

# A QUEBRA DO SIGILO TELEFONICO E PRIVACIDADE DOS DADOS COMO MEIO DE PROVA NA ERA PÓS INTERNET<sup>1</sup>

Dayane da Silva Fideris<sup>2</sup>  
Yzamara de Caldas Serpa<sup>3</sup>  
Franklin Jones Vieira<sup>4</sup>

## RESUMO

A quebra do sigilo telefônico e privacidade dos dados são disciplinados pela Lei n. 9.296/1996 e, de acordo com a lei, deve ser utilizada se preenchido os requisitos e indícios razoáveis de autoria ou participação em infração penal, devendo ser fundamentada por meio de documentos, testemunhas, entre outros. De acordo com a legislação a interceptação somente será concedida quando for o único meio de prova a conduta delituosa. Observando o cenário e o advento das redes sociais, o artigo traz a necessidade em debater sobre a interceptação e quebra do sigilo e privacidade nos aplicativos de rede social privada e do próprio telefone, observando as permissões e proibições do ordenamento jurídico. Trata-se de um trabalho de cunho bibliográfico, que se utilizou de levantamento literário em leis, artigos, revistas eletrônicas e doutrinas que abordam a temática, diante de tais estudos se alcançou os resultados e conclusões.

**Palavras-chave:** Sigilo telefônico. Privacidade de dados. Redes Sociais. Legislação. Tipificação penal.

Data da aprovação: 20 de outubro de 2020.

---

<sup>1</sup> Artigo apresentado como requisito parcial para a conclusão do curso de Graduação em Direito da Faculdade de Ensino Superior da Amazônia Reunida – FESAR. 2020.

<sup>2</sup> Acadêmica do curso de Bacharelado em Direito da Faculdade de Ensino Superior da Amazônia Reunida – FESAR. E-mail: [dayanefideris@hotmail.com](mailto:dayanefideris@hotmail.com)

<sup>3</sup> Acadêmica do curso de Bacharelado em Direito da Faculdade de Ensino Superior da Amazônia Reunida – FESAR. E-mail: [yzaserpa10@gmail.com](mailto:yzaserpa10@gmail.com)

<sup>4</sup> Orientador do artigo. Graduado em Direito pela Universidade Iguazu. Especialista em Direito Processual Civil pela faculdade Integrada de Jacarepaguá. Mestrando em Ciências Criminais pela Universidade Autônoma de Lisboa- PT. Promotor de Justiça do Ministério Público do Estado do Pará. E-mail: [franklinjonesvieira@gmail.com](mailto:franklinjonesvieira@gmail.com).

## 1 INTRODUÇÃO

A evolução digital e o avanço das ciências eletrônicas facilitaram o acesso ao universo dos computadores, à internet e diversas outras tecnologias, permitindo a comunicação através de sistemas *online*, aplicativos e a telefonia. O acesso a esses meios de comunicação trouxe à sociedade impactos, conceitos e regras que precisaram ser revistos para a nova realidade.

O uso das redes sociais e aplicativos de comunicação como Instagram, Mensseger, Whatsapp, Facebook entre outros estão presentes diariamente nos meios eletrônicos, seja para relacionamento pessoal ou comercial, e em muitos casos são utilizados para cometer crimes e causar problema a usuários e população em geral.

A internet proporcionou muitos benefícios, mas também trouxe fraudes, estelionatos, atividade criminal, oportunismo e algumas inseguranças. Porém, atualmente, não há como viver sem os meios de comunicações, aplicativos e outros benefícios que a rede de computadores e a internet oferece para facilitar nossa vida.

Todo o processo de exposição do usuário se inicia ao se conectar, pois é necessário o uso de aparelhos controlados por provedores de internet e os registros ficam em logs de acessos discados, por meio de algumas técnicas é possível identificar o IP da máquina usada para o acesso e, por conseguinte, analisar textos e documentos que foram enviados ou recebidos, no entanto, a privacidade das informações digitais nas redes sociais tem sua proteção garantida pelo Marco Civil da Internet.

Esse é o primeiro ponto da vulnerabilidade dos dados dos usuários da rede de internet, outras formas de exposição dos dados podem acontecer no momento da prisão do indivíduo, que sem ordem judicial pode ter seu celular apreendido e os dados do telefone revelado durante o processo de investigação. O importante é conhecer o que é legal e ilegal durante a apreensão de bens, prisão e outras formas de exposição das pessoas.

Partindo dessa premissa, o artigo traz em seu bojo uma discussão fundamentada sobre as formas de quebra de sigilo telefônico e privacidade dos dados permitidas por lei, apontando as formas legais de se fazer uso desse instituto para composição de provas durante o processo. Por outro lado, em se tratando de sigilo dos dados do telefone, a pesquisa traz, em breves considerações, as formas ilegais que vem acontecendo essa quebra de privacidade do usuário da internet e/ou suspeitos de ter cometido crimes.

Trata-se de um trabalho bibliográfico com fundamentação em lei, artigos científicos, revistas eletrônicas, sites da justiça nacional, doutrinas e outros. O objetivo é conhecer as formas de quebra de sigilo telefônico e privacidade dos dados permitidos por lei, somente com o conhecimento dos requisitos podemos resguardar nossos direitos em situações que envolve a guarda de nossa privacidade.

A pesquisa é de suma importância, pois com o avanço tecnológico e a rapidez na transmissão dos dados, os usuários ficam vulneráveis a exposição, e isso tem acontecido constantemente, porém, muitos não sabem como agir e nem quais medidas tomar ao sofrer a exposição.

O artigo descreve de forma sucinta sobre o acesso à internet no Brasil, aborda sobre a criminalidade no cyberspaço, a interceptação telefônica e de dados e ainda exemplo prático do STJ sobre uma forma ilegal de interceptação de dados do telefone por meio das redes sociais e aplicativos de mensagens. Nesse sentido, o trabalho traz as informações de forma objetiva, direta e coerente sobre o assunto abordado.

## **2 ACESSO A INTERNET NO BRASIL**

Para entender melhor sobre a exposição do usuário das redes de internet é necessário entender como funciona todo o sistema e, por conseguinte, entender qual a forma legal de se utilizar dessas informações como meio de prova. Por isso, é preciso conhecer todo o mecanismo desde a base, o acesso à internet no Brasil.

Primeiro temos que entender que os direitos, deveres e responsabilidades de provedores, internautas, empresas, bem como dos poderes executivo, legislativo e judiciário na Web, no Brasil, são regulados pela disposição normativa chamada Marco Civil da Internet. De acordo com o art. 4º da Lei n.º 12.965/2014, o acesso à internet é um direito de todo cidadão brasileiro, porém é um espaço com regras e tem como objetivos a promoção:

I - do direito de acesso à Internet a todos os cidadãos; II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos; III- da inovação e fomentar a ampla difusão de novas tecnologias e modelos de uso e acesso; e IV- da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados (BRASIL, 2014).

A partir do Marco Civil da Internet o direito ao acesso à internet passou a ser tratado como direito essencial e universal ao exercício da cidadania, um direito universal, tomando um

status de direito fundamental. O art. 7º da Lei 12.965/2014 descreve que o acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados vários direitos, dentre eles, a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação (inciso I).

O art. 7º da referida lei também assegura a inviolabilidade e sigilo de suas comunicações pela internet, além da inviolabilidade e sigilo das comunicações privadas armazenadas, salvo por ordem judicial, na forma da lei (inciso II e III). No que concerne à livre manifestação de pensamento, ao direito À privacidade e sigilo das comunicações do usuário pela internet, o art. 8º do Marco Civil da Internet reafirma o previsto pela Constituição Federal de 1988, que a “garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à Internet”.

O problema, no entanto, se concentra no uso inescrupuloso da web, o que ocasiona um número significativo de crimes cibernéticos, o que promove preocupação a usuários dos meios tecnológicos. Por tais motivos, é necessário cuidados básicos ao navegar pela web, porém, Kunrath (2017, p. 21) aponta que ao contrário do que se apregoa, a maioria dos usuários da internet utiliza a rede com boas intenções. E que apenas uma pequena parcela de usuários extrapola a linha da boa-fé, da ética e da urbanidade, violando os basilares direitos à privacidade, ao sigilo das informações, em desrespeito aos direitos e em proveito promíscuo individual e de grupos delinquentes.

A rede de computadores possibilitou a criação de um novo espaço, o virtual, conhecido como ciberespaço composto de multiplicidade de formas de comunicação e sociabilidade. Lemos (2003, p. 1) conceitua ciberespaço como um espaço sem dimensões, com uma gama de informações navegáveis, instantânea e reversível, trazendo ao usuário elementos da magia como manipulação do mundo.

Rover (2004, p. 237-238) descreve que ciberespaço não é um lugar, mas um meio de comunicação, assim como a escrita, o telefone, a radiodifusão, fax, entre outros. Nesse caso, a internet é um sistema global de redes de computadores interligados que utilizam o conjunto de protocolos padrão da internet (TCP/IP) para servir vários bilhões de usuários no mundo inteiro.

No entanto, mesmo com os riscos eminente de práticas delitivas nas relações cibernéticas, tal constatação não impediu a sociedade contemporânea de desenvolver o sentimento de confiança e encantamento para com a rede mundial de computadores, tanto que atualmente a rede é utilizada para as mais diversas necessidades e relevantes objetivos, pela facilidade, rapidez e relativa segurança.

Lemos (2003) ainda aborda sobre as profundas modificações no espaço urbano da sociedade contemporânea, acentua que o cenário se transformou em suas formas sociais e nas práticas da cibercultura emergindo, então, novas formas de comunicação:

A cibercultura nada mais é do que a cultura contemporânea em sua interface com as novas tecnologias de comunicação e informação, ela está ligada às diversas influências que estas tecnologias exercem sobre as formas de sociabilidade contemporâneas, influenciando o trabalho, a educação, o lazer, o comércio, etc. Todas as áreas da cultura contemporânea estão sendo reconfiguradas com a emergência da cibercultura. (LEMOS, 2003, p. 1).

Portanto, uma nova época é definida a partir do uso das tecnologias presentes nos dias atuais e ocorre na dimensão do ciberespaço. Dessa forma, Kunrath (2017, p. 24) aponta que o espaço físico vem perdendo sua importância, frente às novas possibilidades tecnológicas que também influenciam e outras variáveis como o tempo e distância, volumes e medidas.

O ciberespaço é um ambiente diferenciado do modelo físico tradicional, nesse espaço, por exemplo, abriga uma biblioteca virtual enorme, com um número bem superior de obras em relação a uma biblioteca física e o espaço para abrigar todas as obras é bem reduzido, necessitando apenas de ferramentas de busca para chegar ao usuário em questão de segundos. Da mesma forma que acontece em outras áreas científicas, as novas tecnologias vêm revolucionando a ciência com o uso crescente das tecnologias digitais, marcadas por uma relação entre a técnica e a vida social.

Essa nova forma de agregação social de maneira espontânea no ambiente virtual, com práticas culturais específicas conhecida como a cibercultura, alude uma nova realidade com transformações rápidas e avanços tecnológicos. A sociedade vive uma nova era, a da revolução da informação e comunicação, através da tecnologia da informação (TI).

Tecnologia da informação e comunicação ou TIC é a área que utiliza ferramentas tecnológicas com o objetivo de facilitar a comunicação e o alcance de um alvo comum. As TICs também servem para potencializar os processos de comunicação (SCHMIDLIN FILHO, 2016).

Kunrath (2017, p. 25) descreve que nesse cenário, a problemática ligada ao acesso e não acesso, implica nas consequências da inclusão e exclusão social e digital, nesse fenômeno pode ser visto a produção e acesso as informações coletivas, com fluxo mais intenso de informações, no qual não é mais possível identificar com precisão onde se situa o mundo real e o virtual.

Assim, a utilização dessa tecnologia pode ser para difundir informações úteis à sociedade, ou mesmo ser utilizada como meio de divulgação de informações falsas, que prejudiquem direitos de terceiros, por exemplo, dados que possam ludibriar vítimas para obter vantagens ilícitas, ou gerar danos, causando prejuízos. Por essa razão que, na sociedade atual, requer um olhar especial sobre a internet, principalmente para as questões éticas, a livre expressão, o controle de acesso, dentre outras questões.

### **3 A CRIMINALIDADE NO CIBERESPAÇO**

A literatura científica internacional demonstra que o universo dos crimes informáticos teve seus primeiros indícios no século XX, mais precisamente em 1960, onde se deu as primeiras referências sobre essa modalidade de crimes nas mais diversas denominações, com maiores incidências em casos de manipulação e sabotagem de sistemas de computadores (LIBERATI, 2011).

Na década de 1970, a figura do hacker (invasor de sistemas) já era citada com o advento de crimes como invasão de sistema e furto de software, mas foi em 1980 que houve maior propagação dos diferentes tipos de crimes como a pirataria, pedofilia, invasão de sistemas, propagação de vírus, surgindo então com isso a necessidade de se despender maiores preocupações com a segurança virtual que exige uma atenção especial para identificação e punição dos responsáveis, que a essa altura estão em todos os lugares do mundo (CARNEIRO, 2012).

Ao contrário do que muita gente pensa, a origem dos crimes informáticos pode não estar diretamente relacionado com o surgimento da internet, como exemplo pode-se citar: manipulações de caixas bancários, pirataria de programas de computadores, sabotagem de equipamentos, obtenção de dados não autorizados. São formas diversas que não dependem essencialmente da internet para executar os crimes cibernéticos.

#### **3.1 DA TIPIFICAÇÃO DOS CRIMES VIRTUAIS**

As tipificações dos crimes cibernéticos estão distribuídas no Código Penal e leis especiais, não há uma lei específica que engloba todos os crimes virtuais. Abaixo segue os principais crimes tipificados no ordenamento jurídico, entre outros, que podem ser realizados por meio da tecnologia da informação, são os chamados crimes virtuais impróprios.

Por haver essa dissociação do mundo virtual para o real, os usuários penetram nas redes como se fosse um ambiente seguro no qual a propagação de suas palavras, supostamente não passariam da tela de seu computador, o que acarreta a disseminação de opiniões, imagens e palavras ofensivas, podendo configurar em crimes contra a honra: calúnia, difamação e injúria, previstos nos art. 138, 139 e 140 do Código Penal.

Lucena (2012 *apud* Kunrath, 2017, p. 25) aborda a dissociação do comportamento frente a internet como efeito desinibitivo on-line, tendo como fatores interativos o anonimato dissociativo, invisibilidade, assincronismo, introjeção solipsta, imaginação dissociativa e mineralização da autoridade. Do ponto de vista criminológico, Lucena (2012, *apud* Kunrath, 2017) equipara o quadro ao que se denomina subcultura criminal do mundo virtual.

Nesse prisma, a dissociação entre os dois mundos acarreta outros crimes como a ameaça prevista no art. 147 do CP e ainda os crimes de furto, dano, apropriação indébita, estelionato, violação ao direito autoral, ambos previstos nos art. 155, 163, 168, 171, 184 e pedofilia, crime previsto no art. 247 da Lei n. 8.069/90 (Estatuto da Criança e do Adolescente).

Além das tipificações citadas ainda temos os crimes contra a propriedade industrial, Art. 183 e segs. da Lei 9.279/96; os crimes virtuais próprios tipificados no ordenamento jurídico como a Interceptação de comunicações de informática, art. 10 da Lei n. 9.296/96; Interceptação de E-mail Comercial ou Pessoal, art. 10 da Lei n. 9.296/96 e os crimes contra software -“Pirataria”, Art. 12 da Lei n. 9.609/98.

Observando as tipificações penais previstas para os crimes virtuais um deles merece destaque, a interceptação das comunicações de informática e dados nos meios sociais virtuais. Mesmo que a inviolabilidade dessas informações seja amparada pela Constituição Federal como um direito fundamental, ainda há muitos casos em que a quebra de sigilo desses dados acontecem sem ordem judicial. Para melhor entendimento é necessário entender como acontece a interceptação ilegal de dados.

### **3.1.1 Da interceptação ilegal de dados**

A Constituição Federal de 1988 garantiu a inviolabilidade das comunicações, fixando tal garantia como um direito fundamental (BRASIL, 1988). Todavia, a inviolabilidade não é absoluta, sendo autorizada mediante ordem judicial a interceptação das comunicações para fins de investigação policial (CNJ, 2008; BRASIL, 2014).

Assim, a Lei n. 9.296/96 regulamenta as interceptações telefônicas, autorizando, todavia, a interceptação de comunicação em sistemas de informática e telemática.

Ademais, prevê a tipificação da conduta de quem realiza as ingerências sem autorização judicial ou em desconformidade com aquela concedida. Assim aduz o Art. 5º, inciso XII da referida lei:

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, 1996).

O artigo acima descreve a forma legal de se realizar a interceptação de informações, no entanto, a Lei n. 9.296/96 prevê, no seu art. 10, como crime o fato de alguém realizar a interceptação telefônica, telemática ou informática sem autorização judicial ou em desconformidade com a lei. Essa disposição não deixa de ser uma incriminação contra a interceptação, de forma a cumprir a o proposto na Convenção de Budapeste.

Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa (BRASIL, 1996).

Sem dúvida, a conduta de interceptação ilegal de dados em sistemas informáticos ou telemáticos deve ser coibida, já que cada vez mais as pessoas dependem dos meios de comunicação para o trato diário das relações pessoais e profissionais.

De forma bem sucinta temos que distinguir violação das comunicações telefônicas de quebra de sigilo de registro de dados. Sendo que o primeiro corresponde a interceptação das comunicações propriamente dita, consiste na captação da conversa alheia e corre em tempo real por meio de interceptações como escuta e gravações. Já a quebra de sigilo dos registros de dados telefônicos corresponde à obtenção de registros existentes na companhia telefônica sobre ligações já realizadas, dados cadastrais do assinante, data da chamada, horário, número de telefone chamado, duração do uso e outros dados.

A interceptação ilegal tanto em dados telefônicos quanto em dados telemático acontecem sem a permissão da vítima e sem ordem judicial, ou seja, não obedece os requisitos legais, infringindo um direito fundamental tutelado pela Constituição Federal.

#### 3.1.1.1 DO MARCO CIVIL DA *INTERNET* X CRIMES VIRTUAIS

Em 2014 foi instituída a Lei n. 12.965 conhecida como Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da internet, porém, a lei não tipificou crimes, a lei se limitou a regulamentação e responsabilização civil, enfatizando a privacidade das informações digitais. Os dispositivos trazem, ainda, a regulamentação do armazenamento de dados realizado pelos provedores, fixando conceitos importantes relativos a internet.

O Marco Civil da internet traz a complementação para as leis de crimes virtuais e representa um grande avanço para o direito digital (BRASIL, 2014). O artigo 3º da referida lei estabelece como princípios a liberdade de expressão, a proteção da privacidade e a proteção dos dados pessoais (necessitando de regulamentação de como se dará essa proteção):

Art. 3º A disciplina do uso da *internet* no Brasil tem os seguintes princípios: I- garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II- proteção da privacidade; III- proteção dos dados pessoais, na forma da lei (BRASIL, 2014).

Já o artigo 5º da Lei n. 12.965/2014 traz em seu bojo os conceitos relacionados a internet como registro de log de conexão e aplicação de internet, endereço de protocolo de internet, conhecido como IP, terminal, internet dentre outros, dessa forma, a comunicação do mundo jurídico com os provedores e administradores de redes ficam mais alinhadas.

A lei conceitua *internet* como o sistema constituído por um “conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes” (inciso I). O conceito comum descreve que internet é um sistema global de redes de computadores interligadas que utilizam um conjunto próprio de protocolos (**Internet** Protocol Suite ou TCP/IP) com o propósito de servir progressivamente usuários no mundo inteiro.

A rede de internet é interligada a um “terminal denomina computador ou qualquer dispositivo que se conecte à *internet*” (inciso II) e o acesso é realizado por meio de endereço de protocolo de internet (endereço de IP), que é o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais (inciso II da Lei n. 12.965/2014).

A Lei 12.965/2014 menciona em seu inciso IV sobre como acontece a administração do sistema autônomo de internet, na qual “a pessoa física ou jurídica administra blocos de endereço IP específicos e o respectivo sistema autônomo de

roteamento, devidamente cadastrado no ente nacional”. Sendo que para se conectar o usuário deverá ‘possuir a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço de IP (inciso V da Lei 12.965/2014).

De acordo com o inciso VI do Marco Inicial da Internet, o conjunto de informações referentes à data e hora de início e término de uma conexão à *internet*, sua duração e o IP utilizado pelo terminal para o envio e recebimentos de pacotes de dados ficam registrados em todas as conexões. O inciso VII e VIII descrevem sobre as aplicações de internet que compreendem o conjunto de funcionalidades que podem ser acessados por meio de um terminal conectado a internet, que registra todos os cessos de aplicações da internet.

A Lei também trouxe avanços no que se refere a proteção de dados pessoais, o objetivo é evitar o compartilhamento de dados, facilitando o uso de mala direta, ou melhor, spam, impondo ao provedor a obrigação de guardar os dados e determinando que sua disponibilidade aconteça somente com a ordem judicial, sob pena de responsabilização civil em caso de violação (INFORMÁTICA TERRA, 2015, p. 1).

Sobre a proteção dos dados a Lei 12.965/2014 expressa que:

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de *internet* de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

A legislação é bem enfática ao determinar que o provedor é responsável pela guarda dos dados e que a empresa somente será obrigada a disponibilizar os registros guardados mediante ordem judicial, é o que preconiza o § 1º e 2º do art. 10, da Lei 12.965/2014. A lei não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação endereço, desde que seja requisitados pelas autoridades administrativas que detenham a competência para a solicitação, assim define o § 3º da lei.

A Lei fixa regras aplicadas ao processo penal dos crimes informáticos, o que facilita sua apuração, representando mais um aliado no combate aos crimes virtuais. Dentre as regras a mais importante está relacionada com o registro de log por parte dos provedores de serviços de internet, impondo a esses o dever de manter os registros de log pelo prazo de 1 (um) ano para as conexões e de 6 (seis) meses para as aplicações de internet (MAGGIO, 2015).

Estabelecendo ainda, que esses registros poderão ser guardados cautelarmente por prazo superior ao fixado, por meio de determinação da autoridade competente, observado o

prazo de 60 dias para ingressar com pedido de autorização judicial de acesso aos registros de log, conforme arts. 13 e 15 da Lei n. 12.965/2014:

Apesar da relevância de responsabilização penal dos administradores de redes ou de servidores de serviços internet, a legislação penal brasileira não tipifica punições específicas relacionadas aos provedores de internet. O marco civil da internet trouxe a responsabilização civil nos casos de danos decorrentes de conteúdo gerados por terceiros, tendo sua aplicação condicionada a ordem judicial (Arts. 18, 19, 20, 21 da Lei 12.965/2014).

Apesar de a lei n. 12.965/2014 ser voltada para a regulamentação e responsabilização civil, o Marco Civil da Internet representa um importante aliado no combate aos crimes virtuais, se tornou um avanço para o direito digital com penas que abrangem responsabilização penal, inclusive com possibilidade de reclusão.

#### 4.1 A INTERCEPTAÇÃO POR MEIO DE APLICATIVOS DE MENSAGEM

A interceptação telefônica tradicional não possui, atualmente, a mesma eficiência que costumava ter como meio de obtenção de prova, pois, hoje há uma expansão muito grande das redes de comunicação de dados e da internet. O crescente número de outras formas de comunicação como redes sociais e aplicativos de mensagens está tornando a vocalização intercomunicativa cada vez mais escassa na era pós internet.

A mitigação do sistema convencional de comunicação para o modelo globalizado de interconexão coloca em xeque a obtenção de provas por meio da interceptação telefônica. Nesta senda, os aplicativos de envio e recepção de mensagens, áudios e vídeos whatsapp, telegrama e outros, são de comunicação de natureza privada, com proteção ponta a ponta restrita aos interlocutores ou grupo limitado de pessoas se equiparam a informações por meio telemático.

Como já foi citado, a Lei n. 12.965 de 23 de abril de 2014, Marco Civil da Internet determina o sigilo das comunicações por meio de informática, sendo este inviolável. Porém, os dados cadastrais dos usuários, bem como o acesso aos provedores de aplicação de internet podem ser requisitados por determinação judicial.

Apesar de o acesso aos dados cadastrais serem previstos pelo seu parágrafo 3º do artigo 10 da Lei nº. 12.965/2014 é bem comum o desrespeito das empresas detentoras dos direitos de aplicativos de mensagens. Um dos fatores que levam ao desrespeito é a falta de especificidade sobre a matéria, principalmente em relação a interceptação de aplicativos de celular, o embate sobre o assunto chegou até o Supremo Tribunal Federal, que na ocasião emitiu decisão pelo

bloqueio temporário do aplicativo whatsapp pelo fato de a empresa não colaborar com as investigações.

O certo é que tanto a Lei nº 9.296, de 24 de Julho de 1996 (Lei da Interceptação Telefônica) quanto a Lei nº 12.965, de 23 de Abril de 2014 (Marco Civil da Internet), no que se refere ao acesso de dados e trocas de mensagens por aplicativos de celular como meio e obtenção de prova pouco inovaram sobre o tema abordado nesse artigo.

Na prática, o que se observa são decisões em que mensagens de textos, imagens e arquivos em geral são obtidos durante a busca e apreensão ou ainda durante a prisão em flagrante do agente investigado. No entanto, a extração de dados não é abarcada pela lei 9.296/1996, uma vez que o acesso as informações não ocorrem no momento da conversação.

Por outro lado, Lei nº 12.965/2014 traz a necessidade da proteção dos dados pessoais produzidos pelo uso da internet incluindo os dados armazenados no celular como as mensagens privadas mídias sociais (WhatsApp, Messenger, Telegram, etc.), sendo estes aplicativos passíveis de acesso mediante ordem judicial.

#### **4.1.1 Interceptação de aplicativos de mensagens: uma visão prática do STJ**

O entendimento do STJ é de que o exame pericial realizado em aparelhos de telefone celular diretamente após a apreensão pela polícia, sem prévia autorização judicial viola os direitos e garantias fundamentais do acusado (REsp 1.727.266/SC, j. 05/06/2018). A autoridade policial poderá examinar o aparelho, obter dados e mensagens armazenadas, mas somente após a devida autorização do juiz.

Diversas formas de comunicação trazidas pela tecnologia em proporcionadas situações inusitadas que escapam ao sistema legal de produção de provas. Um caso interessante foi envolvendo o aplicativo de mensagens Whatsapp foi parar no STJ ao qual decidiu que a prova foi obtida de forma ilícita. Ocorre que as autoridades policiais estavam fazendo uma investigação sobre tráfico de drogas, o delegado requereu ao Juiz a autorização para apreender o celular do suspeito Após a apreensão do celular e de posse do instrumento o Delegado de Polícia requereu ao Juiz a interceptação telefônica e telemática do celular apreendido o qual fora deferido.

No entanto, o whatsapp possui criptografia de ponta a ponta que protege o teor das mensagens, então as autoridades policiais decidiram espelhar o aplicativo com o recurso para *web*, abrir o aplicativo de mensagens no computador, manter conectado e devolver o celular ao suspeito com a indagação de que não fora encontrado nada suspeito no aparelho.

A partir disso as mensagens trocadas entre o proprietário do aparelho e outras pessoas passaram a ser monitoradas pela autoridade policial até conseguirem a informação das quais colocava o suspeito na cena do tráfico de drogas. O caso chegou ao Superior Tribunal de Justiça que decidiu pela impossibilidade da analogia entre a lei de interceptação telefônica e o espelhamento de conversas pelo whatsapp.

Ao proferir a decisão o STJ se utilizou dos seguintes argumentos *in verbis*:

(a) Ao contrário da interceptação telefônica, no âmbito da qual o investigador de polícia atua como mero observador de conversas empreendidas por terceiros, no espelhamento via Whatsapp Web o investigador de polícia tem a concreta possibilidade de atuar como participante das conversas que vem a ser realizadas quanto das conversas que já estão registradas no aparelho celular, haja vista ter o poder conferido pela própria plataforma online, de interagir nos diálogos mediante envio de novas mensagens a qualquer contato presente no celular e exclusão, com total liberdade, e sem deixar vestígios, de qualquer mensagem passada, presente ou, se for o caso, futura. (b) ao contrário da interceptação telefônica, que tem como objeto a escuta de conversas realizadas apenas depois da autorização judicial (ex-nunc), o espelhamento via Código QR viabiliza ao investigador o acesso amplo e irrestrito a toda e qualquer comunicação realizada antes da mencionada autorização, operando efeitos retroativos (ex-tunc). (c) ao contrário da interceptação telefônica, que é operacionalizada sem a necessidade simultânea de busca pessoal ou domiciliar para a apreensão de aparelho telefônico, o espelhamento via Código QR depende da abordagem do indivíduo ou do vasculhamento de sua residência, com apreensão de seu aparelho telefônico por breve período de tempo e posterior devolução desacompanhada de qualquer menção, por parte da autoridade policial, a realização da medida constritiva, ou mesmo, porventura, embora não haja nos autos notícia de que isso tenha ocorrido no caso concreto, acompanhada de afirmação falsa de que nada foi feito (RHC 99.735/SC, Rel. Ministra LAURITA VAZ, SEXTA TURMA, julgado em 27/11/2018, DJe 12/12/2018)

Portanto, a Sexta Turma concluiu que é inaplicável a analogia entre interceptação telefônica e espelhamento, por meio do WhatsApp Web, das conversas realizadas pelo aplicativo WhatsApp.

## 5 METODOLOGIA

A metodologia utilizada no presente artigo permitiu conhecer e aprofundar nos objetivos a que se propôs a pesquisa, que foi o de realizar um estudo acerca das legislações voltadas para a interceptação telefônica após o advento da internet, ressaltando sobre a interceptação ilegal

de dados e, por conseguinte, a interceptação telemática que após a era digital forma um conjunto de dados presentes no telefone que acaba fazendo parte do pacote quando há uma quebra de sigilo ou interceptação.

É importante traçar o percurso a percorrer em uma pesquisa, pois a sistematização dos dados é uma forma de pensar para se chegar à natureza de um determinado problema, seja para explicá-lo ou estudá-lo (KAHLMEYER-MERTENS et al., 2007. p. 15). Assim, as etapas utilizadas na investigação sobre a temática compreendem, primeiramente, no levantamento de dados por meio dos instrumentos de pesquisas como legislações, doutrinas, publicações, atualizações de leis, jurisprudências, resoluções do CNJ e outras fontes capazes de traduzir o entendimento sobre a interceptação.

A investigação se pautou no método hipotético-dedutivo, um modelo de pesquisa que se resume a análise da legislação brasileira, extraindo as hipóteses de condutas concretas e abstratas que permitem deduzir possíveis tipificações de crimes que ocorrem ao utilizar a interceptação, quebra de sigilo ou o uso indiscriminado da internet.

Para fundamentar a pesquisa foi necessário entender o conceito de interceptação telefônica, quebra de sigilo telefônico, interceptação de dados e ainda os conceitos básicos de tecnologia da informação e sua utilização indiscriminada pelos usuários. O levantamento bibliográfico sobre o tema traz a sustentação do assunto a ser abordado. “A pesquisa bibliográfica tem por finalidade conhecer as diferentes formas de contribuição científica que se realizaram sobre determinado assunto ou fenômeno” (JUNG, 2003, p. 128).

## **CONSIDERAÇÕES FINAIS**

O direito a intimidade e o sigilo das comunicações telefônicas, dentre outros, estão previstos nos direitos fundamentais da Constituição Federal, inclusive o ordenamento jurídico traz esse direito como uma cláusula pétrea. No entanto, a interceptação telefônica tem sido essencial como fonte de prova, desde que seja realizada conforme os requisitos previstos em lei, pois somente assim poderá ser aceita como prova lícita e tendo o resultado como fonte de prova no processo.

Porém, de acordo com os estudos pudemos perceber que nem todos os preceitos foram abarcados pela Lei 9.296/96, restando a interpretação das lacunas aos tribunais superiores. O artigo buscou compreender o advento da internet e os reflexos do progresso digital na interceptação telefônica e telemática, demonstrando que a legislação ainda apresenta a

necessidade de lei específica que alcance a quebra do sigilo de dados em aplicativos de mensagens.

Durante a investigação notou-se que a interceptação telefônica tradicional já não possui mais a mesma eficácia quanto aos meios de obtenção de prova, nem possui mais a mesma eficiência que costumava ter antes da expansão da era digital e o avanço da comunicação em redes. É notório que a telefonia fixa móvel perdeu bastante espaço para os aplicativos de mensagens instantâneas, que possuem maior privacidade, rapidez, qualidade e segurança com menor custo para o usuário.

Essa mitigação da telefonia por voz e a expansão de aplicativos de mensagens e outros meios de comunicação ocasionou o surgimento da Lei 12.965/2014, conhecida como Marco Civil da Internet que trata expressamente da necessidade de proteção dos dados pessoais produzidos pelo uso da internet, incluindo as mensagens privados em mídias sociais (WhatsApp, Messenger, Telegram, etc.), que somente podem ser acessadas com autorização judicial.

Ante o exposto, percebe-se que o legislador tem dificuldades em acompanhar o progresso tecnológico e o modelo globalizado de interconexão, fragilizando, dessa forma, os órgãos de segurança quanto a obtenção de provas quando o assunto é interceptação telefônica, telemática e extração de dados. A dificuldade se concentra por ser institutos que estão em constante transformação, que requer do legislador um acompanhamento mais rápido do progresso da internet.

Enquanto isso não acontecer, o sistema jurídico brasileiro terá conflitos para legislar sobre a quebra de sigilo e privacidade nas comunicações entre os usuários de aplicativos de mensagens instantâneas.

## REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm) . Acesso em: 16/08/2020.

BRASIL. Código Penal Brasileiro. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/decreto-lei/del2848compilado.htm](http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm) Acesso em: 16/08/2020.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Brasília: Presidência da República, 2012. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/LEIS/L9296.htm](http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm). Acesso: 20/08/2020.

BRASIL. Conselho Nacional de Justiça. **Resolução n. 59/2008 de 9 de agosto de 2008**. Trata das rotinas dos procedimentos de interceptação de comunicação telefônica, de informática e telemática utilizados pelo Poder Judiciário nas investigações criminais, com base na Lei n. 9.296/1996. Brasília: CNJ, 2008. Disponível em: <http://www.cnj.jus.br/noticias/cnj/81544-cnj-altera-resolucao-sobre-interceptacoes-judiciais>. Acesso: 20/08/2020.

BRASIL. Lei Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2012. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso: 25/08/2020.

BRASIL. Lei nº 8.069/90, Estatuto da Criança e do Adolescente. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l8069.htm](http://www.planalto.gov.br/ccivil_03/leis/l8069.htm) Acesso: 25/08/2020.

BRASIL. Lei nº 9.279/96. Regula direitos e obrigações relativos à propriedade industrial. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/Leis/L9279.htm](http://www.planalto.gov.br/ccivil_03/Leis/L9279.htm) Acesso: 25/08/2020.

BRASIL. Lei nº 9.609/98. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l9609.htm](http://www.planalto.gov.br/ccivil_03/leis/l9609.htm) Acesso: 25/08/2020.

CARNEIRO, Adenele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. In: Âmbito Jurídico, Rio Grande, XV, n. 99, abr 2012. Disponível em: <[http://www.ambito-juridico.com.br/site/?n\\_link=revista\\_artigos\\_leitura&artigo\\_id=11529](http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529)>. Acesso: 25/08/2020.

CORREIA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 5ed. São Paulo: Saraiva, 2010.

INFORMÁTICA TERRA. O que é Spam. Informática Terra, cit.176. Disponível em: <<http://www.spam.com>>. Acesso: 25/08/2020.

JUNG, C.F. Metodologia científica. Ênfase em pesquisa tecnológica. Taquara: UFSM, 2003. Disponível em: <http://www.jung.pro.br>. Acesso: 25/08/2020.

KUNRATH, Josefa Cristina Tomaz Martins. A expansão da criminalidade no cyberspaço. UEFS, 2017.

LEMOS, André. **As estruturas antropológicas do ciberespaço**. Salvador: texto produzido para os seminários do grupo Cyberpesquisa/Facom-UFBA, 1996, p.1 Disponível em: <http://www.facom.ufba.br/ciberpesquisa> Acesso em: 20/08/2020.

LEMOS. **Cibercultura**: entrevista [2003]. Disponível em: <http://informática.terra.com.br> Acesso em: 16/08/2020.

MAGGIO, Vicente de Paula Rodrigues. Novo crime: invasão de dispositivo informático - CP, Art. 154-A. Ciências Humanas e Sociais Unit. Aracaju. v. 2. n. 3. p. 215-236. 22 Março 2015. Disponível em: <http://vicentemaggio.jusbrasil.com.br/artigos/121942478/novo-crime-invasao-de-dispositivo-informatico-cp-art-154-a>. Acesso: 25/08/2020.

LIBERATI, Maria José Crepaldi Ganância. Crimes informáticos. Campinas: PUC, 2011.

PERON, André; DEUS, Flávio Elias Gomes de; SOUSA JUNIOR, Rafael Timóteo. Ferramentas e metodologia para simplificar as investigações criminais utilizando interceptação telemática . Brasília: UnB, 2011

ROVER, Aires José (Org.). Direito e informática. Barueri: Manole, 2004.

SCHMIDLIN FILHO, Carlos. Redes Sociais e o Tratamento Jurídico Brasileiro. Publicado em 09 de out de 2016. Disponível em: <http://www.betoschimidlin.jusbrasil.com.br/artigos/180346661/redes-sociais-e-o-tratamento-juridico-brasileiro>. Acesso: 09/09/2020.

VAZ, Laurita. RHC 99.735/SC, Rel. Ministra LAURITA VAZ, SEXTA TURMA, julgado em 27/11/2018, DJe 12/12/2018. Disponível em: <https://canalcienciascriminais.com.br/espelhamento-de-conversas-no-whatsapp/> Acesso: 24/09/2020



