, contudo, possivelmente serão utilizados vocábulos diametralmente opostos ao crime em comento, como por exemplo, nome do grupo “Ação social”. Esse é um método bem comum de disfarce de práticas delituosas em nomes de grupos.

Agenda de contatos: Os aplicativos de trocas de mensagens instantâneas fornecem a agenda de contatos do investigado, e informam se o contato é simétrico ou assimétrico. Geralmente quando falamos em simetria e assimetria num contexto de tecnologia da informação, fala-se em diferentes tipos de criptografia, todavia, neste caso não. Para a quebra de sigilo dos dados telemático dos aplicativos

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

de trocas de mensagens instantâneas, os contatos simétricos traduzem os contatos que o alvo tem salvado em sua agenda virtual, de forma recíproca; já os contatos assimétricos apontam para os contatos que o alvo tem salvado em sua agenda virtual, mas sem reciprocidade. As informações de contatos podem denotar proximidade entre dois investigados, e servem como prova técnica da relação entre as partes.

6 CONCLUSÃO

As mudanças dos padrões comportamentais de comunicação projetam a segurança pública para áreas do conhecimento que outrora não eram exploradas, como o das comunicações interpessoais estabelecidas pela internet. Neste contexto, o presente artigo científico destrincha um tema pouco explorado na literatura, como a aplicabilidade de medidas telemáticas exclusivamente sobre os aplicativos de trocas de mensagens instantâneas.

A utilização dos referidos aplicativos são uma realidade pujante num contexto social onde as comunicações se estabelecem em sua grande maioria pela internet, pelo que também se faz necessário a aplicação de técnicas diferenciadas como: a preservação dos dados armazenados, a interceptação telemática, e a quebra do sigilo dos dados telemáticos, em relação aos aplicativos de trocas de mensagens instantâneas, para fazer frente ao avanço tecnológico.

Em convergência com a narrativa do parágrafo anterior, observa-se que as ações telemáticas apresentadas ao longo desta síntese, são auxiliadoras em relação a produção de provas e/ou como fonte produtora de conhecimento. Todavia o desenvolvimento dessas ações demandam um conhecimento específico, e a compreensão de legislações próprias.

Outrossim, é importante compreender quais dados pode-se extrair a partir de cada medida discutida ao longo deste artigo científico, e desmistificar a existência de uma suposta complexidade por detrás das ações telemáticas sobre os aplicativos de trocas de mensagens instantâneas, as quais sempre devem ser realizadas com autorização judicial, dentro dos ditames legais.

Por fim, conclui-se que as ações telemáticas são importantíssimas para a produção e qualificação de provas. Além do mais, são riquíssimas fontes produtoras de conhecimento, capazes de assessorar o tomador de decisão responsável pelo policiamento ostensivo, portanto indispensáveis para a Segurança Pública moderna.

REFERÊNCIAS

AGRELA, Lucas. Ligações gratuitas do WhatsApp derrubam tempo médio de chamadas tempo médio de chamadas telefônicas. **Exame**, 2015. Disponível em: https://exame.com/tecnologia/ligacoes-gratuitas-do-whatsapp-provocam-queda-no-tempo-medio-de-chamadas-telefonicas/. Acesso em: 24 jan. 2023.

BRASIL. Agência Brasileira de Inteligência (ABIN). **Inteligência e Contrainteligência**. Brasilia: Telemática, s. d. Disponível em: https://www.gov.br/abin/pt-br/assuntos/inteligencia-e-contrainteligencia. Acesso em: 12 mar. 2023.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

BRASIL. **Constituição da República Federativa do Brasil**. Brasilia: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 fev. 2023.

BRASIL. **Lei 12.850, de 2 de agosto de 2013**. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção de provas, infrações penais correlatas e o procedimento criminal. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 12. mar. 2023.

BRASIL. **Lei 12.965/14, de 23 de abril de 2014**. Marco Civil da Internet no Brasil. Estabelece princípios, garantias, direitos e deveres para o uso da internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 fev. 2023.

BRASIL. **Lei 9296, de 24 de julho de 1996. Dispõe o inciso XII, parte final, do artigo**. 5º da Carta Magna. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 10 fev. 2023.

BRASIL. **Resolução do Conselho Nacional de Justiça, 59/2008, de 9 de agosto de 2008**. Disponível em: https://www.conjur.com.br/dl/resolucao-59-cnj.pdf. Acesso em: 16 fev. 2023.

FERNANDES, Carol. Dez anos de WhatsApp: Relembre os recursos mais marcantes do *App*. **Tech Tudo**, 2019. Disponível em: https://www.techtudo.com.br/noticias/2019/02/dez-anos-do-whatsapp-veja-as-novidades-mais-marcantes-do-app.ghtml. Acesso em: 15 fev. 2023.

GONZALES, Gabriel. **Para que serve e como se faz uma busca reversa de imagens**. [S. l.]: Blog think big, 2016. Disponível em: https://br.blogthinkbig.com/2016/06/24/para-que-serve-e-como-se-faz-uma-busca-reversa-de-imagens/. Acesso em: 18 fev. 2023.

ITU - INTERNATIONAL TELECOMMUNICATION UNION. **E164**, de novembro de 2010. International operation – Numbering plan of the international telephone service. Disponível em: https://www.itu.int/rec/T-REC-E.164/en. Acesso em: 16 fev. 2023.

PATRIZIO, Andy. **O que é um endereço IP?**. [S. l.]: Avast, 2022. Disponível em: https://www.avast.com/pt-br/c-what-is-an-ip-address. Acesso em: 17 fev. 2023.

PMPR. **Portaria nº. 612/2021 – CG**. Política de Inteligência da Polícia Militar do Paraná. Curitiba: Ajudância-Geral, Boletim do Comando-Geral nº. 118, de 29 jun. 2021.

SAMPAIO, Nílian Chrystine Rosa. **Investigação criminal: atuação suplementar do Ministério Público**. [*S. l.: s. n.*], 2014. Disponível em: https://repositorio.uniceub.br/jspui/handle/235/5963. Acesso em: 11 mar. 2023.

TELEMÁTICA. *In*: **Estraviz, Dicionário online de português**. [*S. l.: s. n.*], 2023. Disponível em: https://estraviz.org/telem%C3%A1tica. Acesso em: 4 mar. 2023.

WHATSAPP. **Law eforcement request online system**. [*S. l.: s. n.*], 2023. Disponível em: https://www.whatsapp.com/records/login/?locale=pt_BR. Acesso em: 14 mar. 2023.