UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS
GRADUAÇÃO EM DIREITO

THIAGO FERREIRA DOS SANTOS

SIGILO DE DADOS, INTERCEPTAÇÃO TELEMÁTICA E DIREITO FUNDAMENTAL À PROVA: UM OLHAR SOBRE O HACKEAMENTO DE DISPOSITIVOS INFORMÁTICOS NA OPERAÇÃO *SPOOFING*

Cidade de Goiás
2021

UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO NO REPOSITÓRIO INSTITUCIONAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio do Repositório Institucional (RI/UFG), regulamentado pela Resolução CEPEC no 1240/2014, sem ressarcimento dos direitos autorais, de acordo com a Lei no 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo dos Trabalhos de Conclusão dos Cursos de Graduação disponibilizado no RI/UFG é de responsabilidade exclusiva dos autores. Ao encaminhar(em) o produto final, o(s) autor(a)(es)(as) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do Trabalho de Conclusão de Curso de Graduação (TCCG)

Nome(s) completo(s) do(a)(s) autor(a)(es)(as): THIAGO FERREIRA DOS SANTOS

Título do trabalho: SIGILO DE DADOS, INTERCEPTAÇÃO TELEMÁTICA E DIREITO FUNDAMENTAL À PROVA: UM OLHAR SOBRE O HACKEAMENTO DE DISPOSITIVOS INFORMÁTICOS NA OPERAÇÃO *SPOOFING*

2. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador) Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante: a) consulta ao(à)(s) autor(a)(es)(as) e ao(à) orientador(a); b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo do TCCG. O documento não será disponibilizado durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;

- Submissão de artigo em revista científica;

- Publicação como capítulo de livro.

Obs.: Este termo deve ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Bruna Pinotti Garcia Oliveira**, **Professora do Magistério Superior**, em 19/06/2021, às 15:52, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **THIAGO FERREIRA DOS SANTOS**, **Usuário Externo**, em 19/06/2021, às 17:09, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Referência: Processo nº 23070.025892/2021-66 SEI nº 2148239

THIAGO FERREIRA DOS SANTOS

SIGILO DE DADOS, INTERCEPTAÇÃO TELEMÁTICA E DIREITO FUNDAMENTAL À PROVA: UM OLHAR SOBRE O HACKEAMENTO DE DISPOSITIVOS INFORMÁTICOS NA OPERAÇÃO *SPOOFING*

Monografia jurídica apresentada à Unidade Acadêmica Especial de Ciências Sociais Aplicadas da Regional Goiás da Universidade Federal de Goiás, como trabalho de conclusão do curso de bacharelado em direito, sob a orientação da Profa. Dra. Bruna Pinotti Garcia Oliveira.

Cidade de Goiás
2021

Dados Internacionais de Catalogação na Publicação (CIP)

Santos, Thiago Ferreira dos

SIGILO DE DADOS, INTERCEPTAÇÃO TELEMÁTICA E DIREITO FUNDAMENTAL À PROVA: UM OLHAR SOBRE O HACKEAMENTO DE DISPOSITIVOS INFORMÁTICOS NA OPERAÇÃO *SPOOFING*. Thiago Ferreira dos Santos – 2021.

Orientação: Profa. Dra. Bruna Pinotti Garcia Oliveira.

Monografia (Graduação em Direito) – Universidade Federal de Goiás, Unidade Acadêmica Especial de Ciências Sociais Aplicadas, Goiás, 2021.

1. Direito Constitucional. 2. Direito Processual Penal. 3. Direito digital. 4. Interceptação telemática. 5. *Spoofing*.

CDU 343.211.3

UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Aos 10 dias do mês de junho do ano de 2021 iniciou-se a sessão pública de defesa do Trabalho de Conclusão de Curso (TCC) intitulado "SIGILO DE DADOS, INTERCEPTAÇÃO TELEMÁTICA E DIREITO FUNDAMENTAL À PROVA: UM OLHAR SOBRE O HACKEAMENTO DE DISPOSITIVOS INFORMÁTICOS NA OPERAÇÃO *SPOOFING*", de autoria de THIAGO FERREIRA DOS SANTOS, do curso de Direito, da Unidade Acadêmica Especial de Ciências Sociais Aplicadas da UFG. Os trabalhos foram instalados pela Profa. Dra. Bruna Pinotti Garcia Oliveira (UAECSA/UFG) – orientadora com a participação dos demais membros da Banca Examinadora: Prof. Dr. José do Carmo Alves Siqueira e Profa. Ma. Renata Botelho Dutra. Após a apresentação, a banca examinadora realizou a arguição do estudante. Posteriormente, de forma reservada, a Banca Examinadora deliberou, tendo sido o TCC considerado **aprovado**.

Proclamados os resultados, os trabalhos foram encerrados e, para constar, lavrou-se a presente ata que segue assinada pelos Membros da Banca Examinadora.

Documento assinado eletronicamente por **Bruna Pinotti Garcia Oliveira**, **Professora do Magistério Superior**, em 19/06/2021, às 16:15, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **José Do Carmo Alves Siqueira**, **Professor do Magistério Superior**, em 19/06/2021, às 16:17, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Renata Botelho Dutra**, **Professora do Magistério Superior**, em 19/06/2021, às 17:50, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2148238** e o código CRC **35445618**.

Referência: Processo nº 23070.025892/2021-66 SEI nº 2148238

Dedico este trabalho à minha família e amigos, os poucos.

AGRADECIMENTOS

Escrever uma monografia jurídica não é tarefa fácil; se for voltada à área de tecnologia, mais complexo ainda, dada à volatilidade e a sua rápida expansão; agora, escrever uma obra em que se concatena o conhecimento jurídico aliado à tecnologia é extremamente penoso.

Penso que este material não deveria ser uma monografia, visto que não foi escrito apenas por mim, como já dito, motivo pelo qual me socorri a grandes mentes e experiências, notadamente do saber jurídico.

A todas as pessoas que me incentivaram, que puderam ler, criticar, e sugerir mudanças e/ou melhorias, por menores que foram, só me resta concluir o seguinte: agradecer é um ato simples, basilar e que é entendido como sendo nobre, por se revestir de humildade. Todavia, em que pese ser simples não significa, necessariamente, que é fácil – não pelo autor ser vaidoso ou presunçoso – mas sim porque corre-se o risco de esquecer alguém que contribuiu, direta ou indiretamente, com os resultados.

Tentarei ser o mais detalhado possível e se alguém que ler este trabalho e seu nome não estiver aqui, perdoe-me pelo esquecimento.

Aos meus pais amados, Maria Aparecida Ferreira dos Santos e Luiz Ferreira dos Santos, por, simplesmente, tudo. Não há palavras para descrever o que sinto pelos senhores terem lutado para que eu me tornasse a pessoa que sou hoje.

À minha esposa, Ana Luíza Cruvinel, por ser a companheira que é, por estar ao meu lado – ainda que nos meus momentos de crises de humor e estresse – principalmente no momento de produção desta obra.

Ao meu amigo 1º Tenente Policial Militar Erivaldo Soares, da Agência Central de Inteligência da Polícia Militar de Goiás, que sempre acreditou e investiu em mim, como ser humano, como profissional, como estudante, e onde soube visualizar e instigar aquela chama da Inteligência. Se estou onde estou hoje, acadêmica e profissionalmente, devo a você. Saiba que os aprendizados por você ensinados me moldaram como a pessoa que sou hoje. É um exemplo de profissional e humano que está em falta hoje em dia: honesto, humilde e que não esquece as origens.

Ao major Policial Militar, Daniel Machado, gerente de operações de Inteligência da Coordenadoria de Segurança Institucional e Inteligência do Ministério Público de Goiás, pelo apoio, orientações e dicas para a produção desta obra.

Ao Dr. Rodney da Silva, promotor de Justiça, coordenador da CSI – Coordenadoria de Segurança Institucional e Inteligência do Ministério Público do Estado de Goiás, por realizar o excelente trabalho à frente deste mister, conduzindo a todos os servidores com sabedoria, integridade e honestidade. Além de ser um ícone e uma pessoa extremamente gabaritada quando o assunto é investigação e inteligência, abriu-me as portas do Núcleo Especial de Inteligência Cibernética, para que eu pudesse exercer minhas atribuições com muita garra.

Ao Dr. Luiz Carlos Wolff de Pina, Promotor de Justiça, subcoordenador da CSI, que é um profissional humilde e sempre nos apoia no serviço diário. Obrigado, ainda, pelo livro de questões jurídicas a que fui presenteado, e por sempre me apoiar nos estudos sobre o direito.

Ao Filipe da Silva Coutinho, gerente do Núcleo Especial de Inteligência Cibernética, servidor extremamente batráquia, dedicada, por ter me aceitado na Cyber, acreditado e investigado em mim. Esta obra não teria sido realizada sem seus ensinamentos acerca da telemática, como um todo.

Ao Dr. Kleyton de Oliveira Alencar, delegado de polícia civil e gerente do Laboratório de Lavagem de Capitais, da CSI, por ter disposto de seu escasso tempo, no final de semana, para analisar esta obra e sugerir melhorias cirúrgicas conforme sua experiência investigativa.

A Adriana Shimabukuro, do Ministério Público Federal, de São Paulo, especialista em investigação cibernética, que, com grande atenção e dispôs de seu tempo para ajudar na produção desta obra, além de sempre estar à disposição para esclarecimentos de dúvidas quanto ao desenrolar do serviço.

Ao major do Exército Brasileiro, Eder Luís Oliveira Gonçalves (certificado em CISSP, C|EH, C|HFI, ECSA, CEI, CSCU, OSCP, OSWP, ACE, *Leader Assessor* 27001, GCFA e GPEN) por sempre me ajudar com soluções de problemas no que concernem ao hacking, forense e investigação cibernética.

A minha orientadora, Prof. Dra. Bruna Pinotti, pelo acompanhamento, orientação e apoio para que esta obra pudesse ser concretizada.

“Se vi mais longe foi por estar de pé sobre ombros de gigantes”.
(Isaac Newton)

LISTA DE SIGLAS E ABREVIATURAS

ABIN Agência Brasileira de Inteligência

APCF Associação Nacional dos Peritos Criminais

ADI Ação Direta de Inconstitucionalidade

CEJIL Centro para a Justiça e o Direito Internacional

CIDH Comissão Interamericana de Direitos Humanos

CNJ Conselho Nacional de Justiça

COAF Conselho de Controle de Atividades Financeiras

CP Código Penal

CPC Código de Processo Civil

CPP Código de Processo Penal

CF Constituição Federal

DoS *Denial of Service* (ataque de negação de serviço)

DDoS *Distributed Denial of Service* (ataque de negação de serviço distribuído)

LGDP Lei geral de Proteção de Dados

GTI Grupo de Trabalho Interministerial

IP *Internet Protocol*

MCI Marco Civil da Internet

NAT *Network Address Translation*

STF Supremo Tribunal Federal

STJ Superior Tribunal de Justiça

TCP/IP *Transfer Control Protocol/Internet Protocol*

RESUMO

Este trabalho busca analisar o contexto das interceptações telemáticas em termos normativos e práticos, tomando como parâmetro recentes discussões acerca da Operação Spoofing. Inicia-se com o estudo do sigilo de dados e da interceptação telemática no sistema jurídico brasileiro. Adiante, aborda a investigação de crimes em meios tecnológicos e os procedimentos para requisição de dados informáticos adotados usados pelas polícias judiciárias e pelos Ministérios Públicos. Por fim, faz um estudo de caso acerca da Operação Spoofing, analisando a consecução de provas por meio de hackeamento de dispositivos informáticos e a possibilidade ou não de validação das provas conseguidas por meios fraudulentos por parte das defesas. O trabalho se desenvolve pelo método analítico-doutrinário, colacionando doutrina especializada com documentos oficiais, sendo amparado por procedimentos técnicos bibliográfico e documental. Ao final, conclui-se que o direito de defesa não pode ser limitado pela forma como se obtém a prova consubstanciada em dado telemático, havendo prevalência da presunção de inocência sobre a vedação às provas ilícitas.

Palavras-chave: Direito Constitucional. Direito Processual Penal. Direito digital. Interceptação telemática. Operação *Spoofing*.

ABSTRACT

This paper seeks to analyze the context of telematic interceptions in normative and practical terms, taking as a parameter recent discussions about Operation Spoofing. It begins with the study of data confidentiality and telematic interception in the Brazilian legal system. Ahead, it addresses the investigation of crimes in technological means and the procedures for requisition of computer data adopted by the judicial police and the prosecution. Finally, it makes a case study about Operation Spoofing, analyzing the achievement of evidence through hacking of computer devices and the possibility or not of validating the evidence obtained by fraudulent means by the defenses. The work is developed by the analytical-doctrinal method, collecting specialized doctrine with official documents, being supported by bibliographic and documentary technical procedures. In the end, it is concluded that the right of defense cannot be limited by the way in which the evidence embodied in a telematic data is obtained, with the presumption of innocence prevailing over the prohibition against illicit evidence.

Keywords: Constitutional Law. Criminal Procedural Law. Digital law. Telematic interception. Spoofing operation.

SUMÁRIO

INTRODUÇÃO

Uma das principais realizações do homem foi o desenvolvimento da inteligência que se materializou, aos poucos e muito lentamente, na aptidão em realizar tarefas rotineiras, dentre as quais, a fundamental: a capacidade de interagir-se e a de comunicar-se com outros de mesma espécie. Essas aptidões não ficaram apenas em verbalizar ou exteriorizar alguma sílaba ou gesto, mas também a escrita e desenho de sinais.

Muito tempo se passou e, obviamente, tudo se desenvolveu. A capacidade de comunicação e interação social, seja por meio verbal ou sensorial, se especializou. O modo de comunicação que, antigamente, era utilizado em forma de escritas em pedras rupestres ou no interior de cavernas, hoje se dá por meio de bits[1], impulsos magnéticos e altas taxas de transmissões de dados de um lado para o outro em um curtíssimo intervalo de tempo.

O uso da comunicação evoluída, tecnológica, não faz do homem apenas um ser que se comunica rápida e sabidamente com outro par, por exemplo; muito pelo contrário, o faz mais forte em relação a outro e, sendo assim, há violações de direito entre eles. Aqui, nascem as violações materiais de direitos de uma ou mais pessoas.

Atualmente, os meios tecnológicos de comunicação trazem infindáveis benefícios e, de igual forma, prejuízos, dada a maneira de utilização para práticas delitivas e, em relação a essas práticas, é oportuno trazer à tona a previsão legal quando o assunto é comunicações de dados e o cometimento de crimes.

Quando se fala em comunicação de dados é necessário fazer remissão sobre o que a Constituição Federal fala do assunto, em seu art. 5º, XII. Além da Carta Política verifica-se proteção legal acerca de sigilo de dados e seu respectivo afastamento em outras leis, a exemplo, a Lei n. 9.296/96 (interceptação telefônica), Lei n. 12.850/13 (Organização Criminosa), Lei n. 9.613/96 (Lavagem de Capitais), Lei n. 12965/14 (Marco Civil da Internet), dentre outras.

A investigação brasileira, como um todo, seja por parte da polícia judiciária, seja pelo Ministério Público, diuturnamente demandam o Poder Judiciário no que tange à quebra de dados (ou ao afastamento de sigilo) telemáticos em desfavor de seus investigados, com o fito de angariar provas para levar a uma condenação. Todavia, há percalços de ordem legislativa, jurídica e tecnológica entre uma investigação e outra.

O primeiro dos percalços é que com a evolução da tecnologia e sua maciça ofertas de

[1] Bit (*Binary digit):* é a menor unidade de informação que pode ser armazenada ou transmitida e que pode assumir somente dois valores: 0 ou 1, verdadeiro ou falso e assim por diante. Nomenclaturas serão demonstradas em capítulo próprio.

serviços de armazenamento, redes sociais etc., muitos dos quais na qualidade “for free”, ou seja, gratuitos, levam a uma grande quantidade de pessoas que se cadastram nestas tecnologias, por exemplo, Google (e todos os seus serviços), Microsoft (e seus diversos serviços), Uber, WhatsApp. Entretanto, estas empresas são tidas como provedores de aplicação e isso significa que elas ofertam seus serviços diretamente ao usuário-fim, que tecnicamente falando operam na Camada de aplicação da pilha TCP/IP. Esses provedores de aplicação situam-se, quase na totalidade, em outros países que são regidos por suas leis locais e não as brasileiras.

O problema sobre a ordem legislativa é que as leis brasileiras são frágeis quando o assunto é o fornecimento de dados telemáticos por parte de provedores de aplicação e não lhes trazem consequências graves, na ordem cível, penal e/ou administrativa, caso não cumpram uma ordem judicial, ou o fazem de maneira deficitária.

Neste contexto, o objetivo geral do trabalho é refletir sobre as repercussões dos meios lícitos e ilícitos de obtenção de dados telemáticos, os quais podem impactar diretamente na prova para fins processuais penais. Para tanto, a monografia está dividida em três capítulos, sendo que: no capítulo 1, o leitor é levado a ter uma noção sobre sigilo de dados e a interceptação telemática no sistema jurídico brasileiro e suas principais leis em uso; no capítulo 2, será falado sobre a investigação de crimes em meios tecnológicos e seus procedimentos para requisição de dados informáticos, com demonstração de alguns procedimentos usados pelas polícias judiciárias e pelos Ministérios Públicos para requisição de dados e as barreiras encontradas neste intuito; por fim, no capítulo 3, será realizado um estudo de caso acerca da Operação Spoofing, analisando a consecução de provas por meio de hackeamento de dispositivos informáticos e, também, a possibilidade ou não de validação das provas conseguidas por meios fraudulentos por parte das defesas.

O trabalho se desenvolverá pelo método hipotético-dedutivo, colacionando doutrina especializada com documentos oficiais, sendo assim amparado por procedimentos técnicos bibliográfico e documental. Busca-se responder aos seguintes problemas de pesquisa: o direito de defesa pode ser limitado diante da obtenção de dados telemáticos por vias transversas, como o hackeamento de dispositivo informático? Fixa-se, como hipótese, a de que o direito de defesa não pode ser limitado pela origem da prova consubstanciada em dado telemático, havendo prevalência da presunção de inocência sobre a vedação às provas ilícitas.

CAPÍTULO 1 – SIGILO DE DADOS E INTERCEPTAÇÃO TELEMÁTICA NO SISTEMA JURÍDICO BRASILEIRO

Por muitos anos o uso da interceptação telefônica foi tido como uma das melhores técnicas de investigação pelo fato de que diversas pessoas se comunicavam diariamente via aparelhos telefônicos, especialmente os celulares, dada a facilidade de transporte, ou seja, portabilidade etc.

A interceptação telefônica possui lei específica própria que trata do assunto: Lei n. 9.296/96, lei pequena que passou alguns revezes até a sua publicação e entrada em vigor. Várias pessoas tinham o sigilo de seus dados telefônicos afastados pela Justiça brasileira e muitas das provas obtidas terminavam em condenações.

O tempo passou e a tecnologia se fez mais presente, e o uso da comunicação telefônica cedeu espaço para os smartphones, aparelhos celulares inteligentes, que combinam em si todas as facilidades que se pode ter: agenda telefônica, conexão à Internet via redes WI-FI ou redes de dados, acesso aos serviços da Google e seus serviços, Microsoft, Zoom, WhatsApp, Telegram, Discord, tudo apenas pelo simples fato de estar o usuário conectado à Internet.

Estas facilidades têm seu preço, o qual é um tanto caro aos usuários da internet e, ironicamente, muito valioso à investigação brasileira: dados armazenados em diversas plataformas e serviços. Com isso, a tecnologia trouxe melhorias à investigação, mas há de se fazer ponderações acerca dos dados – e suas diversas roupagens – e o assunto muito conhecido como telemática, o qual será muito debatido no decorrer deste capítulo.

1.1 Proteção Constitucional do Sigilo de Dados e suas Limitações

No que concerne à proteção de sigilo de dados, de modo geral, a Constituição Federal trata do assunto no art. 5º, incisos X e XII. A garantia de sigilo de dados como norma constitucional é atual, visto ter sido trazida com a Constituição Federal de 1988. Com a inovação vieram muitas consequências jurídicas.

É preciso, no entanto, antes de se adentrar à tratativa do assunto acerca de sigilo, discorrer sobre a privacidade e a intimidade, garantias constitucionais previstas no art. 5º, X, da CF. André Ramos Tavares (2020) ensina que compete ao titular de direito, apenas, a escolha da divulgação ou não de dados, manifestações e referências individuais; e, caso opte por divulgar dados, cumpre ao titular, ainda, decidir como, quando, onde e a quem.

Tavares (2020) traz que a Lei n. 13.709/18 – Lei Geral de Proteção de Dados –

representa um marco importante sobre a proteção de dados pessoais (de pessoas físicas ou jurídicas), que impacta, diretamente, na salvaguarda de direito à intimidade, imagem e honra.

> A Lei introduz as hipóteses nas quais se pode admitir o tratamento de dados pessoais considerados sensíveis, assim considerado aquele "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5º, inc. II, da Lei). (TAVARES, 2020, p. 678).

A defesa da privacidade, garantia constitucionalmente assegurada, tem o escopo de proteger o homem contra:

> a) Interferência em sua vida privada, familiar e doméstica; (b) a ingerência em sua integridade física ou mental, ou em sua liberdade intelectual e moral; (c) os ataques à sua honra e reputação; (d) sua colocação em perspectiva falsa; (e) a comunicação de fatos relevantes e embaraçosos relativos à sua intimidade; (f) o uso de seu nome, identidade e retrato; (g) a espionagem e a espreita; (h) a intervenção na correspondência; (i) a má utilização de informações escritas e orais; (j) a transmissão de informes dados ou recebidos em razão de segredo profissional. Com relação a esta necessidade de proteção à privacidade humana, não podemos deixar de considerar que as informações fiscais e bancárias, sejam as constantes nas próprias instituições financeiras, sejam as constantes na Receita Federal ou organismos congêneres do Poder Público, constituem parte da vida privada da pessoa física ou jurídica. (MORAES, 2017, p. 66).

Não há exatidão quanto ao significado mais acertado da palavra privacidade, ou seja, não existe um conceito único. Há diversos posicionamentos doutrinários que tratam sobre o possível significado, de modo que podem ser mais restritos ou mais abrangentes (ASSIS, 2015). Para Bastos (2000, p. 56), a privacidade é entendida como a escolha que cada pessoa tem "de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano".

É digno de realce que a privacidade adquiriu nova roupagem com o decorrer dos anos e a evolução da tecnologia, em especial, o ambiente cibernético. A privacidade voltada ao ambiente cibernético, nos ensinamentos de Paesani (2014, p. 39),

> apresenta duas ordens de problemas: o primeiro reporta-se ao respeito à esfera privada alheia que nos conduz no terreno tradicional da tutela da privacidade. O segundo refere-se à privacidade de quem se movimenta naquele espaço e,

> consequentemente, requer o anonimato. Contudo, os dois problemas estão destinados a saberem as consequências que o indivíduo pode ter se for considerada que a sua privacidade está sendo violada por uma informação na rede.

O direito à intimidade, consoante René Ariel Dotti (1980), deve ser analisado como inserido na vida privada sob a perspectiva da teoria dos círculos concêntricos: "a intimidade seria um círculo concêntrico e de menor raio que a vida privada. Quanto maior for a proximidade das informações a revelar das esferas de intimidade e segredo, maior peso terão que assumir as razões para a sua revelação, do ponto de vista do interesse público".

De acordo com o previsto no art. 5º, XII, da Constituição Federal, "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".

Através de uma análise superficial da norma insculpida no art. 5º, XII, da Constituição Federal, nota-se há proteção constitucional quanto à inviolabilidade do sigilo das correspondências, das comunicações telegráficas e de dados, sendo que para as comunicações telefônicas é necessária a autorização judicial para a sua devassa, nas hipóteses de investigação criminal e instrução processual. Porém, cumpre destacar que essas garantias individuais acima não são absolutas e são, obviamente, passíveis de relativização.

Conforme ensinamento do Min. Celso de Mello, do Supremo Tribunal Federal, os direitos e garantias individuais não têm caráter absoluto: "Não há, no sistema constitucional brasileiro, direitos ou garantias que se revistam de caráter absoluto, mesmo porque razões de relevante interesse público ou exigências derivadas do princípio de convivência das liberdades legitimam" (BRASIL, 2000).

O art. 5º, XII, citado acima pode ensejar a inúmeras interpretações equivocadas por parte diversos profissionais. Neste sentido, cumpre trazer os ensinamentos do mestre Renato Brasileiro de Lima (2020a, p. 759):

> [...] Essa linha de interpretação vai de encontro ao posicionamento doutrinário e jurisprudencial sedimentado no direito pátrio e no direito alienígena de que os direitos fundamentais, por mais importantes que sejam, não são dotados de caráter absoluto. *Na verdade, não há falar em direito fundamental absoluto. Todos os direitos fundamentais devem ser submetidos a um juízo de ponderação quando entram em rota de colisão com outros direitos fundamentais, preponderando aquele de maior relevância*. (grifo nosso).

De igual forma, Alexandre de Moraes (2017, p. 60) entende que apesar da exceção constitucional acima referir-se, expressamente, somente à interceptação telefônica, nenhuma liberdade individual é absoluta, sendo possível, respeitados outros parâmetros, que haja a interceptação das correspondências, telegráficas e de dados sempre que as liberdades públicas forem utilizadas como mecanismo de proteção às práticas ilícitas.

Vale analisar cada um dos elementos do art. 5º, XII, CF:

• Sigilo da correspondência

Por correspondência entende-se a troca de informações via carta, recados, mensagens digitadas ou manuscritas. Lenza (2020, p. 1238) entende que, via de regra, o sigilo de correspondência é inviolável, com exceção nas hipóteses de decretação de estado de defesa e de sítio (arts. 136, §1º, I, "*b*", e 139, III), quando poderá ser restringido.

Este direito, no entanto, não é absoluto e poderia, conforme caso concreto, ser afastado, como por exemplo numa interceptação de uma carta enviada por sequestradores. A suposta prova ilícita é convalidada em razão da excludente de ilicitude, legítima defesa.

Vejamos o teor dos artigos citados, *litteris*:

> Art. 136. O Presidente da República pode, ouvidos o Conselho da República e o Conselho de Defesa Nacional, decretar estado de defesa para preservar ou prontamente restabelecer, em locais restritos e determinados, a *ordem pública ou a paz social ameaçadas por grave e iminente instabilidade institucional ou atingidas por calamidades de grandes proporções* na natureza.
> § 1º O decreto que instituir o estado de defesa determinará o tempo de sua duração, especificará as áreas a serem abrangidas e indicará, nos termos e limites da lei, as *medidas coercitivas* a vigorarem, dentre as seguintes:
> *I - restrições aos direitos de:* [...]
> b) *sigilo de correspondência*; [...]
>
> Art. 139. Na vigência do estado de sítio decretado com fundamento no art. 137, I, só poderão ser tomadas contra as pessoas as seguintes medidas: [...]
> III - *restrições relativas à inviolabilidade da correspondência, ao sigilo das comunicações, à prestação de informações e à liberdade de imprensa, radiodifusão e televisão, na forma da lei*; [...] (grifos nossos).

Neste sentido, é o posicionamento do Supremo Tribunal Federal:

> [...] *A administração penitenciária, com fundamento em razoes de segurança pública, de disciplina prisional ou de preservação da ordem jurídica, pode, sempre excepcionalmente, e desde que respeitada a norma inscrita no art. 41, parágrafo único, da Lei n. 7.210/84, proceder a interceptação da correspondência remetida pelos sentenciados, eis que a cláusula tutelar da inviolabilidade do sigilo epistolar não pode constituir instrumento de salvaguarda de praticas ilícitas* [...] (BRASIL, 1994). (grifo nosso).

Ainda, de acordo com Mendes e Branco (2015), não havendo direitos absolutos, também o sigilo de correspondência e o de comunicações telegráficas são passíveis de ser restringidos em casos recomendados pelo princípio da proporcionalidade. O sigilo das correspondências e das comunicações é verdadeiro princípio corolário das inviolabilidades previstas na Carta Política.

• Sigilo das comunicações telegráficas[2]

Quanto ao sigilo das comunicações telegráficas é importante mencionar que, basicamente, são aquelas comunicações realizadas por meio do aparelho denominado telégrafo, o qual é destinado à comunicação baseada em eletricidade para enviar mensagens codificadas através de fios, que foi muito utilizado nos anos XX. O aparelho, entretanto, está em desuso ante a tecnologia avançada das comunicações. Lenza (2020, p. 1238) alega que esse tipo de comunicação é inviolável, salvo nas hipóteses de decretação de estado de defesa e de sítio, que poderá ser restringido, nos termos dos arts. 136, §1º, I, "*c*", e 139, III, CF) ou em razão de eventual ponderação a ser feita num caso concreto.

Vejamos, pois, o disposto nos artigos citados, *litteris*:

> Art. 136. O Presidente da República pode, ouvidos o Conselho da República e o Conselho de Defesa Nacional, decretar estado de defesa para preservar ou prontamente restabelecer, em locais restritos e determinados, a ordem pública ou a paz social ameaçadas por grave e iminente instabilidade institucional ou atingidas por calamidades de grandes proporções na natureza.
> § 1º O decreto que instituir o estado de defesa determinará o tempo de sua duração, especificará as áreas a serem abrangidas e indicará, nos termos e limites da lei, as *medidas coercitivas a vigorarem*, dentre as seguintes:
> I - *restrições* aos direitos de: [...] *c) sigilo de comunicação telegráfica e telefônica*; (grifo nosso)

Ainda, temos o que está disposto abaixo:

> Art. 139. Na vigência do estado de sítio decretado com fundamento no art. 137, I, só poderão ser tomadas contra as pessoas as seguintes medidas: [...]
> III - *restrições relativas à inviolabilidade da correspondência, ao sigilo das comunicações, à prestação de informações e à liberdade de imprensa, radiodifusão e televisão, na forma da lei*; (grifo nosso).

• Sigilo de dados

Trata-se de um desdobramento do direito à privacidade e à intimidade previstos nos arts. 5º, X e XII, da CF. Como citado em linhas anteriores, o sigilo de dados comporta

[2] Para informações específicas de caráter técnico, acesse: https://escola.britannica.com.br/artigo/tel%C3%A9grafo/482651

relativização. A *contrario sensu* posiciona-se Lênio Streck (1997) no sentido de que o sigilo de dados é absoluto.

Em apertada síntese, de maneira objetiva e sem delongar nas diversas possibilidades de classificações dos dados, quando se fala em sigilo de dados, esses podem ser bancários, fiscais, telemáticos, cadastrais, informáticos, estáticos (classificação recentemente feita pelo Superior Tribunal de Justiça), dentre outros.

Há diferença entre os tipos de dados, senão vejamos:

> Em primeiro lugar, a expressão "dados" manifesta uma certa impropriedade (Celso Bastos/Ives Gandra; 1989:73). Os citados autores reconhecem que por "dados não se entende o objeto de comunicação, mas uma modalidade tecnológica de comunicação. [...] Os dados aqui são os dados informáticos (v. incs. XIV e LXXII)". [...] O sigilo, no inciso XII do art. 5°, está referido à comunicação, no interesse da defesa da privacidade. Isto é feito, no texto, em dois blocos: a Constituição fala em sigilo "da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas". [...]. Obviamente o que se regula é comunicação por correspondência e telegrafia, comunicação de dados e telefônica. O que fere a liberdade de omitir pensamento é, pois, entrar na comunicação alheia, fazendo com que o que devia ficar entre sujeitos que se comunicam privadamente passe ilegitimamente ao domínio de um terceiro. [...] Mas se alguém entra nesta transmissão, como um terceiro que nada tem a ver com a relação comunicativa, ou por ato próprio ou porque uma das partes lhe cede o acesso indevidamente, estará violado o sigilo de dados. (FERRAZ JÚNIOR, 1993).

Ferraz Júnior (1993) é categórico: "A distinção é decisiva: o objeto protegido no direito a inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação". Ferraz Júnior (1993) ainda defende:

> Antes de mais nada, que dos quatro meios de comunicação ali mencionados – correspondência, telegrafia, dados, telefonia – só o último se caracteriza por sua instantaneidade. Isto é, a comunicação telefônica só é enquanto ocorre. Encerrada, não deixa vestígios no que se refere ao relato das mensagens e aos sujeitos comunicadores.

Importa destacar que, na 2ª Turma do Supremo Tribunal Federal, em caso de relatoria do Min. Carlos Velloso, a respeito do sigilo de dados bancário e fiscal, o entendimento da Corte "consolidou-se no sentido de não possuir caráter absoluto a garantia dos sigilos bancários e fiscal, sendo facultado ao juiz decidir acerca da conveniência da sua quebra em caso de interesse público relevante e suspeita razoável de infração penal" (BRASIL, 2005a).

É oportuno ressaltar que, de fato, dos quatro meios de comunicação citados no art. 5º, XII, da Constituição Federal, apenas a telefônica, em regra, é a destinatária de uma possível interceptação, com ordem judicial, pelo fato de que ela não guarda registros após a realização da ligação. Todavia, ousa-se discordar do mestre, de sorte que, atualmente, por exemplo, serviços de e-mails, tais como Gmail, da Google, Outlook, da Microsoft, ainda que eles guardem registros, é possível realizar a interceptação telemática desses, os quais serão estudados em capítulos próximos.

1.2 Lei n. 9.296/1996: Regulamentação da Interceptação Telefônica e Telemática

Conforme já destacado no tópico anterior, a Constituição Federal dispõe, em seu art. 5º, XII, que "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".

Numa leitura inicial do dispositivo constitucional, poder-se-ia inferir, erroneamente, que apenas a violação do sigilo das comunicações telefônicas necessitaria de ordem judicial para a sua devassa, ou seja, que ela possui caráter relativo e as demais hipóteses mencionadas no artigo caráter absoluto, a não ser que as pessoas envolvidas na relação concedessem a devida autorização para o acesso e revelação do conteúdo. A interpretação nesse sentido não merece prosperar, eis que não existem direitos e garantias fundamentais absolutos.

De acordo com Renato Brasileiro de Lima (2020b, p. 759), "fossem os demais sigilos (de correspondência, das comunicações telegráficas e de dados) de natureza absoluta, não teria o Supremo Tribunal Federal considerado válida a interceptação de correspondência de presos". Neste sentido, o julgamento relatado pelo Min. Celso de Mello (BRASIL, 1994).

A Lei n. 9.296/1996 pode ser invocada para a quebra dos sigilos constitucionalmente assegurados e, nesta toada, para devassa de dados telemáticos. Aplica-se de forma imediata no ordenamento brasileiro a partir da sua vigência, regendo-se pelo princípio processual penal do *tempus regit actum*, nos ditames do art. 2º, do Código de Processo Penal, à exceção do art. 10 (e 10-A após inclusão pelo Pacote Anticrime, Lei n. 13869/19), visto que se trata de dispositivo cuja natureza é penal (LIMA, 2020b, p. 760). Sendo assim, conforme explicam Luiz Flávio Gomes e Sílvio Maciel (2018, p.28), a norma "é composta eminentemente processuais (âmbito de incidência, requisitos, sujeito ativo e passivo, forma de execução das interceptações etc.)".

1.2.1 Histórico

No Brasil, após muitos anos de questionamentos jurídicos acerca da interceptação telefônica e sua regulamentação quanto ao disposto no art. 5º, XII, da Constituição Federal, na parte "por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal", houve, em 24 de julho de 1996, a publicação da Lei n. 9.296/96, conhecida como Lei de Interceptação Telefônica.

A referida lei teve que enfrentar diversos percalços até à promulgação. Algumas constituições brasileiras não trataram diretamente sobre a interceptação telefônica, a exemplo da Constituição de 1946 que, segundo o destaque de Luiz Flávio Gomes e Sílvio Maciel (2018, p. 21), não fazia "[...] sequer referência à comunicação telefônica. Entendia-se, no entanto, que estava compreendida a figura do art. 141, §6º, que cuidada da inviolabilidade do sigilo de correspondência". Já "na Constituição de 1969 – Emenda I, de 1967 (art. 153, §9º) – contemplava-se a inviolabilidade do sigilo de correspondência e das comunicações telegráficas e telefônicas"; sendo que esta norma constitucional, aparentemente, "assegurava o sigilo das comunicações telefônicas de 'modo absoluto', já que mencionava a inviolabilidade do 'sigilo da correspondência e das comunicações telegráficas e telefônicas, *sem prever qualquer exceção ou restrição a esse sigilo*" (GOMES; MACIEL, 2018, p. 21).

Diversos magistrados faziam uso do art. 57, II, "e" da Lei n. 4.117/62 (Código Brasileiro de Telecomunicações) para autorizarem as medidas de interceptação e havia sérias dúvidas sobre a constitucionalidade do referido dispositivo legal e o seu alcance jurídico. Após a promulgação da Constituição Federal de 1988 mudam-se os horizontes. Nesse sentido, assim se posicionou Ada P. Grinover (1999, p. 91):

> Ainda antes da convocação da Assembleia Nacional Constituinte, em diversas ocasiões havíamos manifestado o entendimento de que se fazia imprescindível a interceptação do legislador brasileiro, para o adequado tratamento das interceptações telefônicas autorizadas, delineando, para tanto, as linhas mestras a serem observadas pela lei ordinária. Agora aprovado o projeto de texto constitucional, o próprio mandamento da Lei Maior obriga o legislador a disciplinar minunciosamente a matéria.

O Supremo Tribunal Federal e o Superior Tribunal de Justiça chegaram a se manifestar pela inconstitucionalidade do art. 57, II, "e" do Código Brasileiro de Telecomunicações, pelo fato de ele não ter sido recepcionado pela atual Constituição Federal, *in verbis*:

> [...] o art. 5º, XII, da Constituição, que prevê, excepcionalmente, a violação do sigilo das comunicações telefônicas para fins de investigação criminal ou instrução processual penal, não é autoaplicável: exige lei que estabeleça as hipóteses e a forma que permitam a autorização judicial. Precedentes. a) Enquanto a referida lei não for editada pelo Congresso Nacional, *é considerada prova ilícita a obtida mediante quebra do sigilo das comunicações telefônicas, mesmo quando haja ordem judicial* (CF, art. 5º, LVI). b) *O art. 57, II, e, do Código Brasileiro de Telecomunicações não foi recepcionado pela atual Constituição* (art. 5º, XII), a qual exige *numerus clausus* para a definição das hipóteses e formas pelas quais é legítima a violação do sigilo das comunicações telefônicas [...]. (BRASIL, 1997) (grifo nosso)

A partir de então, a preocupação foi a de regulamentar o art. 5º, XII, CF, todavia, havia a necessidade extrema de uma lei específica que tratasse do assunto. Houve diversos projetos que tratava da matéria no Congresso Nacional, sendo que o último, PL n. 4/96, foi enviado ao Legislativo com a exposição de motivos do Ministro da Justiça Nelson Jobim, que pugnava pela urgência da medida "indispensável à investigação de certos crimes que vêm intranquilizando os habitantes das grandes cidades e, por isso, torna-se imperiosa a edição de lei ordinária a fim de aparelharem-se a polícia e a Justiça para combate à criminalidade mais grave, de alta incidência, nos dias atuais cidades" (JOBIM, 1996).

A lei que fosse regulamentar o art. 5º, XII, da Carta Maior, deveria abarcar três requisitos constitucionais, segundo Luiz Flávio Gomes e Sílvio Maciel (2018, p. 25): (a) lei regulamentadora, com as hipóteses de cabimento e forma de realização das medidas; (b) utilização exclusivamente para fins criminais; e, por fim, (c) por meio de ordem judicial.

Neste sentido, em meio à falta de interesse político sobre o assunto, houve a regulamentação do uso da interceptação telefônica como prova para investigação criminal e processual penal, por meio da Lei n. 9.296, de 24 de julho de 1996, que respeitou um dos requisitos constitucionais para as interceptações telefônicas, qual seja, a lei regulamentadora (GOMES; MACIEL, 2018, p. 28), e criminalizou. por meio do art. 10 e 10-A, após o Pacote Anticrime (Lei n. 13.869/19), condutas.

1.2.2 Conceito, finalidade, requisitos e forma

No entendimento de Renato Brasileiro de Lima (2020b, p. 762), "interceptar uma comunicação telefônica não quer dizer interrompê-la, impedi-la, detê-la ou cortá-la. A expressão deve ser compreendida como o ato de captar a comunicação telefônica alheia, tendo conhecimento do conteúdo de tal comunicação". Ainda, prossegue Lima (2020b, p. 762),

dizendo que é "da essência da interceptação a participação de um terceiro, que passa a ter ciência do conteúdo de uma comunicação *alheia*".

A interceptação telefônica possui, como finalidade, a obtenção de elementos probatórios para investigação criminal ou instrução processual penal, nos termos do art. 5º, XII, da CF e art. 1º, *caput*, da Lei 9.296/96, o qual estatui que a "interceptação de comunicações telefônicas, de qualquer natureza, *para a prova em investigação criminal e instrução processual penal*, observará o disposto nesta lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça" (grifo nosso).

Vale ressaltar que, em que pese a Constituição Federal e a Lei n. 9.296/96 mencionem "investigação criminal" – e não inquérito policial –, o entendimento é da possibilidade da realização da interceptação telefônica, ainda que não haja um inquérito policial devidamente instaurado (LIMA, 2020b, p. 777). A interceptação telefônica para fins de investigação criminal pode se efetivar antes mesmo da instauração do inquérito policial, pois nada impede que as investigações precedam esse procedimento. A providência pode ser determinada para a investigação criminal (até antes, portanto, de formalmente instaurado o inquérito) e para a instrução criminal, depois de instaurada a ação penal (BRASIL, 2005b).

Embora disposto expressamente no art. 5º, XII, da CF e no art. 1º, *caput*, da Lei 9.296/96, sobre "investigação criminal ou instrução processual penal", há julgado no sentido de autorização da interceptação para fins que não matéria criminal, ou seja, administrativo, cível, dentre outras áreas. É o que decidiu o Superior Tribunal de Justiça:

> [...] 1. A possibilidade *de quebra do sigilo das comunicações telefônicas*[3] fica, em tese, restrita às hipóteses de investigação criminal ou instrução processual penal. *No entanto, o ato impugnado, embora praticado em processo cível, retrata hipótese excepcional, em que se apuram evidências de subtração de menor, crime tipificado no art. 237 do Estatuto da Criança e do Adolescente*. [...] (grifo nosso) (BRASIL, 2011a).

Outro ponto que merece destaque é que as provas obtidas por meio da interceptação telefônica podem ser utilizadas como prova emprestada. O Superior Tribunal de Justiça, quando do julgamento do MS n. 17.815/DF, entendeu que "é possível a utilização, como prova emprestada, de interceptações telefônicas derivadas de processo penal, com autorização judicial, no processo administrativo disciplinar, desde que seja assegurada a garantia do contraditório" (BRASIL, 2011b).

[3] Chama-se atenção ao fato de que, muito embora se faça menção à expressão "quebra do sigilo das comunicações telefônicas" na ementa do julgado, há a previsão de seu para interceptação telefônica.

Assevera-se que além dos requisitos dispostos no art. 5º, XII, da CF, para a legalidade das interceptações telefônicas e telemáticas é necessário que se preencham os requisitos, cumulativamente, elencados no art. 2º da Lei n. 9.296/96, quais sejam: não haver indícios razoáveis da autoria ou participação em infração penal; possibilidade de produção de prova por outros meios disponíveis; e configuração do fato investigado como infração penal punida, no máximo, com pena de detenção. Ademais, a interceptação telefônica (e também a telemática) é medida cautelar preparatória, quando concluída na fase policial, ou medida cautelar incidental, caso realizada em juízo, durante o processo penal (GOMES; MACIEL, 2018, p. 104). Em sendo medida cautelar, há exigência do preenchimento dos requisitos básicos: *fummus comissi delicti* e o *periculum in mora*.

Dada à diversidade de nomenclaturas acerca do assunto, convém fazer algumas distinções que se reputam de grande importância para a evolução e aprofundamento do assunto. Resumidamente, estão elencados abaixo alguns conceitos:

Tabela 1 – Conceitos dos meios extraordinários de captação de conversas

Tipo	Interceptação telefônica (ou em sentido estrito)	Escuta telefônica	Gravação telefônica (ou gravação clandestina)
Conceito	É realizada por terceira pessoa, que atua sem o conhecimento dos interlocutores.	Captação da conversa realizada por terceiro, mas com a ciência de um dos interlocutores.	Gravação da comunicação telefônica por um dos comunicadores, isto é, trata-se de uma autogravação (ou gravação própria da comunicação). Feita sem o conhecimento do outro comunicador.
Exemplo	Polícia intercepta a ligação de membros de organização criminosa.	Polícia grava, através do viva-voz, a conversa telefônica que o pai mantém com o sequestrador de sua filha	Caso em que Joesley Batista grava o diálogo entre ele e o ex-presidente da República, Michel Temer.
Validade	**Válida**, desde que autorizada via judicial. Cláusula de reserva de jurisdição. **Pacífico** no STF e STJ.	STJ, HC 161.053/SP: **Válido.**	STJ, REsp 1026605/ES: **Válido**.

Fonte: (CAVALCANTE, 2020).

Tabela 2 – Captação em sentido amplo

Tipo	Interceptação ambiental	Escuta ambiental	Gravação ambiental
Conceito	Ocorre quando um terceiro capta o diálogo ou as imagens envolvendo duas ou mais pessoas, sem que nenhum dos alvos saiba.	Ocorre quando um terceiro capta o diálogo ou as imagens envolvendo duas ou mais pessoas, sendo que um dos alvos sabe que está sendo realizada a escuta.	Ocorre quando o diálogo ou as imagens envolvendo duas ou mais pessoas é captado, sendo que um dos alvos é o autor dos registros. Também é chamada de gravação ambiental clandestina (no sentido de feito às escondidas).

Exemplo	Polícia, com autorização judicial, instala um microfone e um gravador escondidos no gabinete de um servidor público investigado por corrupção.	Polícia filma o momento em que determinado empresário (ciente da filmagem) entrega quantia em dinheiro exigida por fiscal corrupto.	Mulher instala uma câmera na casa e filma o momento em que o ex-marido ameaça matá-la.

Fonte: (CAVALCANTE, 2020).

Importante citar que segundo Márcio André Lopes Cavalcante (2020), antes da edição e promulgação da Lei n. 13.964/19 (Pacote Anticrime), para que houvesse a interceptação ou escuta ambiental deveria ser verificado o seguinte: caso as pessoas investigadas estivessem em ambiente público, o entendimento prevalecido era de que não havia necessidade de autorização judicial, visto que não havia violação à intimidade e à privacidade das pessoas; se a captação se desse em local restrito, necessitar-se-ia de autorização judicial.

Na jurisprudência do STF, conforme destacou o Ilustre Ministro Sepúlveda Pertence, ao proferir seu voto no julgamento do Habeas Corpus n. 87.341-3/PR, "[...] não há nenhuma ilicitude na documentação cinematográfica da prática de um crime, a salvo, é claro, se o agente se encontra numa situação de intimidade" (BRASIL, 2006a).

Agora, para a gravação ambiental o entendimento que prevalecia era a de que, via de regra, a gravação ambiental realizada por um dos interlocutores não necessita de autorização judicial, visto que é "lícita a prova consistente em gravação ambiental realizada por um dos interlocutores sem conhecimento do outro" (BRASIL, 2009). Com o advento da Lei n. 13.964/19, que inseriu o art. 8º-A na Lei n. 9.296/96, passou-se a fixar que a "investigação ou instrução criminal, poderá ser autorizada pelo juiz, a requerimento da autoridade policial ou do Ministério Público, a captação ambiental de sinais eletromagnéticos, ópticos ou acústicos", e estas regras, por sua vez, segundo o Superior Tribunal de Justiça, "aplicam-se subsidiariamente à captação ambiental as regras previstas na legislação específica para a interceptação telefônica e telemática" (BRASIL, 2020).

Contudo, caso a captação ambiental seja realizada por um dos interlocutores, não é necessária a autorização judicial, nos termos do art. 10-A, §1º, da Lei n. 9.296/96, e do STJ, de modo as alterações trazidas pela Lei n. 13.964/19, Pacote Anticrime, à Lei n. 9.296/96, "alteraram o entendimento de que é LÍCITA (válida) a prova consistente em gravação ambiental realizada por um dos interlocutores sem o conhecimento do outro" (BRASIL, 2020).

1.2.3 Interceptação do fluxo de comunicações em sistemas de informática e telemática

O conceito de interceptação telefônica já foi amplamente debatido no tópico anterior,

mas vale pontuar desde logo que o mesmo raciocínio quanto a requisitos, finalidades e prazos se aplica à interceptação telemática, que, nos termos do art. 1º, parágrafo único, Lei n. 9.296/96, é conceituada como "interceptação do fluxo de comunicações em sistemas de informática e telemática"[4]. A interceptação telemática "diferentemente da obtenção de dados que repousem em servidores, constitui a captação de uma comunicação contemporânea, ou seja, que esteja ocorrendo no momento em que for captada" (SILVA, 2014, p. 48).

Não há um consenso na computação acerca da precisa definição do que seria a telemática. Porém, ensinam Luiz Flávio Gomes e Sílvio Maciel (2018, p. 92) que é "a ciência que cuida da comunicação (transmissão, manipulação) de dados, sinais, imagens, escritos e informações por meio do uso combinado de informática (do computador) com as várias formas de telecomunicação", ou seja, é a associação de telecomunicação com informática.

Telecomunicação, por sua vez, segundo o disposto no art. 60, §1º, da Lei n. 9.472/97, que dispõe sobre a organização dos serviços de telecomunicações, a criação e o funcionamento de um órgão regulador e outros aspectos institucionais, é "[...] a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza". Basicamente, trata-se da possibilidade de transmissão e recepção de dados, vídeos, imagens, escritos, isto é, a conjugação de telefonia com informática (GOMES; MACIEL, 2018, p. 94). O legislador brasileiro anteviu, por meio da Lei n. 9.296/96, a evolução a que poderia chegar à tecnologia notadamente voltada a dados e informática.

O leitor poderia realizar o seguinte questionamento: o que diferencia uma troca de SMS por meio de celulares entre duas pessoas de uma troca de mensagem via aplicativo WhatsApp, por exemplo? A diferença reside no fato de que o serviço de SMS (*short message service*) utiliza protocolo de comunicação baseado em texto; ao passo que uma mensagem enviada pelo aplicativo WhatsApp (ou outro similar) utiliza-se de dados e conexão com a Internet, por meio de um endereço IP[5].

Atualmente, a interceptação do fluxo de comunicações telemáticas e informática trata

[4] Segundo Vicente Greco Filho (1996, p. 10), "a norma citada é inconstitucional porque a expressão constitucional 'no último caso' somente se refere às comunicações telefônicas". Para Greco Filho (1996, p. 10), "a Constituição autoriza, nos casos nela previstos, somente a interceptação de comunicações telefônicas, e não a de dados e muito menos as telegráficas [...]". O parágrafo único do art. 1º, da Lei n. 9.296/96 foi objeto da ADIn n. 1.488, relatada por Néri da Silveira, a qual teve o pleito liminar indeferido e, consequentemente, foi extinta por falta de legitimidade ativa do requerente (BRASIL, 1996). Sendo assim, em que pese o posicionamento minoritário, sustenta-se a constitucionalidade da interceptação telemática.

[5] IP – *Internet Protocol* é um número identificador dado ao seu computador ou roteador, ao conectar-se à rede. É através desse número que seu computador pode enviar e receber dados na internet. O IP é definido pelo seu provedor de Internet.

objetivamente da consecução de dados armazenados e/ou protegidos em diversos servidores de aplicação, por exemplo, Google, WhatsApp/Facebook/Instagram, Microsoft (e seus diversos serviços), além de outros (FREITAS JÚNIOR; JORGE; GARZELLA, 2020, p. 37). É importante esclarecer que há diferença entre a quebra do sigilo telemático (ou afastamento do sigilo telemático) e a interceptação do fluxo das comunicações telemática. A quebra do sigilo telemático é a consecução, por meio de ordem judicial, de dados armazenados em servidores de aplicação, ao passo que a interceptação telemática consiste em realizar, no momento em que ocorre, o "desvio" (que na verdade é uma cópia) para os serviços de investigação da comunicação entre duas pessoas via aplicativo.

Outro exemplo de quebra do sigilo de dado telemático ocorre quando determinada pessoa investigada possui serviço de e-mail em nuvem, por exemplo, Google Gmail (que é conhecido como servidor de aplicação). Um pedido de quebra de sigilo do e-mail dessa pessoa faz com que o Google Gmail repasse todos os e-mails (enviados, deletados, arquivados) que estão lá armazenados. O fornecimento dessa quebra varia conforme a decisão judicial, visto que cada órgão investigador deve mencionar um intervalo de tempo para o fornecimento da quebra de sigilo telemática.

Atualmente, alguns dos principais servidores de aplicações são: WhatsApp, Telegram, UOL, Facebook/Instagram, Microsoft (OneDrive, Xbox etc), Uber (todas as corridas, dados de clientes, transações, geolocalização, dentre outros, estão armazenados em seus servidores) e Google (e seus variados serviços, Google Drive, Google Maps, Google Gmail). Cada servidor de aplicação tem seu modo de operar, no sentido de coletar, armazenar e processar os dados dos clientes, e alguns deles podem não realizar a interceptação telemática em virtude de condições de infraestrutura técnica de seus serviços. Normalmente, no dia-a-dia de investigação é extremamente comum se deparar com respostas incompletas, mal formuladas, incoerentes, dentre outras justificativas, as quais serão estudadas nos próximos tópicos.

1.3 Marco Civil da Internet (Lei n. 12.965/14) e Lei Geral de Proteção de Dados (Lei n. 13.709/18)

Até o ano de 2014 não havia legislação que tratasse e assegurasse o sigilo das comunicações e a privacidade dos usuários do mundo virtual. Em 23 de abril de 2014, após intenso debate da sociedade sobre o assunto, foi promulgada a Lei n. 12.965/2014, mais conhecida como Marco Civil da Internet, tendo como escopo o respeito a princípios, garantias, direitos e deveres para o uso da internet no Brasil.

> O Marco Civil da Internet traz como pedra fundamental o princípio da privacidade. Nesse sentido vale destacar no art. 3º o seguinte: proteção da privacidade; inviolabilidade da intimidade e da vida privada; inviolabilidade ao sigilo do fluxo de suas comunicações; inviolabilidade ao sigilo de suas comunicações privadas armazenadas e outros. (VIEIRA, 2017, p. 12)

Neste sentido, abaixo realizar-se-á uma exposição dos principais pontos da Lei n. 12.965/14 que tocam este trabalho. Para começar, seguem alguns conceitos elementares sobre tecnologia situados no art. 5º do Marco Civil da Internet:

> Art. 5º Para os efeitos desta Lei, considera-se:
> *I - internet*: o sistema constituído do 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;
> *II - terminal*: o computador ou qualquer dispositivo que se conecte à internet;
> *III - endereço de protocolo de internet (endereço IP):* o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;
> *IV - administrador de sistema autônomo:* a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;
> *V - conexão à internet:* a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;
> *VI - registro de conexão:* o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
> *VII - aplicações de internet:* o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
> *VIII - registros de acesso a aplicações de internet:* o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Feitas algumas considerações terminológicas, é oportuno elencar alguns princípios presentes no Marco Civil da Internet, conforme seu art. 3º:

> 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;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

O acesso à Internet é essencial ao exercício da cidadania e ao usuário são assegurados os seguintes direitos: inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação, inviolabilidade e sigilo do fluxo de suas comunicações pela internet e de comunicações privadas armazenadas que apenas pode ser rompida por ordem judicial, além de outros direitos previstos no art. 7º da lei.

Dentre os pontos principais da lei, citam-se o princípio da neutralidade. Segundo o art. 9º, *caput*, por neutralidade de rede tem-se que o responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação. O Marco Civil da Internet se fundamenta em três pilares, são eles: neutralidade da rede, privacidade de usuários e liberdade de expressão. (MASSO; ABRUSIO; FLORÊNCIO FILHO, 2014).

A lei previu e reservou capítulo específico para a proteção aos registros, aos dados pessoais e às comunicações privadas, de modo que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet, 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 (art. 10º, *caput*).

Semelhante ao art. 5º, XII, CF, o Marco Civil da Internet também prevê que o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º. O art. 11, do Marco Civil da Internet, prevê que:

> Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade [...] e aos sigilos das comunicações privadas [...].

Tomasevicius Filho (2014, p. 164 apud VIEIRA, 2017, p. 209) alega que o art. 11,

> [...] mostra a "falência" da regulação da privacidade na Internet, uma vez que se procurou conferir aplicação extraterritorial à proteção da vida privada dos

> usuários brasileiros. No entanto, tal norma não tem como ser aplicada, visto que os principais mecanismos de busca, servidores de e-mails e páginas das redes sociais estão situados nos Estados Unidos, em face dos quais o Brasil não tem jurisdição.

A lei prevê sanções cíveis, criminais ou administrativas às empresas que descumprirem o Marco Civil da Internet, que vão desde advertência até proibição de exercício das atividades.

Contudo, empresas de grandes provedores de aplicação (Google, Facebook, WhatsApp, Instagram) com escritórios situados no Brasil comumente desrespeitam a legislação brasileira e não colaboram para implementação do ordenamento jurídico brasileiro ou com os processos de investigação. Sendo assim, a lei tratou sobre sanções pelo descumprimento:

> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa: [...]
> Parágrafo único. Tratando-se de empresa estrangeira, *responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.* (grifo nosso).

Abaixo, segue quadro-resumo com as hipóteses de retenção de dados segundo os arts. 13 ao 17 do Marco Civil da Internet:

Tabela 3 – Retenção de dados segundo Marco Civil da Internet

<table>
<tr><th></th><th>Provedor de conexão</th><th>Provedor comercial de aplicação</th><th>Provedor <u>NÃO</u> comercial de aplicação</th></tr>
<tr><td>Tipos de dados a serem retidos</td><td>Registros de conexão à Internet</td><td colspan="2">Registros de acesso a aplicações</td></tr>
<tr><td>Obrigatoriedade de retenção dos dados</td><td colspan="2">Obrigatório</td><td rowspan="2">Mediante ordem judicial</td></tr>
<tr><td>Período de retenção dos dados</td><td>1 ano</td><td>6 meses</td></tr>
<tr><td>Aumento do período de retenção</td><td colspan="3">Mediante requisição sem ordem judicial</td></tr>
<tr><td>Acesso aos dados retidos</td><td colspan="3">Ordem judicial</td></tr>
</table>

(CPICIBER, 2021a)

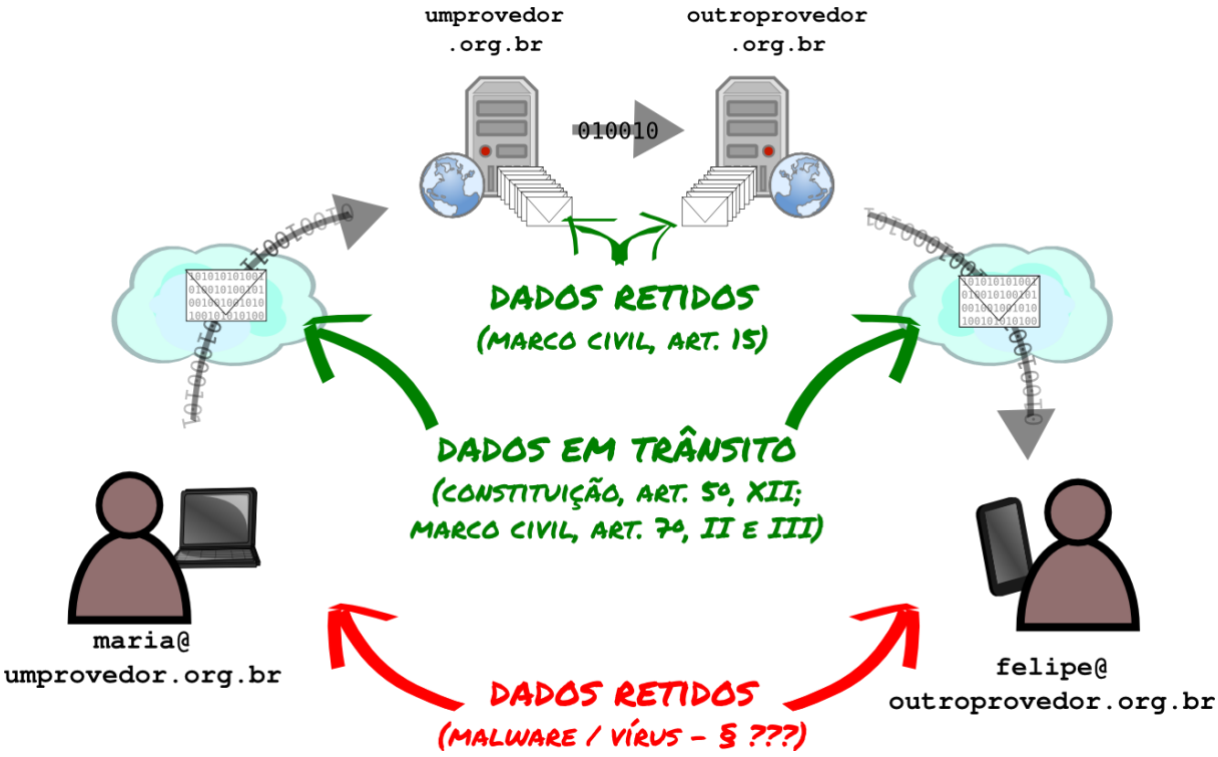
Acerca da interceptação e/ou quebra (ou afastamento do sigilo telemática), não se pode deixar de lado o que entendeu o STF quando do julgamento do Recurso Extraordinário n.

418.416/SC, no sentido de que “a proteção a que se refere o art. 5º, XII, [da Constituição], é da ‘comunicação de dados’ e não dos dados em si considerados”, ainda que armazenados em computador (BRASIL, 2006b). Todavia, em que pese ser uma decisão muita acertada no que concerne à diferenciação entre a comunicação de dados de dados em si, ela não previu as hipóteses, muito comuns e atuais, de armazenamento em *Cloud*, isto é, em nuvem.

Interpretando a decisão mencionada, há de se concluir a nítida classificação das comunicações em duas categorias: comunicação em trânsito, que configura a interceptação telemática propriamente dita, e comunicação armazenada, aquela em que os dados ficam armazenados localmente em celulares, notebooks, computadores, desktop do usuário ou em servidores/provedores de aplicação.

Evidentemente, insta mencionar que, neste caso, não há legislação que trata, especificamente, do acesso a estes dados armazenados nos dispositivos e nas hipóteses discorridas acima. O raciocínio mais coerente, em termos de acesso a estes dados, seria nas hipóteses consagradas no Código de Processo Penal, via mandado de busca e apreensão, ou ainda, em hipótese extrema, via infecção por *malwares* (CPICIBER, 2021b).

Imagem 1 – Dados em trânsito vs. dados retidos (armazenados)



(CPICIBER, 2021b)

Depois de alguns anos de vigência do Marco Civil da Internet, a disciplina sobre os

dados informáticos ganhou novo rumo com a edição da Lei n. 13.704/18, mais conhecida como Lei Geral de Proteção de Dados – LGPD, a qual dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A lei está dividida em 10 (dez) capítulos, os quais vão desde as disposições gerais, fundamentos, propósito, direitos/deveres e garantias do titular, responsabilidades e sanções administrativas pela não implementação de dados e/ou vazamento (em inglês, *leak*[6], ou *data beach*). Dentro da lei, importante destacar o art. 2º, que consubstancia seus fundamentos:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Merece destaque, para os fins deste trabalho, a distinção feita pela Lei n. 13.704/18 entre três tipos de dados: dado pessoal, dado pessoal sensível e dado anonimizado. Segundo disposto no art. 5º, I, da lei, entende-se por dado pessoal a informação relacionada à pessoa natural identificada ou identificável. Já dado pessoal sensível, nos termos do art. 5º, II, é aquele que se refere à origem racial ou étnica, à convicção religiosa, à opinião política, à filiação a sindicato ou a organização de caráter religioso, filosófico ou político, à saúde ou à vida sexual, à genética ou à biometria, sempre vinculado a uma pessoa natural. Por fim, dado anonimizado, conforme art. 5º, III, é dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

[6] Expressões do mundo da segurança ofensiva que significam vazamento de dados.

CAPÍTULO 2 – INVESTIGAÇÃO DE CRIMES EM MEIOS TECNOLÓGICOS E PROCEDIMENTOS PARA A REQUISIÇÃO DE DADO INFORMÁTICO

2.1 Uso de dispositivo informático na práxis delituosa: crimes eletrônicos e provas decorrentes de comunicação telemática

No ano de 2019 o Brasil virou palco para diversas notícias ruins veiculadas todos os dias nos mais diversos meios de comunicação. Em um primeiro momento, obviamente, estão as notícias relacionadas à pandemia da COVID-19. Todavia, não são "apenas" veiculações de informações sobre a pandemia, que ganham destaque entre as notícias ruins mais recentes. No último ano, o Brasil tem sido alvo de ataques cibernéticos de diversas modalidades, com variados alvos e com vasta gama de objetivos: desde práticas de hacktivismo até ataques criminosos, tal qual ocorreu com o STJ, em novembro de 2020 (STJ É VÍTIMA..., 2021).

Além de invasões de dispositivos, citam-se práticas delituosas de *phishing*[7], *Distributed Denial of Service* (DDoS)[8], *defacements*[9] e outras. O resultado, como não é novidade, são diversos vazamentos de dados e, não bastasse isso, comercialização destes em ambiente da *Darknet*[10]. A respeito dos ataques cibernéticos é muito importante destacar que, aos poucos, o direito e a doutrina vêm se especializando sobre o assunto, de modo a tentar acompanhar a evolução criminosa cibernética.

Nas palavras de Spencer Toth Sydow (2015, p. 37):

> Ataques cibernéticos são aquelas condutas, singulares (individuais) ou orquestradas (coletivas) utilizando-se exlusivamente do meio informático para o atingimento de bem jurídico. São denominados ataques cibernéticos próprios quando voltados para danos a bem informáticos (aqui considerados a segurança informática, tripartida em disponibilidade, confidencialidade ou integridade de dados ou sistemas). Porém há grande espectro, ante a variedade de alvos e maior danosidade potencial, em ataques cibernéticos impróprios, ou seja aqueles voltados contra bens jurídicos comuns. Assim, não se limitam à invasão remota de sistemas como alguns entendem. As hipóteses de danos cibernéticos aumentam à medida em que mais áreas passam a ser controladas por sistemas informatizados. Mais do que o acesso às informações armazenadas, o risco cada vez mais reside na tomada de controle, seja para bloqueio e paralisação de seu funcionamento (indisponibilidade), seja – com ainda maior lesividade – para exercitar o comando – normalmente temporário – do sistema.

[7] *Phishing* é uma prática fraudulenta de apropriação de dados on-line por meio da provocação de cliques em links aparentemente autênticos por parte de usuários inadvertidos.
[8] *Distributed Denial of Service* (DDoS) são ataques informáticos cujo objetivo é a derrubada ou a sobrecarga de servidores da *Web*.
[9] *Defacements* são ataques informáticos com o propósito de desfiguração de sites.
[10] A *Deep Web* é uma das redes que compõem a *Darknet*.

Importante mencionar que os ataques cibernéticos são usados como verdadeiras armas cibernéticas, tendo em vista a sua lesividade e ofensividade, que expõem a risco diversos bens jurídicos tutelados. Os ataques cibernéticos podem ocorrer a diversas instituições e motivações, dentre as quais se destacam os ataques cibernéticos de cunho militar.

Segundo Magalhães e Sydow (2018, p. 147), o ataque cibernético militar "além daqueles verificados entre nações em guerra, abrangem os dirigidos a alvos militares estratégicos, a infrastruturas nacionais críticas ou que promovam a ameaça ao território ou à soberania por meio de ferramenta ou recurso cibernético". Neste sentido, os ataques cibernéticos podem ser classificados em:

> *Ataque cibernético fim ou ataque cibernético propriamente dito* – quando o objetivo é destruir, adulterar, interferir ou assumir o controle de banco de dados, redes de comunicação, infraestrutura cibernética, sistemas de comando e monitoramento de proteção da própria informação estratégicade uma força conjunta ou nacional.
> *Ataque cibernético meio ou ataque cibernético ferramenta* – quando o objetivo é destruir, adulterar, interferir ou controlar informações ou sistemas destinados a proteger alvos militares, estratégicos, infraestruturas críticas diversas dos sistemas de informação da nação ou força atracada. Por sua vez, infraestruturas críticas são aquelas necessárias à própria sobrevivência ou funcionamento da nação. (MAGALHÃES; SYDOW, 2018, p. 147)

No que concerne aos ataques cibernéticos, especificamente, no Brasil, contata-se que existe legislação que tipifica alguns crimes cibernéticos (ou informáticos, conforme previsão no Código Penal) e trata das respectivas penas, valendo pontuar algumas destas previsões.

Existe muita dificuldade em se tratando de criação e aprovação de leis que versam sobre matérias penais, tendo em vista diversas possibilidades: a motivação, o clamor social, a correta subsunção (adequação, encaixe à "moldura") do fato à norma penal, evitar que se puna inocentes, bem como a violação dos direitos e garantias fundamentais da pessoa, como o devido processo legal (art. 5º, LIV, CF), a intranscendência da pena (art. 5º, XLV, CF), a presunção de inocência (art. 5º, LVII, CF) e a não incriminação ou "*nemo tenetur se detegere*". Não seria diferente com os crimes eletrônicos, mas quanto a esses há outras peculiaridades que chamam atenção. Neste sentido, discorre Patrícia Peck Pinheiro (2013, p.158):

> O crime eletrônico é, em princípio, um crime de meio, isto é, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por hackers, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros. Isso quer dizer que o meio de materialização da conduta criminosa pode ser virtual; contudo,

> em certos casos, o crime não. [...] As principais inovações jurídicas trazidas no âmbito digital se referem à territorialidade e à investigação probatória, bem como à necessidade de tipificação penal de algumas modalidades que, em razão de suas peculiaridades, merecem ter um tipo penal próprio. [...] Os crimes eletrônicos ou cibernéticos têm modalidades distintas, dependendo do bem jurídico tutelado. Nesse sentido, podemos dar como exemplo o crime de interceptação telefônica e de dados, que tem como bem jurídico tutelado os dados, ou seja, o que se quer é proteger a transmissão de dados e coibir o uso dessas informações para fins delituosos, como, por exemplo, captura de informações para envio de "e-mail bombing", o "e-mail com vírus", o "spam". Esse tipo penal protege também a questão da inviolabilidade das correspondências eletrônicas.

A primeira das leis a surgir de relevância neste campo temático foi a Lei n. 12.737/2012, também conhecida como Lei Carolina Dieckman, atriz que no ano de 2012 foi vitimada pela invasão de seu computador e extração de fotos íntimas. Nos termos da lei,

> [...] é considerado crime invadir o computador, celular, *tablet* e qualquer outro equipamento de terceiros, conectados ou não à *Internet*, para obter, destruir ou divulgar dados sem a autorização do dono do aparelho. As penas para o crime variam de multa a até um ano de prisão. [...] Se a invasão do equipamento resultar em divulgação de dados privados, segredos comerciais e industriais e informações sigilosas, a pena aumenta para seis meses a dois anos de prisão, além da multa. Caso o crime seja cometido contra autoridades como presidente e vice do Executivo, Legislativo e Judiciário, governadores, prefeitos ou presidentes e diretores de órgãos públicos, a pena aumenta pela metade. A invasão de sistemas para obter determinadas informações, destruí-las ou divulgá-las não encontrava correspondente na legislação penal vigente, de forma que os computadores não eram apenas *modus operandi* de uma conduta punível. Surpreende que a legislação aprovada num momento de clamor social delimite com qualidade – sem ampliar em excesso o tipo nem criar óbices para punição caso a tecnologia evolua – estas condutas que não se encontravam abrangidas pela lei penal, embora devessem. Afinal, a intimidade é um direito consagrado internacional e constitucionalmente, devendo ser regulamentada quando for preciso resguardar os fundamentos da segurança e da conservação dos laços sociais. (GARCIA, 2013, p. 256).

Mais recentemente, no dia 01 de abril de 2021, foi publicada a Lei n. 14.132/2021, que tipifica e inclui o art. 147-A, no Código Penal (crime de *stalking*) e revoga o art. 65 da Lei de Contravenções Penais. O crime do art. 147-A do CP é de forma livre, de modo que pode ser praticado "por qualquer meio". No entanto, atualmente, é extremamente comum a prática de perseguição pelos meios digitais, o que se denomina *cyberstalking*. Na internet, formas comuns de *cyberstalking* são deixar comentários em excesso por e-mail, nos serviços de mensagens como WhatsApp e redes sociais da vítima, geralmente com teor obsessivo ou intimidatório. (CASTRO; SYDOW, 2017).

Outras formas, segundo a ONG Safernet (2021), são: divulgar na *Web* as informações pessoais da pessoa, incluindo nome e endereço completo; invadir aparelhos eletrônicos para acessar contas pessoais; preencher a caixa de entrada dos e-mails com spam; enviar vírus ou outros programas nocivos aos computadores de suas vítimas.

Já sobre o "crime de interceptação telefônica e de dados", que interessa especialmente a este trabalho, é preciso deixar claro que ele não é, necessariamente, crime informático. Ele está previsto nos artigos 10 e 10-A da Lei de Interceptação Telefônica, com alteração dada pela Lei n. 13.869/2019, e, segundo sua tipificação, "constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei".

O crime é a devassa da comunicação dos dados e não dos dados em si, isto é, o que ocorre é que um terceiro não autorizado judicialmente intercepta uma ligação telefônica ou telemática, por exemplo. Além do mais, o "envio de e-mail bombing", o "e-mail com vírus" e o "spam", não são tipificados como crime, nestas circunstâncias, ou seja, não há tipificação de crime ao ato de "enviar spam" ou "e-mail bombing".

Com efeito, deve ser observado que, a respeito de armazenamento de dados em provedores, se estes forem pagos, existe uma maior facilidade de identificação de usuários e, com isso, a tentativa de coibir ilícitos cibernéticos, visto que há emissão de fatura mensal ou débito em cartão de crédito, cujos bancos de dados são normalmente mais detalhados e seguros. Todavia, para serviços gratuitos, a tentativa de investigação e consecução de dados torna-se difícil (PINHEIRO, 2013).

Pelas informações gerais apresentadas acima, é necessário trazer alguns breves apontamentos conclusivos: nem todo o crime realizado em algum dispositivo informático é considerado crime informático; o uso da interceptação e/ou quebra de dados telemáticos não necessariamente está relacionado a crimes informáticos; o uso desse meio de obtenção de prova vale para crimes comuns e também para os delitos especiais, isto é, informáticos.

2.2 Procedimentos de requisição de dados telemáticos

Rotineiramente diversas pessoas são vítimas de alguma prática criminosa por meio do uso de algum aplicativo como, a título de exemplo, fraudes financeiras por meio do uso do WhatsApp. Surge, então, após a tentativa ou consumação de um ou mais delito, a necessidade de a Polícia Civil ou o Ministério Público, seja no âmbito estadual ou federal, atuar com a finalidade de coletar o máximo possível de elementos de informação para que se proceda à

identificação dos autores.

Juridicamente falando, após o cometimento de uma infração penal, surge para o Estado o dever de perseguir, processar e punir o autor (ou os autores) por meio do *ius puniendi.* Todavia, para que exista uma investigação eficiente e eficaz, os órgãos incubidos de realizar a *persecutio criminis* (persecução penal) devem ter boas práticas amparadas pela legislação, de acordo com o princípio da legalidade, nos termos do art. 5º, II, CF, ou seja, ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei. Tais práticas devem ser amparadas legalmente, sob pena de nulidade do ato, nos termos do art. 5º, LVI, CF, cujo ensinamento é de de que "são inadmissíveis, no processo, as provas obtidas por meios ilícitos".

Além da disposição constitucional, o art. 157 do Código de Processo Penal, com redação dada pela Lei n. 11.690/08, traz que "são inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais" e que "são também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras".

A invalidação de prova por violação à legalidade irá ensejar a quebra da cadeia de custódia, conforme previsto nos artigos 158-A e seguintes do Código de Processo Penal, com alteração dada pela Lei n. 13.964/19. Nesta senda, eis o posicionamento do STJ:

> [...] 1. A quebra da cadeia de custódia tem como objetivo garantir a todos os acusados o devido processo legal e os recursos a ele inerentes, como a ampla defesa, o contraditório e principalmente o direito à prova lícita. O instituto abrange todo o caminho que deve ser percorrido pela prova até sua análise pelo magistrado, sendo certo que qualquer interferência durante o trâmite processual pode resultar na sua imprestabilidade (RHC 77.836/PA, Rel. Ministro Ribeiro Dantas, Quinta Turma, julgado em 05/02/2019, DJe 12/02/2019). 2. É dever o Estado a disponibilização da integralidade das conversas advindas nos autos de forma emprestada, sendo inadmissível a seleção pelas autoridades de persecução de partes dos áudios interceptados. 3. A apresentação de parcela do produto extraído dos áudios, cuja filtragem foi estabelecida sem a presença do defensor, acarreta ofensa ao princípio da paridade de armas e ao direito à prova, porquanto a pertinência do acervo probatório não pode ser realizado apenas pela acusação, na medida em que gera vantagem desarrazoada em detrimento da defesa. [...] 5. Recursos especiais providos para declarar a nulidade da interceptação telefônica e das provas dela decorrentes, reconhecendo, por consequência, a superveniência da prescrição da pretensão punitiva do Estado, de ofício. (REsp 1795341/RS, Rel. Ministro Nefi Cordeiro, Sexta Turma, julgado em 07/05/2019, DJe 14/05/2019). Com efeito, partindo-se da legalidade, é importante mostrar que a legislação confere às autoridades investigativas poderes-deveres os quais são extremamente úteis para elucidação de crimes, sejam eles cibernéticos ou não. (BRASIL, 2019a)

A Constituição Federal e a legislação definiu, especificamente, quais são os órgãos de investigação criminal, suas funções e prerrogativas. Ela trouxe, no art. 144, os órgãos que compõem a segurança pública no Estado brasileiro, *in verbis*:

> Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos:
> I - polícia federal; [...]
> IV - polícias civis; [...]
> § 1º A polícia federal, instituída por lei como órgão permanente, organizado e mantido pela União e estruturado em carreira, destina-se a:
> [...] IV - exercer, com exclusividade, as funções de polícia judiciária da União.
> [...] § 4º Às polícias civis, dirigidas por delegados de polícia de carreira, incumbem, ressalvada a competência da União, as funções de polícia judiciária e a apuração de infrações penais, exceto as militares.

A Lei n. 12.830/13 dispõe sobre a investigação criminal conduzida pelo delegado de polícia, de modo que ao delegado de polícia, na qualidade de autoridade policial, cabe a condução da investigação criminal por meio de inquérito policial ou outro procedimento previsto em lei, tendo como objetivo a apuração das circunstâncias, da materialidade e da autoria das infrações penais. Consoante o disposto no art. 2º da mencionada lei, as funções de polícia judiciária e a apuração de infrações penais exercidas pelo delegado de polícia são de natureza jurídica, essenciais e exclusivas de Estado e, durante a investigação criminal, cabe ao delegado de polícia a requisição de perícia, informações, documentos e dados que interessem à apuração dos fatos. Em que pese ser uma lei que reconhece poderes investigativos da autoridade policial, ela é bem sucinta e não discorre, especificamente, sobre requisições de dados por parte do delegado de polícia, federal, distrital ou estadual.

O Ministério Público, por sua vez, conforme disposição contida no art. 127, *caput*, da Carga Política, é instituição permanente, essencial à função jurisdicional do Estado, incumbindo-lhe a defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais. Apesar do dispositivo não tratar expressamente dos poderes investigatórios do Ministério Público, importa mencionar que é adotada a teoria dos poderes implícitos. Nos dizeres de Márcio André Lopes Cavalcante (2021), "a CF/88 confere ao MP as funções de promover a ação penal pública (art. 129, I). Logo, ela atribui ao *parquet* também todos os meios necessários para o exercício da denúncia, dentre eles a possibilidade de reunir provas para que fundamentem a acusação". No entanto, prossegue Cavalcante (2021), "a CF/88 não conferiu à Polícia o monopólio da atribuição de investigar crimes. Em outras palavras, a colheita de provas

não é atividade exclusiva da Polícia. Desse modo, não é inconstitucional a investigação realizada diretamente pelo MP".

O STF, pacificando o assunto, editou a tese no sentido de que o Ministério Público:

> [...] dispõe de competência para promover, por autoridade própria, e por prazo razoável, investigações de natureza penal, desde que respeitados os direitos e garantias que assistem a qualquer indiciado ou a qualquer pessoa sob investigação do Estado, observadas, sempre, por seus agentes, as hipóteses de reserva constitucional de jurisdição [...]. (BRASIL, 2015)

Feitas as devidas considerações sobre o escopo da Polícia Judiciária e do Ministério Público, vale trazer à baila o que traz a Lei n. 12.850/13, que define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, as infrações penais correlatas e o procedimento criminal, sendo que ao fazê-lo dispõe precisamente sobre a requisição de dados telemáticos.

Inicialmente, é preciso situar que existe diferença entre requisição administrativa de dados cadastrais e requisição judicial. A primeira é aquela em que a autoridade policial e/ou o Ministério Público requisitam dados cadastrais de usuários/clientes aos provedores de conexão, de aplicação, dentre outros; a segunda, conforme o próprio nome já fala, é aquela em que há a autorização judicial para o fornecimento de dados de conexão, sendo esta mais invasiva no que concerne à privacidade de usuário, motivo pelo qual, há cláusula de reserva de jurisdição.

A respeito, dispõem os arts. 3º e 15 da Lei n. 12.850/13:

> Art. 3º Em qualquer fase da persecução penal, serão permitidos, sem prejuízo de outros já previstos em lei, os seguintes meios de obtenção da prova: [...]
> IV - *acesso a registros de ligações telefônicas e telemáticas, a dados cadastrais constantes de bancos de dados públicos ou privados e a informações eleitorais ou comerciais;*
> V - *interceptação de comunicações telefônicas e telemáticas*, nos termos da legislação específica; [...]
> Art. 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito. (grifo nosso).

Por seu turno, a Lei n. 9.613/98, que versa sobre lavagem de capitais, dispôs em seu art. 17-B sobre a requisição de dados cadastrais, de modo que a autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que

informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito.

O art. 13-A do Código de Processo Penal, incluído pela Lei n. 13.344/16, prevê a possibilidade de requisição de dados e informações cadastrais da vítima ou de suspeitos pelo membro do Ministério Público ou pelo delegado de polícia nos crimes previstos nos arts. 148, 149 e 149-A, no § 3º do art. 158 e no art. 159 do Código Penal, e no art. 239 da Lei n. 8.069/90 (Estatuto da Criança e do Adolescente).

O Marco Civil da Internet (Lei n. 12.965/14), em seu art. 10, §3º, atenta 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. [...] § 3º O disposto no caput *não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço,* na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição. (grifo nosso)

De acordo com a advertência de Jorge Figueiredo Júnior *et. al.* (2020, p. 125):

> A Lei do Marco Civil da Internet (Lei 12.965/14) ainda com mais propriedade é utilizada para subsidiar cautelar de afastamento de sigilo de Registro de Acesso a Aplicações de Internet. Deve ser destacado que a Lei 9.926/1996 (Lei de Interceptação Telefônica) ainda pode ser utilizada quando, em determinados casos, houver a necessidade da interceptação do fluxo de comunicações em sistemas de informática e telemática.

Conforme se tentou demonstrar, a Lei confere poderes-deveres às autoridades policiais e aos Ministérios Públicos, em sede de investigação criminal e/ou inteligência, possibilitando a requisição de dados cadastrais de usuários de diversos serviços, como, por exemplo, ISP – *Internet Service Provider* – provedores de serviço de internet, servidores de aplicação, empresas de telefonia e empresas privadas, requisições essas que não se confundem com requisições judiciais e se prestam à composição da prova para fins de persecução penal.

2.3 Barreiras ao fornecimento de dados telemáticos requisitados: caso Google, *Network Address Translation* (NAT) e portas lógicas

Realizar investigação criminal de crimes comuns no Brasil não é tarefa fácil, em caso

de crimes que envolvam alguma conduta delitiva por meio de computador, a tarefa se torna muitas vezes hercúlea. É comum, em diversas investigações comandadas pela polícia judiciária e pelo *Parquet*, em âmbito federal, distrital ou federal, que haja dificuldades de todas as espécies, quer por alguma limitação técnica e/ou de efetivo, quer por óbices legais.

Ocorre que a resposta aos crimes cometidos com emprego da tecnologia exige profissionais de polícia que dominem, no mínimo, essa mesma tecnologia, a ponto de estarem em condições técnicas de cometerem o mesmo crime objeto da investigação. Se não for assim, dificilmente a ação repressora logrará êxito em comprovar materialidade, autoria e circunstâncias do crime que possibilitem ao juiz decidir pela condenação do acusado e sentenciá-lo consoante à gravidade da conduta, à seriedade dos resultados e demais circunstâncias legalmente previstas (CERQUEIRA; ROCHA,2013, p.154 apud COSTA, 2021).

Em se tratando de práticas criminosas, afirma-se que a quebra e/ou interceptação de dados telemáticos não estão diretamente relacionadas ao uso de computadores ou algum aparelho celular. É plenamente possível que haja pedido formulado pelo *parquet* ou pela autoridade policial em desfavor de um investigado que tenha cometido algum crime de homicídio, por exemplo. Entretanto, há barreiras com as quais as autoridades precisam saber lidar. O primeiro exemplo disso é a famosa questão do endereçamento IP por meio de NAT (*Network Address Translation*) e portas lógicas. O NAT é uma técnica que é utilizada em virtude da escassez de endereços IP em todo o mundo, de modo que cada usuário usa o mesmo IP. Assim, pode ocorrer, por exemplo, de em determinada cidade cerca de um mil pessoas estarem compartilhando determinado endereço IP, inclusive com criminosos que estejam eventualmente praticando crimes. O problema se inicia justamente com o uso compartilhado de mesmo IP público. A solução mais aconselhável é o uso do IPv6[11] para a identificação e individualização de cada dispositvo conectado a alguma rede, implementando portas lógicas.

A técnica de NAT ocorre no âmbito das operações de roteamento da conexão de rede e, entre outras funções, acrescenta às comunicações uma função adicional ao endereço de IP, que é a atribuição de portas lógicas adicionais, também numeradas e adicionadas ao final do endereço para auxiliar na identificação da origem do pacote de dados quando dois dispositivos compartilharem um mesmo número de endereço IP (ARMAZENAMENTO DE PORTAS, 2019). As portas lógicas seriam o endereço de uma residência localizada em determinada rua. Elas são, no âmbito da Internet, um conjunto de protocolos que atuam de forma lógica com a finalidade de realizar a individualização do tráfego de dados que o usuário utiliza. O assunto

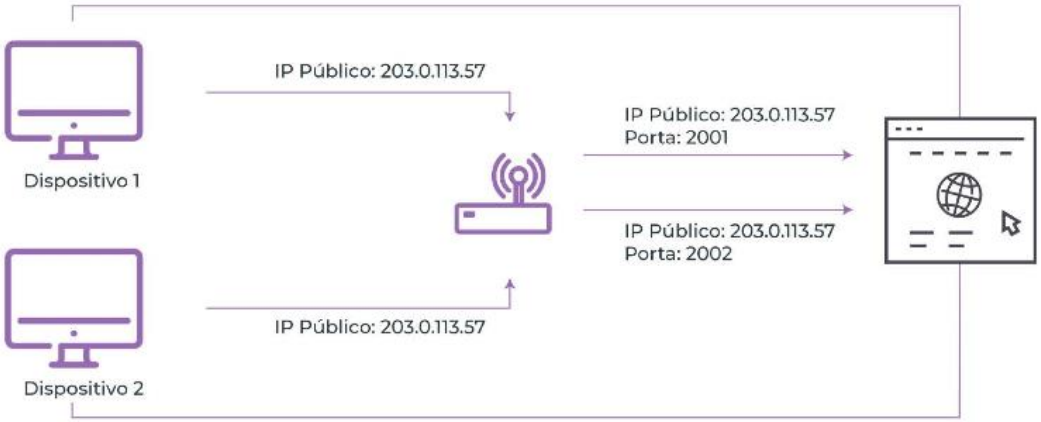
[11] IPv6: endereçamento IP versão 6.

foi extremamente debatido por diversos profissionais, de modo que chegou a ser judicializada a obrigação dos provedores de aplicação fornecerem estes dados, entre eles o Google. Neste sentido, decidiu a 6ª Turma do STJ, quando do julgamento do REsp n. 1784156/SP:

> [...] IDENTIFICAÇÃO DO DISPOSITIVO UTILIZADO PARA ACESSO À APLICAÇÃO. INDICAÇÃO DO ENDEREÇO IP E PORTA LÓGICA DE ORIGEM. [...] 1. O recurso especial debate a extensão de *obrigação do provedor de aplicações de guarda e fornecimento do endereço IP* de terceiro responsável pela disponibilização de conteúdo ilícito às informações *acerca da porta lógica de origem associada ao IP*. [...] 3. Cabe aos provedores de aplicações a manutenção dos registros dos dados de acesso à aplicação, entre os quais se inclui o endereço IP, nos termos dos arts. 15 combinado com o art. 5º, VIII, da Lei n. 12.965/2014, os quais poderão vir a ser fornecidos por meio de ordem judicial. 4. *A obrigatoriedade de fornecimento dos dados de acesso decorre da necessidade de balanceamento entre o direito à privacidade e o direito de terceiros, cujas esferas jurídicas tenham sido aviltadas, à identificação do autor da conduta ilícita*. 5. Os endereços de IP são os dados essenciais para identificação do dispositivo utilizado para acesso à internet e às aplicações. 6. *A versão 4 dos IPs (IPv4), em razão da expansão e do crescimento da internet, esgotou sua capacidade de utilização individualizada e se encontra em fase de transição para a versão 6 (IPv6), fase esta em que foi admitido o compartilhamento dos endereços IPv4 como solução temporária*.7. *Nessa fase de compartilhamento do IP, a individualização da navegação na internet passa a ser intrinsecamente dependente da porta lógica de origem, até a migração para o IPv6*. 8. *A revelação das portas lógicas de origem consubstancia simples desdobramento lógico do pedido de identificação do usuário por IP*. (BRASIL, 2019b) (grifos nossos).

Vejamos esquema simples sobre funcionamento das portas lógicas de origem e o uso do NAT para fazer uma análise com mais exatidão:

Imagem 2 – NAT e portas lógicas



Fonte: (ARMAZENAMENTO DE PORTAS..., 2021)

Outra barreira – dentre as várias a que os serviços de investigação brasileira estão sujeitos – é o fato de diversos servidores de aplicação estarem hospedados fora do país, prática que enseja muitos esforços técnicos e legais, os quais sua grande maioria não são atendidos.

Imagine-se uma situação hipotética em que usuários do Telegram estão compartilhando e comercializando dados de contas *fakes*, contas laranjas, clonagens de cartões de créditos e outras fraudes em determinado grupo para esta finalidade. Uma investigação é iniciada, seja por parte do MP, seja pela polícia judiciária.

Ao se coletar os dados necessários para se demandar a Justiça, verifica-se um grande problema: o responsável pelos dados dos usuários, neste caso, é o Telegram, o qual não está hospedado dentro do Brasil, ou seja, provavelmente Rússia, Estados Unidos, Emirados Árabes, dentre outras possíveis localizações. Com isso, torna-se muitas vezes impossível obter, com uso dos procedimentos legalmente previstos, os dados telemáticos essenciais para a investigação processual penal.

CAPÍTULO 3 – HACKEAMENTO COMO VIA TRANSVERSA DE OBTENÇÃO DE DADO INFORMÁTICO: A OPERAÇÃO *SPOOFING* E O CONFLITO AMPLA DEFESA X LICITUDE/INTEGRIDADE PROBATÓRIA

3.1 Operação *Spoofing*: exposição do caso

A Polícia Federal, em 21 de janeiro de 2019, deflagrou a "Operação Spoofing", motivo de agitação no cenário político e jurídico brasileiro, cuja principal finalidade era a de investigar invasões ocorridas em conta de Telegram do então Ministro da Justiça e Segurança Pública, Sérgio Moro.

Consta na denúncia às fls. 3-15, assinada pelo procurador da República Wellington Divino de Oliveira, do Ministério Público Federal – MPF, que Sérgio Moro "recebera três ligações no seu aparelho celular em que a identificação da chamada apresentava o mesmo número da linha que estava recebendo a ligação sendo que a primeira foi atendida e as duas posteriores foram ignoradas".

Após diligências realizadas, os investigadores chegaram às seguintes conclusões do que ocorrera:

> i) Antes de receber qualquer ligação, o telefone em questão recebeu duas mensagens SMS informando um código de verificação do aplicativo Telegram;
> ii) A primeira das chamadas cujo número de origem é omesmo do de destino foi transmitida para o telefone celular questionado e atendida (duração entre 6 e 7 segundos);
> iii) O telefone não registrou o recebimento da chamada cuja origem é o número 17147073350, tendo tal ligação sido encaminhada para a caixa de mensagens do celular. A partir de testes realizados pelos peritos, verificou-se o número 17147073350 é utilizado pelo aplicativo para informar o código de validação por meio de mensagem de voz. Provavelmente o redirecionamento da chamada se deu porque a linha telefônica do celular n. (41) 99944-4140 estava ocupada pela ligação recebida do próprio número. Ao ser redirecionado para a caixa de mensagens, o código informado por mensagem de voz teria sido gravado na caixa de mensagens, o que é evidenciado pela mensagem SMScom data de recebimento às 17:46:16 do dia 04/06/2019;
> iv) As três chamadas com número de origem igual ao número de destino, apesar de terem sido registradas no celular n. (41) 99944-4140, não foram atendidas, mas acabaram sendo direcionadas para a caixa de mensagens, etiveram duração de 7, 8 e 58 segundos, respectivamente. (DISTRITO FEDERAL, 2020)

Além da referida autoridade, outras tantas foram alvos da empreitada criminosa, conforme se verifica às fls. 6-7 da denúncia do MPF:

> Quando noticiada a invasão do aparelho celular do Sr. Ministro da Justiça, outras autoridades públicas denunciaram fatos semelhantes sendo, então, juntadas informações quanto às invasões perpetradas contra aparelhos celulares (*smartphones*) do Desembargador Federal Abel Gomes (TRF 2ª Região) e do Juiz Federal Flávio Lucas (18ª Vara Federal do Rio de Janeiro - Fls. 21/36), do Chefe da Delegacia da Polícia Federal de Campinas, DPF Edson Geraldo de Souza, e do Chefe do Núcleo de Inteligência daquela unidade, DPF Flávio Vieitez Reis (fls. 37/39), Delegado de Polícia Federal Rafael Fernandes, lotado na SR/PF/SP (Apenso I); Deputada Federal Joice Hasselmann (fl. 98); Ministro de Estado da Economia Paulo Guedes (fls. 188/194); Conselheiro do Conselho Nacional do Ministério Público (CNMP) Marcelo Weitzel (fls. 462/480); e Conselheiro do CNMP Sílvio Roberto de Oliveira de Amorim Júnior (518/520), sendo que os esforços investigativos acabaram unificados em um único inquérito policial. (DISTRITO FEDERAL, 2020)

Conforme está descrito na denúncia do MPF, às fls. 9, "em resumo, os denunciados utilizavam um sistema de telefonia IP para explorar uma brecha existente no sistema de telefonia móvel do país em conjunto com o sistema de ativação e recuperação de conta do aplicativo TELEGRAM".

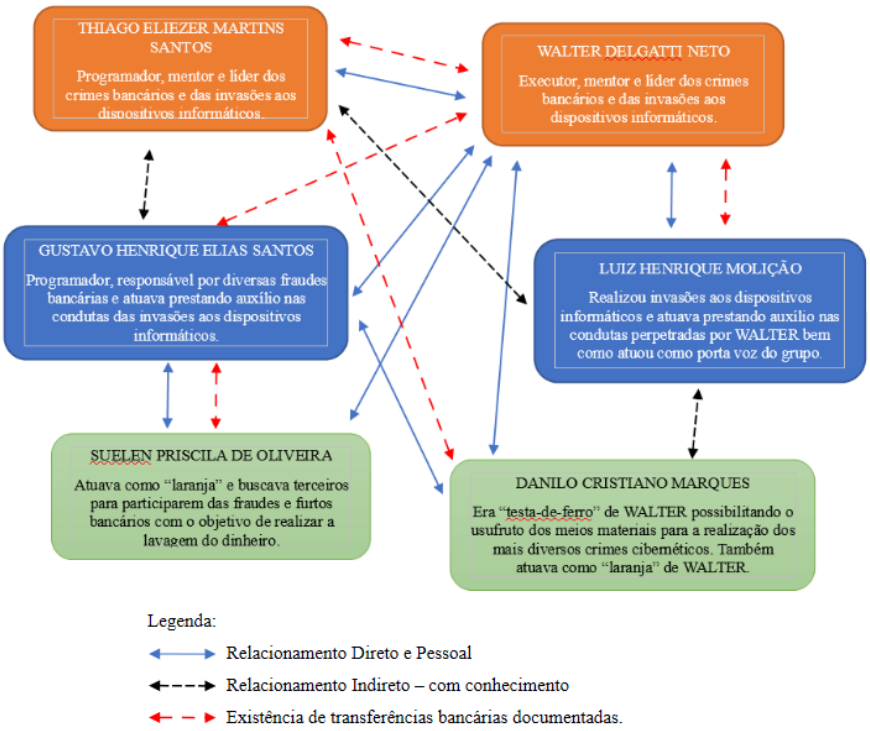
A técnica realizada por "hackers", resumidamente, funcionava da seguinte forma:

> 1. Obtenção do número de telefone do alvo a ser invadido.
> 2. Utilização de sistema VOIP (voz sobre IP) alterando o número de origem para o número de telefone do alvo a ser invadido (A=B).
> 3. Instalação do aplicativo Telegram no aparelho celular utilizado pela organização criminosa.
> 4. Solicitação de ativação do aplicativo Telegram para envio do código de acesso e ativação.
> 5. Nesse momento, quando solicitado o código de acesso, o invasor efetuava ligações para o número que estava sendo invadido de modo a manter a linha ocupada para que a ligação proveniente do aplicativo Telegram fosse redirecionada para a caixa-postal do cliente.
> 6. Ligação, via VOIP, para o número do alvo a ser invadido utilizando o "número de origem" igual ao "número de destino" (A=B) para acessar, de maneira direta, a caixa-postal em que estava registrado o código de acesso ao Telegram.
> 7. Ativar o aplicativo Telegram no celular invasor com o código obtido na caixapostal do cliente e baixar as mensagens salvas na "nuvem" ou realizar o monitoramento das conversas em tempo real. (DISTRITO FEDERAL, 2020)

Após todas as diligências investigativas por meio de autorização judicial de afastamento de sigilo telemático em relação às operadoras de telefonia, as provedores de serviço de voz por IP (ou VoIP), aqui no Brasil, Google, Apple, além de perícias realizadas em equipamentos apreendidos, foi possível chegar às seguintes pessoas e às práticas criminosas realizadas por elas: Walter Delgatti Netto e Thiago Eliezer Martins Santos, que atuavam como

mentores e líderes do grupo; Danilo Cristiano Marques, que era “testa-de-ferro” de Walter, proporcionando meios materiais para que o líder executasse os crimes; Gustavo Henrique Elias Santos, que era programador e desenvolveu técnicas que permitiram a invasão do Telegram e cometia fraudes bancárias; Suelen Oliveira, esposa de Gustavo, agia como laranja e “recrutava” nomes para participar dos ilícitos; e, por fim, Luiz Molição, que invadia terminais informáticos, aconselhava Walter sobre condutas que deveriam ser adotadas e foi porta-voz do grupo nas conversas com Glenn Greenwald, conforme organograma elencado na denúncia, fls. 4:

Imagem 4 – Organograma dos envolvidos



Fonte: (DISTRITO FEDERAL, 2020)

Frisa-se que o jornalista Glenn Greenwald também foi denunciado, embora não tenha sido indiciado pela Polícia Federal. O entendimento do MPF é que as provas coletadas na investigação demonstram que ele auxiliou, incentivou e orientou o grupo durante o período das invasões. No que se refere à responsabilização de Glenn Greenwald, o MPF ressalta que o jornalista não era alvo das investigações. A conduta foi adotada em respeito à medida cautelar proferida pelo ministro Gilmar Mendes, que proibiu apurações sobre a atuação do denunciado. Ocorre que, durante a análise de um MacBook apreendido - com autorização da Justiça - na casa de Walter Delgatti, foi encontrado um áudio de um diálogo entre Luiz Molição e Glenn.

Os envolvidos foram denunciados pelo MPF nos seguintes termos, fls. 94/95:

> • WALTER DELGATTI NETO seja condenado pela prática do crime no art. 10 da Lei n. 9.296/96 por 126 vezes e de 176 vezes pelas condutas tipificadas no art. 154-A, §3º com a causa de aumento de pena prevista no §5º, III e IV do Código Penal Brasileiro, nos termos do art. 69 do CPB;
> • THIAGO ELIEZER MARTINS SANTOS, LUIZ HENRIQUE MOLIÇÃO, GUSTAVO HENRIQUE ELIAS SANTOS, DANILO CRISTIANO MARQUES e GLENN EDWARD GREENWALD sejam condenados, nos termos do art. 29 do Código Penal Brasileiro, por praticarem, possibilitarem e concorrem para a consumação de 126 condutas tipificadas no art. 10 da Lei n. 9.296/96 e de 176 vezes pelas condutas tipificadas no art. 154-A, §3º com a causa de aumento de pena prevista no §5º, III e IV do Código Penal Brasileiro, nos termos do art. 69 do CPB;
> • GLENN EDWARD GREENWALD e LUIZ HENRIQUE MOLIÇÃO sejam condenados por associação criminosa nos termos do art. 288 do CPB;
> • WALTER DELGATTI NETO, THIAGO ELIEZER MARTINS SANTOS, GUSTAVO HENRIQUE ELIAS SANTOS, DANILO CRISTIANO MARQUES e SUELEN PRISCILA DE OLIVEIRA sejam condenados por integrarem organização criminosa nos termos do Art. 2º da Lei n. 12.850/2013;
> • WALTER DELGATTI NETO, THIAGO ELIEZER MARTINS SANTOS, LUIZ HENRIQUE MOLIÇÃO, GUSTAVO HENRIQUE ELIAS SANTOS, DANILO CRISTIANO MARQUES e SUELEN PRISCILA DE OLIVEIRA sejam condenados pelo crime de lavagem de dinheiro, previsto no art. 1º da Lei n. 9.613/1998. (DISTRITO FEDERAL, 2020)

É oportuno esclarecer que o nome da operação, "*Spoofing*", derivou do ataque conhecido na comunidade de hacking como "*Caller ID Spoofing*" (falsificação de identificadorde chamadas, em tradução livre). O termo "spoof" deriva do inglês e significa enganar. São vários os tipos de ataques virtuais de *spoofing*, como, por exemplo: de e-mail, de site, de identificador de chamada (*Caller ID*), de IP e de SMS, é tido como um ataque no qual um atacante engana sua vítima falseando seu endereço IP, seu número de telefone, como se fosse verdadeiro. É uma habilidade de que o criminoso se passar por pessoa conhecida, para avítima, em linhas gerais.

3.2 Invasão de dispositivo informático e sua tipificação no direito brasileiro

Neste tópico será realizado um apanhado geral da lei que tipifica o crime de invasão de dispositivo informático e correlatos.

A Lei n. 12.737/12, mais conhecida como "Lei Carolina Dieckman", dispõe sobre a tipificação criminal de delitos informáticos, altera o Código Penal, e dá outras providências. Ela trouxe algumas tipificações penais de crimes informáticos que, diga-se de passagem, são insuficientes para uma vastidão de possibilidades de conduta existentes. São eles: invasão de dispositivo informático (art. 154-A); interrupção ou perturbação de serviço telegráfico,

telefônico, informático, telemático ou de informação de utilidade pública (art. 266); falsificação de documento particular (art. 298) falsificação de cartão (art. 298, parágrafo único), todos incluídos no Código Penal.

Em que pese a lei acima trazer algumas tipificações sobre crimes informáticos, aqui, no Brasil, os crimes mais comuns na rede são o estelionato e a pornografia infantil. Os serviços de e-mails gratuitos são outro agente de expansão, pois seus dados não são necessariamente comprovados (v.g., Protonmail). Uma prática que poderia trazer resultados positivos seria ter legislação que obrigasse os provedores a identificar suas contas ativas e inativas, mediante uso de fotografia do usuário, ou seja, ter a comprovação de seus dados e, se possível, sua imagem digital. Isso, associado a uma prática de recadastramento dos usuários, no mesmo procedimento adotado pelos bancos, permite que realmente existam meios de prova confiáveis, rompendo-se a maior barreira à segurança na rede (PINHEIRO, 2013).

No entendimento de Damásio de Jesus e José Milagre (2016, p. 90),

> não temos um glossário na Lei n. 12.737/2012, o que pode gerar interpretações distintas para o termo“dispositivo informatizado”. Invadir é devassar, ato ou ação de acessar indevidamente, mas à força,irrupção. Entrar em certo lugar e ocupá-lo pela força ou tomar, conquistar, na linguagem técnica, ownar(tomar a propriedade) ou realizar um takeover. Na sociedade da informação, dispositivo informático étodo o dispositivo capaz de tratar informação, diga-se, armazenar ou processar dados (cálculo, alteração,inclusão ou exclusão).

Eis a tipificação penal, *verbis*:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput* .
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos

> dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

A norma penal disposta no art. 154-A foi inserida no Código Penal, no capítulo VI, que trata dos delitos contra a liberdade individual, seção IV, e dispõe sobre os crimes contra a inviolabilidade dos segredos. Esse crime foi "nomeado" como sendo invasão de dispositivo informático e, teoricamente, veio para tentar trazer inovações ao ordenamento jurídico brasileiro, em especial, o direito penal informático.

Spencer Toth Sydow (2020, p. 438) entende que o Brasil andou na contramão diante dos demais países, visto que eles criaram um tipo penal que inclui "intrusão" informática, mais abrangente, e não "invasão" informática, mais específica e com aplicabilidade reduzida. Entende ele, também, que o tipo penal é por demais confuso em sua redação.

Para Rogério Tadeu Romano (2019), trata-se de crime de ação múltipla, visto que envolve os núcleos do tipo: invadir (ingressar, acessar sem permissão) e instalar (copiar, realizar download, baixar ou salvar sem permissão) tendo como objeto material os dados e informações armazenadas bem como o próprio dispositivo informático da vítima que sofre a invasão ou a instalação de vulnerabilidades. Os doutrinadores entendem que é irrelevante se dispositivo está ou não conectado à rede interna ou externa de computadores, ou seja, internet ou intranet. É crime que se trata de tipo misto alternativo, onde o sujeito ativo responde por crime único se, no mesmo contexto fático, praticar uma ou as duas condutas típicas (invadir e instalar).

Rogério Tadeu Romano (2019) entende:

> O sujeito passivo é a pessoa que pode sofrer dano material ou moral em consequência da indevida obtenção, adulteração ou destruição de dados e informações em razão da invasão de dispositivo informático, ou decorrente da instalação no mesmo de vulnerabilidades para obter vantagem ilícita, seja seu titular ou até mesmo um terceiro. Invadir é violação indevida do mecanismo de segurança. A instalação pode ser feita para o delito por qualquer meio de execução existente. A invasão se dá em dispositivo alheio e sem autorização de seu possuidor. O elemento subjetivo é o dolo específico, na vontade consciente de invadir dispositivo alheio. Consuma-se, portanto, o delito no momento em que o agente invade o dispositivo informático da vítima, mediante violação indevida de mecanismo de segurança, ou instala no mesmo vulnerabilidades, tornando-o facilmente sujeito a violações.

Spencer Toth Sydow (2020, p. 467) alega que, quanto ao bem jurídico atingido, as figuras típicas do caput e a eles relacionadas são puras; para o parágrafo primeiro, o delito é classificado como impuro (porque é delito acessório ao caput). Quanto à quantidade de agentes, defende o autor, que todas as figuras podem ser classificadas como unissubjetivas pelo fato de não hão haver necessidade de concurso de agentes.

Damásio de Jesus e José Milagre (2016, p. 112) trazem uma questão importantíssima e nova, embora não tipificada e abarcada no Código Penal, que é o instituto da "legítima defesa informática":

> [...] Vítimas, pessoas físicas ou jurídicas, podem, em caso da detecção de um ataque em andamento, constituindo uma injusta agressão, buscar interromper o ataque, mas também apurar a autoria por meio de provas que podem ser produzidas em uma espécie de "contra-ataque" [...]. Uma empresa poderia acessar a conta de um servidor FTP (*File Transfer Protocol*) de um criminoso digital e lá apagar segredos ou informações sigilosas furtadas ou copiadas após a invasão, visando impedir a divulgação? Poderia acessar um e-mail descoberto na engenharia reversa de um código malicioso e lá obter informações sobre os crimes do atacante? Tais afirmações estão relacionadas a um conceito difundido na doutrina brasileira, denominado "legítima defesa informática". Segundo o inciso II do art. 23 do Código Penal, não há crime quando o agente pratica o fato em "legítima defesa". Entende-se, pois, em legítima defesa quem, usando moderadamente dos meios necessários, repele injusta agressão, atual e iminente, a direito seu ou de outrem. Logicamente, a defesa deve se valer de proporcionalidade e não pode servir de subterfúgio para ataques digitais ou exercício arbitrário das próprias razões. Tal instituto pode afastar a incidência do art.154-A do Código Penal, nos termos da Lei n. 12.737/2012, quando comprovado que a invasão, em resposta, deu-se de forma moderada, pela vítima ou equipe de segurança ou resposta a incidentes, que desenvolveu um protocolo de Ethical Hacking, para garantir direitos ou prevenir responsabilidades. Segundo Crespo (2011, p. 114), acerca da moderação da legítima defesa informática, "mas não se podem generalizar condutas. Se alguém lhe enviar um spam, você não pode responder com um vírus". *Parte da doutrina aceita a legítima defesa informática também nos casos em que o agente produz uma prova ilícita ou ilegítima (como a produzida mediante invasão de computador ou dispositivo informático), porém, para demonstrar sua inocência em face do Estado diante de uma persecução criminal e do princípio da verdade real.* Tais institutos, *embora teorizados, não se manifestam constantemente em casos no Brasil, porém poderão ser ventilados mais constantemente, com a aprovação da Lei n. 12.737/2012. Deste modo, a resposta ativa a um incidente poderá não ser criminalizada, se enquadrar-se no contexto da legítima defesa, esta que deverá ser comprovada pela perícia, que deverá apurar se foram utilizados os meios eficazes e suficientes para repelir a injusta agressão (ataque). [...]* (grifos nossos).

3.3 Licitude e autenticidade probatória: o problema da obtenção e do conteúdo da prova telemática por vias transversas

Quando se fala em direito probatório, imediatamente vem à cabeça sobre provas, principalmente, o que está previsto na Constituição Federal e no Código de Processo Penal, em se tratando de matéria penal. A respeito do assunto, vale destacar que existem diversos julgados dos tribunais superiores, em especial, sobre provas e, especialmente, sobre aquelas provas derivadas das ilícitas.

Antes de discorrer sobre a ilicitude de provas, é preciso trazer importante lição do mestre Edilson Mougenot (2019), para quem a prova é o instrumento usado pelos sujeitos processuais para realizar a comprovação de fatos da causa, ou seja, "aquelas alegações que são deduzidas pelas partes como fundamento para o exercício da tutela jurisdicional". Ainda, a prova tem como finalidade permitir que o julgador conheça os fatos sobre os quais fará incidir o Direito.

O Código de Processo Penal elenca, a partir do capítulo II, algumas espécies de provas, não em rol taxativo, porque outras podem existir no ordenamento jurídico e serem consideradas pelo juiz quando de sua análise, dado o princípio do livre convencimento motivado do juiz (ou sistema de persuasão racional, adotado de forma majoritária pelo processo penal brasileiro). Assim se pronunciou o STF acerca desse princípio/sistema:

> Em observância aos princípios da congruência e do *livre convencimento motivado do juiz*, a decisão proferida em processo de *caráter subjetivo é construída a partir dos argumentos e pedidos expendidos naqueles autos e está fundamentada nas provas nele produzidas*, a fim de oferecer a solução mais adequada ao caso concreto submetido à análise, respeitados os limites do ordenamento jurídico pátrio vigente, razão pela qual não vincula o relator em processo com limites subjetivos e objetivos distintos dos de referência" (BRASIL, 2016). (grifos nossos).

É preciso levar em consideração que quando se trata de provas, deve-se ter cuidado quanto às provas ilícitas. A Constituição Federal dispõe, no art. 5º, LVI, CF, que são inadmissíveis, no processo, as provas obtidas por meios ilícitos. No processo penal, por sua vez, há capítulo específico no que concerne às provas, de modo que o juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas.

Não são admitidas, devendo ser desentranhadas do processo, as provas ilícitas, assim

entendidas as obtidas em violação a normas constitucionais ou legais, inteligência do art. 157 do Código de Processo Penal. O codex em epígrafe, ainda, traz que são também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras.

O grande mestre Edilson Mougenot (2019, p. 108), assim se posiciona quanto às provas ilícitas e as suas derivadas:

> O princípio constitui, em verdade, uma vedação a que o juízo adote, como elemento de convencimento no curso do processo penal, elementos de prova obtidos por meios considerados ilícitos. O valor "justiça" não é absoluto, mas relativo [...] Provas obtidas por meios ilegítimos, portanto, não devem influir na formação do convencimento do juiz.

Frisa-se que, em que pese a Constituição Federal e/ou o Código de Processo Penal nãotratar diretamente sobre provas telemáticas, ela está prevista, conforme já bem delineado, na Lei nº 9.296/96, Lei de Interceptação Telefônica, como meio de prova. Nas palavras objetivas de Guilherme de Souza Nucci (2020, p. 599), meios de provas:

> [...] são todos os recursos, diretos ou indiretos, utilizados para alcançar a verdade dos fatos no processo. Na lição de Clariá Olmedo, é o método ou procedimento pelo qual chegam ao espírito do julgador os elementos probatórios, que geram um conhecimento certo ou provável a respeito de um objeto do fato criminoso (Tratado de derecho procesal penal, v. 1, p. 448). Os meios de prova podem ser lícitos – que são admitidos pelo ordenamento jurídico – ou ilícitos – contrários ao ordenamento. Somente os primeiros devem ser levados em conta pelo juiz. Em relação aos meios ilícitos, é preciso destacar que eles abrangem não somente os que forem expressamente proibidos por lei, mas também os imorais, antiéticos, atentatórios à dignidade e à liberdade da pessoa humana e aos bons costumes, bem como os contrários aos princípios gerais de direito.

Pensando precisamente nas provas a que este trabalho se dedica, quais sejam as telemáticas, retoma-se que são aquelas que podem ser obtidas, com fundamento na Constituição Federal, Código de Processo Penal, e Lei n. 9.296/96, perante os diversos provedores de aplicação, de uma forma geral. Assim, podem ser obtidas através de uma quebra telemática ou interceptação telemática de uma conta de e-mail cujo alvo tem cadastro na Microsoft, Google Drive, iCloud, WhatsApp, Telegram ou outras.

Claro que as provas devem ser produzidas em juízo e respeitando-se o princípio da comunhão das provas, isto é, significa "que a prova, ainda que produzida por iniciativa de uma das partes, pertence ao processo e pode ser utilizada por todos os participantes da relação

processual, destinando-se a apurar a verdade dos fatos alegados e contribuindo para o correto deslinde da causa pelo juiz" (NUCCI, 2020, p. 596).

É preciso salientar, no entanto, que podem existir hipóteses de uma quebra telemática que eventualmente foi obtida por meios inidôneos, ou seja, por via transversal, exemplo disso são as os elementos conseguidos pelos supostos hackers no âmbito da Operação *Spoofing*, notamente com violação ao fluxo de comunicações de dados, e invasão de dispositivos informáticos, além do conteúdo oriundo das mensagens/arquivos angariados. Neste caso, o conflito que pode surgir advém do questionamento sobre a possibilidade de utilização destas provas ilícitas para fins de defesa, eis que embora a vedação de provas ilícitas decorra de previsão constitucional, também o decorre o princípio da presunção da inocência, que traz como consequência o reconhecimento de que o réu pode provar, por qualquer meio, sua inocência.

3.4 Direito de defesa: possibilidade ou não da limitação do acesso a dado informático obtido ilicitamente

No tópico acima tratou, em apertada síntese, acerca do regramento das provas e sua inadmissibilidade, se ilícitas, na Constituição Federal e no Código de Processo Penal. Obviamente que, em termos de legislação, não se esgotam apenas nos dois citados.

De um lado se vê autoridades públicas tendo seus dados devassados por acessos e violações do fluxo de comunicações de dados em virtude de ataques a dispositivos informáticos; de outro, no entanto, há imediata reação da defesa – seja ela qual e de quem for – no sentido a possibilidade do uso de dados telemáticos (informáticos) obtidos ilicitamente.

Há grande debate jurídico sobre a temática. Todavia, ainda que possa causar estranheza, não é raro achar julgado no sentido de possibilidade do uso dos dados originários de fontes ilícitas. Questiona-se: existe a possibilidade de uso desses dados por parte da defesa?

A resposta é positiva e trazida e defendida pelos doutrinadores Eugênio Pacelli e Douglas Fischer (2020, p. 1007-1008):

> A inadmissibilidade da prova ilícita, para além de configurar uma opção ética do Estado, a incentivar a observância das regras jurídicas, surge como um verdadeiro reforço na proteção de tais direitos, invalidando quaisquer iniciativas abusivas por parte de quem deve submeter-se, com maiores razões, ao devido processo legal. Com tais considerações, poucas, mas suficientes, percebe-se *o inevitável paradoxo que resultaria da inadmissibilidade de uma prova ilícita que demonstrasse a inocência de alguém, indevidamente acusado*. Recusar-se-ia a prova com o objetivo de melhor tutelar o Direito (razão da norma constitucional), à custa, porém, da condenação de quem, pela

> qualidade de convencimento da prova, se julga inocente. Equação final: condenação do inocente para proteger direitos outros, como se o primeiro fosse inferior. Valeria aqui a objeção kantiana, segundo a qual "o homem é um fim em si mesmo, não podendo ser instrumentalizado a serviço do bem comum", não fosse a absoluta desnecessidade da aludida instrumentalização na hipótese de que se cuida, já que aberta a via para a condenação do verdadeiro culpado. [...] Então, por quaisquer razões que se entender de direito, seja ao nível de uma principiologia explícita, como a da ampla defesa, seja por considerações em níveis mais abstratos, como a do Estado Democrático de Direto, *não há como recusar a prova ilícita em favor do acusado.* (grifos nossos)

Prova ilícita, para os renomados autores citados acima, é aquela "obtida, produzida, introduzida ou valorada de modo contrário à determinada ou específica previsão legal" (PACELLI; FISHER, 2020, p. 1007-1008). No mais, refere-se à ilicitude que "[...] surgiria nas fases essenciais do aparecimento da prova no processo penal, a saber: (a) a da sua obtenção; (b) a da sua produção; (c) a da sua introdução no processo; e, por fim, (d) a da sua valoração pelo juiz da causa".

> A idoneidade probatória ou de convencimento de uma prova nem sempre dependerá de sua validade. *A prova poderá ser ilícita, ainda que comprovadamente eficaz quanto à reprodução de veracidade dos fatos* (gravações ambientais etc.). *A ilicitude da prova e sua inadmissibilidade decorrem de uma opção constitucional perfeitamente justificada em um contexto democrático de um Estado de Direito.* A afirmação dos direitos fundamentais, característica essencial de tal modalidade política de Estado, exige a proibição de excesso, tanto na produção de leis quanto na sua aplicação. Não se pode buscar a verdade dos fatos a qualquer custo, até porque, diante da falibilidade e precariedade do conhecimento humano a que aqui já nos referimos, no final de tudo o que poderá restar será apenas o custo a ser pago pela violação dos direitos, quando da busca desenfreada e sem controle da prova de uma inatingível verdade real. Daí a *inadmissibilidade da prova ilícita, à maneira das exclusionary rules do direito estadunidense* (grifos nossos). (PACELLI; FISCHER, 2020, p. 1007-1008).

Ensina Douglas Fischer (2021) que a "Prova" (elemento probatório) obtida de maneira ilícita, para a correta validação e valorização por parte da defesa, deve trazer, previamente, a segurança por meio da aferição de integridade: "É dizer, não pode ser uma prova imprestável, se não for possível aferir a sua autenticidade (não alteração), mesmo que, do modo como obtida, seja tecnicamente considerada uma prova ilícita". Neste sentido, é o recente posicionamento do STF, sobre o assunto em comento, em ação ajuizada com o propósito de impedir o uso das provas originárias de hackeamento de dispositivo informático para fins probatórios nos processos judiciais que tramitam contra o ex-presidente Luís Inácio Lula da Silva:

> As decisões contra as quais se insurgem os peticionantes apenas autorizaram, fundadas no direito constitucional – em verdade, universal – à ampla defesa e ao contraditório, o acesso a conteúdos apreendidos na Operação Spoofing relacionados, direta ou indiretamente, ao reclamante, sob rigoroso acompanhamento da Polícia Federal, que detém a sua custódia, com evidente exclusão de conversas privadas. *Já a questão relativa à autenticidade ou ao valor probatório* de elementos colhidos pela defesa é tema a ser resolvido no bojo dos processos nos quais venham a ser juntados, mas não nesta reclamação, sabidamente de estreitos limites, como, de resto, há pouco decidi nos presentes autos (documento eletrônico 198). (BRASIL, 2021)

Isto posto, levando-se em consideração o que a doutrina de Eugêncio Pacelli e Douglas Fischer, consubstanciado no voto do Min. Ricardo Levandowski, do STF, em sede da Reclamação n. 43.007/DF, é possível que haja o uso de provas ilícitas por parte das defesas, no entanto, desde que em sua totalidade, e não apenas excertos de mensagens ou provas, em especial quando há dúvida quanto à integridade e autenticidade delas.

Estas violações à autenticidade e integridade das mensagens e do conteúdo angariado e tido como provas, por exemplo, trazem outras implicações graves: quebra da manutenção da cadeia de custódia trazida pelo Pacote Anticrime, Lei n. 13.964/19, no art. 158-A, CPP. Ela é, resumidamente, nada mais do que a preservação e o registro da rastreabilidade da prova, é dizer, o seu caminho, desde a coleta até a sua preservação pelo Judiciário (PACELLI, FISCHER, 2020).

Nesta senda, o STJ, muito recentemente, entendeu que as informações veiculadas pelo portal *The Intercept* foram obtidas por meios ilícitos em violação ao direito à privacidade ao sigilo das comunicações telefônicas e de dados, nos termos do art. 5º, X e XII, CF, e "não foram submetidas a nenhuma perícia ou averiguação no curso de processo judicial, *sob a égide do contraditório.* Não demonstradas a sua idoneidade, integridade e veracidade, *portanto, não se prestam a sustentar as conclusões que o Embargante busca conferir* […]" (BRASIL, 2021) (grifamos).

Por fim, em recente posicionamento acerca do caso que envolve a Operação Spoofing, o Min. Humberto Martins, presidente do STJ, defendeu o que ele caracterizou como "dever institucional de autodefesa" do Judiciário, o que justifica o uso eventual de provas ilícitas para deflagrar investigações contra os procuradores da Lava-Jato (PRESIDENTE DO STJ.., 2021)

CONSIDERAÇÕES FINAIS

Pretendeu-se com este trabalho chamar atenção do leitor para os meios de investigação que até pouco tempo atrás não faziam parte do cotidiano das atividades investigativas, trazendo as definições jurídicas e técnicas sobre o afastamento de sigilo de dados telemáticos e interceptação telemática, além de expor sobre os procedimentos de requisição administrativa, pela Polícia Judiciária ou Ministério Público.

Em um passado não tão distante, as diversas modalidades de crimes eram investigadas apenas por meio do uso da interceptação telefônica, tida como o melhor meio de obtenção de prova; agora, no entanto, com a evolução da tecnologia e a quantidade maciça de pessoas usando dispositivos conectados à Internet, verificam-se pontos positivos e negativos para a atividade investigativa.

Por meio do lado positivo, facilita-se o trabalho por ser possível obter uma variedade de dados que os disponíveis pela via da interceptação telefônica, os quais são muitas vezes de grande interesse da investigação promovida pela Polícia Judiciária e/ou do Ministério Público brasileiro: dados de localização, de conexão com a Internet, endereçamento IP, portas lógicas, entre outros.

Por outro, dificulta-se o trabalho de investigação porque boa parte dos serviços oferecidos pelos provedores de aplicação aqui no Brasil são estrangeiros, com seus data centers localizados em diversos países, o que ocasiona obstáculos aos investigadores para conseguirem dados de usuários investigados, seja por meio de decisão judicial, seja por meio de Acordo de Cooperação Mútua Internacional em matéria penal (MLAT). Sendo este acordo um processo extremamente moroso e burocrático, tanto por parte do Brasil, quanto por outros países que fazem parte deste acordo, dada às peculiaridades legais ou costumeiras de cada nação.

A única lei brasileira que trata, especificamente, sobre o fornecimento de dados por parte dos provedores de aplicação aqui no brasil é o Marco Civil da Internet, Lei n. 12.965/2014, mas tem se mostrado insuficiente para resolver os óbices rotineiros no que concerne à atividade investigativa.

Paralelamente aos meios de se investigar atuais e eficientes por meio do afastamento de sigilo e interceptação telemática, de forma legal, ganham cenário e espaço no ordenamento jurídico brasileiro as formas ilícitas de obtenção de dados telemáticos, notadamente pelas práticas de invasão de dispositivo informático e hackeamento de contas, perfis de redes sociais, servidores de e-mails, aplicativos de trocas de mensagens etc.

A regra geral em matéria penal é que se deve obter as provas de maneira lícita

estritamente dentro dos ditames legais e valoradas pelo juiz do processo, garantindo o princípio da ampla e do contraditório (art. 5º, LV, CF) e do devido processo legal (art. 5º, LIV, CF) constitucionalmente assegurados.

Porém, o que se pôde analisar no presente estudo processual penal, jurisprudência dos tribunais superiores, doutrina e na prática da Operação *Spoofing* é o surgimento de provas a partir de dados telemáticos (quebra ou interceptação) cuja fonte é ilícita, bem como o seu uso por parte das defesas.

Restou evidenciado que as provas colacionadas por meios transversos, isto é, cuja consecução se deu por meios ilegais estão na dinâmica jurídica de serem aceitas desde que usadas pelas defesas, como já foi mencionado por trechos de alguns julgados do STJ e do STF, além, é claro do entendimento ministro presidente do STJ.

É preciso, no entanto, chamar a atenção que o entendimento doutrinário e jurisprudencial (ainda que timidamente) acerca da validade destas provas ilícitas é o de que elas, por si só, não devem ser aceitas. A exceção se dá quando há outros meios de comprovação e confirmação da autenticidade, integridade e integralidade dessas provas, e não apenas meros trechos de mensagens ou conversas esparsas oriundas de aplicativos de mensagens.

O raciocínio jurídico a despeito dessa temática é oportuno, atual e ainda não pacífico que ensejará diversos debates e argumentação jurídica pelas defesas de modo a tornar esta exceção uma opção mais aceita e viável no ordenamento jurídico brasileiro. Indagações, anulações de atos processuais ou até mesmo de processos ainda ocorrerão até que se consiga introduzir esta tendência jurídica para se fazer alguma Justiça. Merece destaque o raciocínio dos grandes mestres na seara penal e processual penal, Eugênio Pacelli e Douglas Fischer, de que não se pode limitar a possibilidade da defesa realizar seus atos por meio de provas ilícitas.

O direito é isto: é dinâmica, é conflito, é uma balança que por vezes haverá de ser equilibrada para que se faça a Justiça pleiteada.

REFERÊNCIAS

ARMAZENAMENTO DE PORTAS lógicas à luz do MCI. Disponível em: https://baptistaluz.com.br/institucional/a-discussao-sobre-armazenamento-de-portas-logicas-a-luz-do-mci. Acesso em: 20 abr. 2021.

ASSIS, José Francisco de. *Direito à privacidade no uso da internet: omissão da legislação vigente e violação ao princípio fundamental da privacidade*. Revista Âmbito Jurídico, 2015. Disponível em: http://www.ambito-juridico.com.br/site/n_link=revista_artigos_leitura&artigo_id=12848. Acesso em: 22 mar. 2021.

BASTOS, Celso Ribeiro. *Curso de direito constitucional*. 2. ed. São Paulo, 2000.

BRASIL. Supremo Tribunal Federal. Reclamação n. 43007/DF. Relator: Ricardo Levandowski. Brasília, 09 de fevereiro de 2021a.

BRASIL. Supremo Tribunal Federal. Plenário. Mandado de Segurança n. 23.452/RJ. Relator: Celso de Mello. Brasília, 16 de setembro de 1999.

BRASIL. Supremo Tribunal Federal. Agravo Regimental na Reclamação n. 23241/DF. Relator: Dias Toffoli. Brasília, 05 de abril de 2016.

BRASIL. Supremo Tribunal Federal. Pleno. *Habeas Corpus* n.72.588/PB. Relator: Maurício Corrêa. Brasília, 04 de agosto de 2000.

BRASIL. Supremo Tribunal Federal.1ª Turma. Habeas Corpus n. HC 87.341/PR. Relator: Eros Grau. Brasília, 03 de março de 2006a.

BRASIL. Supremo Tribunal Federal. STF. Plenário. *Recurso Extraordinário n. 583937 QO-RG*. Relator: Cezar Peluso. Brasília, 19 de novembro de 2009 (Repercussão Geral – Tema 237).

BRASIL. Supremo Tribunal Federal. *Recurso Especial n. 593.727/MG*. Relator: Gilmar Mendes. Brasília, 14 de maio de 2015.

BRASIL. Supremo Tribunal Federal. Plenário. *Ação Direta de Inconstitucionalidade n.1.488/DF*. Relator: Néri da Silveira. Brasília, 07 de novembro de 1996.

BRASIL. Supremo Tribunal Federal. Plenário. *Recurso Extraordinário n. 418.416/SC*. Relator: Sepúlveda Pertence. Brasília, 10 de maio de 2006b.

BRASIL. Superior Tribunal de Justiça. 5ª Turma. *Habeas Corpus n. 43.234/SP*. Relator: Gilson Dipp. Brasília, 03 de novembro de 2005b.

BRASIL. Superior Tribunal de Justiça. 3ª Turma. *Habeas Corpus n. 203.405/MS*. Relator: Sidnei Beneti. Brasília, 28 de junho de 2011a.

BRASIL. Superior Tribunal de Justiça. *Ofício n. 66/GP/STJ*. Instauração de pedido de providência contra Procuradores da República. Relator: Humberto Martins. Brasília, 05 de fevereiro de 2021a.

BRASIL. Superior Tribunal de Justiça. 1ª Seção. *Mandado de Segurança n. 17.815/DF*. Relatora: Regina Helena Costa. Brasília, 28 de novembro de 2018b.

BRASIL. Superior Tribunal de Justiça.6ª Turma. *Habeas Corpus n. 512.290/RJ*. Relator: Rogério Schietti Cruz. Brasília, 18 de agosto de 2020.

BRASIL. Supremo Tribunal Federal. 1ª Turma. *Habeas Corpus n. 70814*. Relator: Celso de Mello. Brasília, 01 de março de 1994.

BRASIL. Supremo Tribunal Federal. 2ª Turma. *Agravo de Instrumento n. 541.265 AgR/SC*. Relator: Carlos Velloso. Brasília, 04 de outubro de 2005a.

BRASIL. Superior Tribunal de Justiça. *Embargos Declaratórios no Agravo Regimental no Recurso Especial n. 1.765.139/PR*. Relator: Félix Fischer. Brasília, 01 de setembro de 2020a.

BRASIL. Superior Tribunal de Justiça. 5ª Turma. *Embargos de Declaração nos Embargos de Declaração nos Embargos de Declaração no Agravo Regimental no Recurso Especial n. 1.765.139/PR*. Relator: Min. Felix Fischer. Brasília, 9 de fevereiro de 2021b.

BRASIL. Superior Tribunal de Justiça. *Recurso Especial n. 1795341/RS*. Relator: Nefi Cordeiro. Brasília, 07 de maio de 2019.

CAVALCANTE, Márcio André Lopes. *Interessante caso envolvendo infiltração policial, ação controlada, gravação ambiental e cooperação com agência de inteligência*. Dizer o Direito, 09 dez. 2020. Disponível em: https://www.dizerodireito.com.br/2020/12/interessante-caso-envolvendo.html. Acesso em: 20 mar. 2021.

CAVALCANTE, Márcio André Lopes. Ministério Público pode realizar diretamente a investigação de crimes. Dizer o Direito, 2021. Disponível em: https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/05a5cf06982ba7892ed2a6d38fe832d6. Acesso em: 06 abr. 2021

CASTRO, Ana Clara Camargo de; SYDOW, Spencer Toth. *Stalking e cyberstalking: obsessão, internet, amendrontamento.* Belo Horizonte: Editora D´Plácido, 2017. (Coleção Cybercrimes)

COSTA, Thabata Filizolla. *Os desafios para investigação de crimes digitais*. Disponível em: https://thabatafc.jusbrasil.com.br/artigos/351838651/desafios-para-a-investigacao-de-crimes-digitais. Acesso em: 06 abr. 2021.

CPICIBER. *Marco Civil da Internet*. Disponível em: https://cpiciber.codingrights.org/retencao-de-dados/#marco-civil-da-internet. Acesso em: 10 mar. 2021a.

CPICIBER. *Interceptação*. Disponível em: https://cpiciber.codingrights.org/interceptacao. Acesso em: 10 mar. 2021b.

DISTRITO FEDERAL. Denúncia no Processo n. JF-DF-1015706-59.2019.4.01.3400-INQ. Autor: Ministério Público Federal. Brasília, 20 de janeiro de 2020. Disponível em: http://www.mpf.mp.br/df/sala-de-imprensa/docs/denuncia-spoofing. Acesso em: 10 mar.

2021.

DOTTI, René Ariel. *Proteção da vida privada e liberdade de informação*. São Paulo: Revista dos Tribunais, 1980. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2359-56392017000300167. Acesso em: 15 mar. 2021.

FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados: o Direito à privacidade e os limites à função fiscalizadora do Estado.* Revista da Faculdade de Direito da USP, v.88, 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 12 abr. 2021.

FIGUEIREDO JÚNIOR, Jorge; et. al.. *Tecnologia Disruptiva e a Investigação Criminal [Tratado de Investigação Criminal Tecnológica]*. Salvador: Juspodvim, 2020.

FISCHER, Douglas. *Os limites do uso da prova ilícita produzida no curso da Operação Spoofing e o eventual crime de abuso de autoridade*. Disponível em: https://temasjuridicospdf.com/os-limites-do-uso-da-prova-ilicita-produzida-no-curso-da-operacao-spoofing-e-o-eventual-crime-de-abuso-de-autoridade/. Acesso em: 10 maio 2021.

FREITAS JÚNIOR, Adair Dias de; JORGE, Higor Vinicius Nogueira; GARZELLA, Oleno Carlos Faria. *Manual de Interceptação Telefônica e Telemátia – Teoria, prática e legislação*. Salvador: Juspodivm, 2020.

GARCIA, Bruna Pinotti. Ética na Internet: um estudo da autodisciplina moral no ciberespaço e de seus reflexos jurídicos. Dissertação (Mestrado em Direito) – Programa de Mestrado em Direito, Fundação de Ensino "Eurípides Soares da Rocha", mantenedora do Centro Universitário Eurípides de Marília, Marília, 2013.

GRECO FILHO, Vicente. *Interceptação Telefônica*. São Paulo, Saraiva, 1996.

GRINOVER, Ada Pellegrini. *O regime brasileiro das interceptações telefônicas*. Revista Forense, v. 338, 1999.

GOMES, Luiz Flávio; MACIEL, Silvio. *Interceptação Telefônica: comentários à Lei 9.296*. 4. ed. São Paulo: Editora Revista dos Tribunais, 2018.

JESUS, Damásio de; MILAGRE, José Antônio de. *Manual de crimes informáticos*. São Paulo: Saraiva, 2016.

JOBIM, Nelson. *Exposição de Motivos do PL n. 4/96*. Disponível em: https://www.ibccrim.org.br/noticias/exibir/1745/. Acesso em: 20 mar. 2021.

LENZA, Pedro. *Direito Constitucional Esquematizado*. 24. ed. São Paulo: Saraiva, 2020.

LIMA, Renato Brasileiro de. *Nova Lei de Abuso de Autoridade*. Salvador: Juspodivm, 2020a.

LIMA, Renato Brasileiro de. *Manual de processo penal: volume único*. *8. ed.* Salvador: JusPodivm, 2020b.

MAGALHÃES, Marcus Abreu de; SYDOW, Spencer Toth. *Cyberterrorismo: a nova era da criminalidade [Coleção Cybercrimes]*. Belo Horizonte: Editora D´Plácido, 2018.

MASSO, Fabiano Del; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio. *Marco Civil da Internet – Lei 12.965/2014*. São Paulo: Revista dos Tribunais, 2014.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional*. 10. ed. São Paulo: Saraiva, 2015.

MOUGENOT, Ednilson. *Curso de processo penal*. 13. ed. São Paulo: Saraiva Educação, 2019.

MORAES, Alexandre de. *Direito Constitucional*. 33. ed. São Paulo: Atlas, 2017.

NUCCI, Guilherme de Souza. *Código de Processo Penal Comentado.* 19. ed. Rio de Janeiro: Editora Forense, 2020.

PACELLI, Eugênio; FISCHER, Douglas. *Comentários ao Código de Processo Penal* e *sua jurisprudência*. 9. ed. São Paulo: Atlas, 2020.
Presidente do STJ defende o uso de mensagens hackeadas contra Lava-Jato. Disponível em: https://www.cartacapital.com.br/cartaexpressa/presidente-do-stj-defende-uso-das-conversas-hackeadas-contra-lava-jato.Acesso em: 10 mai. 2021.

PAESANI, Liliana Minardi. *Direito e internet: liberdade de informação, privacidade e responsabilidade civil*. 7. ed. São Paulo: Atlas, 2014.

PINHEIRO, Patrícia Peck. *Direito digital*. 5. ed. São Paulo: Saraiva, 2013.

PRESIDENTE DO STJ defende o uso de mensagens hackeadas contra Lava-Jato. Disponível em: https://www.cartacapital.com.br/cartaexpressa/presidente-do-stj-defende-uso-das-conversas-hackeadas-contra-lava-jato. Acesso em: 10 maio 2021.

ROMANO, Rogério Tadeu. *O art. 154-A do Código Penal*. Jus, jun. 2019. Disponível em: https://jus.com.br/artigos/74654/o-art-154-a-do-codigo-penal. Acesso em: 11 maio 2021

SAFERNET. *Cyberstalking.* Disponível em: https://new.safernet.org.br/content/ciberstalking#. Acesso em: 03 abr. 2021.

SILVA, Ricardo Sidi Machado da. *A interceptação das comunicações telemáticas no processo penal*. Tese (Doutorado em Direito) – Universidade de São Paulo, São Paulo, 2014.

STJ É VÍTIMA de ransonware e tem seus dados e backups criptografados. Disponível em: https://thehack.com.br/stj-e-vitima-de-ransomware-e-tem-seus-dados-e-os-backups-criptografados/. Acesso em 01 abr. 2021.

STRECK, Lenio Luiz. *As interceptações telefônicas e os direitos fundamentais*. Porto Alegre: Livraria do Advogado, 1997.

SYDOW, Spencer Toth. *Curso de Direito Penal Informático – Parte Geral e Especial*. Salvador: Juspodivm, 2020.

SYDOW, Spencer Toth. *Crimes Informáticos e Suas Vítimas*. 2. ed. São Paulo: Saraiva, 2015.

TAVARES, André Ramos. *Curso de Direito Constitucional*. 18. ed. São Paulo: Saraiva Educação, 2020.

VIEIRA, Waleska Duque Estrada. *A privacidade no ambiente cibernético: direito fundamental do usuário.* Revista da EMESC, v. 24, n. 30, 2017. Disponível em: https://revista.esmesc.org.br/re/article/view/167.Acesso em: 24 mar. 2021.