UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

FACULDADE DE DIREITO

DEPARTAMENTO DE CIÊNCIAS PENAIS

Gustavo Terra Stangler

PROJETO DE LEI N.º 4.939/2020: REFLEXÕES ACERCA DOS NOVOS MÉTODOS DE OBTENÇÃO DE PROVA TELEMÁTICA EM MEIO A ERA DA CRIPTOGRAFIA

Porto Alegre

2023

GUSTAVO TERRA STANGLER

PROJETO DE LEI N.º 4.939/2020: REFLEXÕES ACERCA DOS NOVOS MÉTODOS DE OBTENÇÃO DE PROVA TELEMÁTICA EM MEIO A ERA DA CRIPTOGRAFIA

Trabalho de conclusão de curso de graduação apresentado ao Departamento de Ciências Penais da Faculdade de Direito do Rio Grande do Sul como requisito parcial para a obtenção do título de Bacharel(a) Ciências Jurídicas e Sociais.

Orientador: Prof. Dr. Pablo Rodrigo Alflen da Silva.

Porto Alegre

2023

Gustavo Terra Stangler

PROJETO DE LEI N.º 4.939/2020: REFLEXÕES ACERCA DOS NOVOS MÉTODOS DE OBTENÇÃO DE PROVA TELEMÁTICA EM MEIO A ERA DA CRIPTOGRAFIA

Trabalho de conclusão de curso de graduação apresentado a Faculdade de Direito da Universidade Federal do Rio Grande do Sul como requisito parcial para a obtenção do título de Bacharel(a) em Ciências Jurídicas e Sociais.

Aprovado em: 10 de abril de 2023.

BANCA EXAMINADORA

_____

Prof. Pablo Rodrigo Alflen da Silva (Orientador)

_____

Prof. Marcus Vinícius Aguiar Macedo

_____

Prof. Paulo Mário Canabarro Trois Neto

Ao meu pai, Alberto, e à minha mãe, Solange, por seus apoios incondicionais em minha vida.

“Matto è chi spera che nostra ragione, possa trascorrer la infinita via, che tiene una sustanza in tre persone.”

Dante Alighieri

RESUMO

A avaliação dos métodos de obtenção de provas no direito processual penal deve ser feita considerando os direitos fundamentais estabelecidos no ordenamento jurídico nacional. Isso porque a utilização destes métodos de prova pode vir a entrar em conflito com direitos constitucionais, tal qual o direito à privacidade e à proteção da intimidade. Neste escopo, o presente trabalho tratará acerca dos procedimentos de obtenção de provas telemáticas em meio a era da criptografia ponta a ponta. Para isto, é abordado, primeiramente, questões tecnológicas inerentes ao recurso da criptografia, perpassando pelo microcosmo da era digital onde conhecer-se-á os conceitos, as estruturas e os agentes informáticos pertinentes às telecomunicações. Em seguida, ao examinar a legislação atual, contida na Lei n.º 9.296/96, as doutrinas apresentadas e as decisões jurisprudenciais, se traçará um paralelo com a proposta legislativa n.º 4.939/20, que se pretende um novo marco penal da internet ao oferecer minuciosas especificações de inúmeros meios de obtenção de provas cibernéticas.

Palavras-chave: Direito Processual Penal. Interceptação Telemática. Sigilo de Dados. Criptografia Ponta a Ponta. Meios de Obtenção de Prova.

ABSTRACT

The evaluation of methods for obtaining evidence in criminal procedural law must be conducted with due regard to the fundamental rights enshrined in the national legal system. This is because the employment of such methods of proof may potentially conflict with constitutional rights, such as the right to privacy and protection of intimacy. Within this purview, the present work will address the procedures for procuring telematic evidence in the era of end-to-end encryption. To this end, technological issues inherent to encryption will first be expounded, traversing the microcosm of the digital age, where one will acquire a comprehensive understanding of the concepts, structures, and pertinent computer agents for telecommunications. Subsequently, through an examination of the existing legislation contained in Law no. 9.296/96, the relevant doctrines and jurisprudential decisions, a comparison will be drawn with Legislative Proposal no. 4.939/20, which aims to provide a novel penal framework for the internet, outlining in detail numerous means of obtaining cyber evidence.

Keywords: Criminal Procedural Law. Electronic Eavesdropping. Data Confidentiality. End-to-End Encryption. Means of Evidence Collection.

LISTA DE ABREVIATURAS E SÍMBOLOS

3G – Third Generation Wireless

4G – Fourth-Generation Wireless

5G – Fifth-Generation Wireless

Art(s). – Artigo, Artigos

CDMA – Code Division Multiple Access

CPP – Código de Processo Penal

E2EE – End-to-end Encryption

EDGE – Enhanced Data rates for GSM Evolution

ERB – Estações Rádio Base

GSM – Global System for Mobile Communications 2G

GPRS – General Packet Radio Services

HC – Habeas Corpus

Inc. – Incorporated

SMS – Short Message Service

LGPD – Lei Geral de Proteção de Dados

LLC – Limited liability company

MCV – Marco Civil da Internet

PL – Projeto de Lei

RHC – Recurso em Habeas Corpus

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

SUMÁRIO

1 INTRODUÇÃO

Os inúmeros embates travados nos últimos anos – a começar por 2015, onde o aplicativo de mensagens WhatsApp teve seu bloqueio determinado judicialmente – trazem à tona a necessidade de se debater a respeito da possível, ou não, regulação de tais aplicativos no território brasileiro. Das mais variadas formas o Poder Judiciário viu-se obrigado a tomar as mais drásticas medidas para pressionar as novas empresas de tecnologia de meios de comunicação por mensagem a aceitarem suas determinações com fim possibilitar o procedimento investigatório da Polícia Judiciária e do Ministério Público e a devida instrução do processo penal.

A criptografia ponta a ponta tornou-se, neste sentido, grande obstáculo a ser vencido no âmbito das apurações cíveis e penais, com os mais diversos serviços negando poderem prestar assistência à Justiça com a justificativa da tecnologia empregada. Embora se apresente a essa questão uma necessidade de natureza regulatória destes meios de comunicação na legislação brasileira, pode-se, também, por meio da própria interpretação jurídica, vislumbrar algumas soluções frente ao já existente no ordenamento atual.

No tocante as discussões dentro dos julgares brasileiros, é demasiado comum o juiz se posicionar no sentido de que não há direito ou garantia absoluta na ordem jurídica brasileira, sendo qualquer que seja o direito ou garantia sempre passível de relativização. Neste aspecto, comum é ver os dizeres que o princípio da relativização tem o poder reexaminar o direito à privacidade e à intimidade, bem como o sigilo das comunicações e correspondências, e, desta forma, reconsiderar tais proteções constitucionais.

Assim, o presente trabalho tem por objetivo refletir acerca da prova telemática, ou digital, e seus meios de obtenção na ordem legal vigente. No primeiro capítulo dissertar-se-á a respeito do tipo de prova no processo penal – a prova telemática –, passando por assuntos introdutórios como conceito, alcance, tecnologias de comunicações e criptografia, ponderações acerca do direito constitucional ao sigilo e à aplicabilidade das leis já existentes no campo.

Já o segundo capítulo trará o panorama geral dos meios de obtenção legais de tais provas da legislação vigente, como a Lei n.º 9.296/96 e o Código de Processo Penal, e as compararão com o Projeto de Lei n.º 4.939/20, que persegue ser uma fundamental atualização dos métodos investigativos a idade digital. Desta maneira, analisar-se-á a busca e apreensão de dispositivos telemáticos de comunicação e de transmissão e dados, a coleta remota de comunicações e dados telemáticos em repouso acessados à distância, a interceptação telemática em transmissão e a controversa coleta por acesso forçado de sistema telemático.

Após isso, se discorrerá relativamente a admissibilidade da utilização de prova telemática ilícita, dissertando sobre a regra geral utilizada no sistema brasileiro, assim como suas exceções, traçando a evolução do direito das leis e das jurisprudências, analisando-se possíveis insuficiências, soluções e propostas para os impasses surgidos no âmbito da proposta legislativa.

2 PROVA TELEMÁTICA NO PROCESSO PENAL BRASILEIRO

2.1 Conceito, conteúdo e alcance da Prova Telemática

A prova telemática fora primeiramente recepcionada pelo ordenamento jurídico brasileiro por meio da Lei n.º 9.296, de 24 de julho de 1996, que veio dispor sobre a interceptação do fluxo de dados provenientes da infraestrutura de telecomunicações no Brasil com propósitos processuais e investigativos. A Lei das Interceptações Telefônicas, como é comumente chamada, trouxe ao processo penal brasileiro novas técnicas de investigação fruto do nascimento da era da informatização, como é, *e.g.*, o caso da interceptação e da escuta telefônica.

Nesta toada, a Lei tentou aglutinar em um só documento as necessidades de trinta anos atrás com fim de perscrutar inúmeros ilícitos que ocorriam no território brasileiro, ficando, a lei, conhecida por ser peça central na investigação de crimes como os de corrupção, de lavagem de dinheiro e de tráfico de drogas.

Embora mencionada no parágrafo único[1] do artigo 1º da Lei n.º 9.296/96, não evocou para expressão "telemática" um sentido claro, em que junto à expressão "telefônica" trouxe, talvez, um significado diverso para ambas as palavras.

O termo "telemático" tem sua origem no francês "télématique", que pode ser entendida, mais apropriadamente ao caso em questão, como a junção de "telecomunicação" com "informática", ou seja, unindo-se os serviços da telecomunicação, como serviços de telefonia, cabo, fibra óptica, ao que há de mais recente mundo da informática, como computadores, *softwares* e sistemas de rede[2].

Por conseguinte, entende-se ser telemático todo o conteúdo armazenado em forma de *bits* que se encontram em repouso em *hardwares* ou perpassam infraestruturas de telecomunicações, utilizando-se das mais variadas estruturas –

[1] Art. 1º. A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática. BRASIL, Lei n.º 9.296/96. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm.

[2] DORE, Eder. O que é Telemática? 16 de março de 2020. Disponível em: https://maplink.global/blog/o-que-e-telematica/.

cabos, torres e satélites – para o uso das mais diversas tecnologias – rádio, telefonia fixa, móvel e internet – disponíveis através de telefones fixos, *smartphones*, *tablets* e computadores. Telemático abraça, portanto, o sentido de telefônico, sendo uma palavra que abrange toda comunicação, ou não, realizada por aparelhos eletrônicos. Neste aspecto, Benjamin Rodrigues fala a respeito da definição de prova eletrônico-digital:

> Qualquer tipo de informação, com valor probatório, armazenada (em repositórios electrónicos-digitais de armazenamento) ou transmitida (em sistemas e redes informáticas ou rede de comunicações eletrônicas, privadas ou publicamente acessíveis, sob a forma binária ou digital.[3]

Assim, para os fins aqui pretendidos, o termo prova será utilizado em dois sentidos distintos, classificados por Nucci como espécies[4], que são tanto o meio, em que se utiliza os instrumentos elencados pela Lei n.º 9.296/96, como a interceptação telefônica, quanto o resultado dela extraído, a mídia e sua respectiva análise, para demonstrar a veracidade de um fato.

Todavia, é conveniente explicitar que a palavra prova possui uma dupla semântica a depender da etapa em que determinado elemento colhido encontra-se na esfera investigativa-processual. Alguns autores como Magalhães ressaltam que em fase anterior à exposição da prova ao contraditório, a melhor expressão técnica será a de elemento de prova. O elemento de prova é, desta feita, os dados objetivos apanhados que venha a confirmar, ou o contrário, se uma afirmação com relação a um fato de interesse à causa, sendo, à vista disso, o dado factual de teor meramente objetivo[5]. Por sua parte, após a judicialização, os elementos de prova expostos ao crivo do contraditório e demais processos intelectivos do magistrado os transformarão em resultado de prova[6].

---

[3] RODRIGUES, Benjamin Silva. Da prova penal: v. IV - Da prova-electrónico-digital e da criminalidade informático-digital. 1. ed. Lisboa: Rei dos Livros, 2011, p. 39.
[4] NUCCI, Guilherme de Souza. Prova no Processo Penal. 4. ed. Rio de Janeiro: Forense, 2015, n.p. *E-book*.
[5] GOMES FILHO, Antonio Magalhães. Estudos em Homenagem à Professora Ada Pellegrini Grinover: notas sobre a terminologia da prova (reflexos no processo penal brasileiro). 1. ed. São Paulo: DPJ, 2005, p. 307.
[6] *Ibidem*, p. 308.

Na acepção de prova colhido, o Projeto de Lei n.º 4.939, de 2020, que tramita no Congresso Nacional, traz em seu artigo 4º uma definição[7] semelhante à prova telemática, chamada desta vez de prova digital, que se fundamentará na ideia de informação armazenada ou transmitida no âmbito eletrônico que possua valor probatório.

Conclui-se, então, que a prova telemática, ou digital, compreenderá toda forma de conteúdo e informação colhida a partir dos mais diversos meios, seja de conversas telefônicas, troca de *e-mails*, conversas em aplicativos de mensagens, postagens em redes sociais ou conteúdos armazenados em qualquer tipo de estrutura para este fim.

2.2 Comunicações e dados telefônicos, informáticos e telemáticos

Na esfera das comunicações telemáticas, faz-se necessário citar a respeito das tecnologias e estruturas em uso dentro do sistema da telecomunicação brasileira. Como anteriormente dito, a hibridização dos sistemas de comunicação originou o vocábulo telemático a partir da junção de telefônico e informático. Nesta esteira, Ivan Jezler Costa Júnior resume bem o fenômeno da hibridização das telecomunicações:

> No fim dos anos 90, as operadoras de telefonia enfrentaram uma nova realidade – a necessidade de efetivarem uma junção entre comunicações e informática –, "saltando para o comboio em andamento da internet." Nos deparamos com uma nova tendência informacional de transmissão sincrética pela mesma infraestrutura de dados, voz e imagem, como as televisões digitais.[8]

Para melhor entendimento, subdividirá o subcapítulo em mais dois tópicos, um destinado a entender as pessoas jurídicas e naturais que compõem o conjunto de infraestruturas e estruturas das telecomunicações e, subsequentemente, descrever as tecnologias na nova era digital, em especial no uso das comunicações virtuais.

---

[7] Art. 4º. Considera-se prova digital toda informação armazenada ou transmitida em meio eletrônico que tenha valor probatório. BRASIL. Projeto de Lei n.º 4.939/20. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1936366&filename=PL%204939/2020.

[8] COSTA JÚNIOR, Ivan Jezler. Prova Penal Digital: Tempo, Risco e Busca Telemática. 1. ed. Florianópolis: Tirant lo Blanch, 2019, p. 25.

2.2.1 Estruturas e Pessoas Telecomunicações

Primeiramente, é indispensável mencionar os conceitos que permitem contemplar o abrangente funcionamento das estruturas de comunicações e de dados, sendo de crucial importância para que se possa entender, posteriormente, as tecnologias de comunicação telefônica e de dados em si. Para tanto, se aproveitará novamente das classificações surgidas a partir do artigo 7º do PL 4.939/20[9], em paralelo à doutrina de Marcel Leonardi, que veio a influenciar as classificações utilizadas no Marco Civil da Internet.

a) Provedores de Estrutura (Provedores de *Backbone*)

São as pessoas jurídicas proprietárias das redes que gerenciam o gigantesco volume do tráfego de informações que interligam as operadoras e servidores do mundo todo, sendo as proprietárias das mais variadas infraestruturas de comunicação como cabos, torres e satélites[10]. No Brasil tem-se a Empresa Brasileira de Telecomunicações, que atualmente uma subsidiária da Claro S.A, é uma das administradoras desta estrutura.

b) Provedores de Acesso (Provedores de Conexão)

São as pessoas jurídicas, que trabalham sob o regime de concessão pública, responsáveis pela implementação e manutenção de acesso à internet, por cabo ou *wireless*, aos demais usuários nacionais[11]. No Brasil há empresas conhecidas como NET Virtua e GVT, e as operadoras de telefonia móvel como Tim e Vivo. São mencionados, embora não conceituados, no Marco Civil da Internet.

---

[9] Art. 7º. Os provedores de infraestrutura, conexão e aplicação deverão manter, além das informações de guarda legal previstas em lei, os registros de dados necessários e suficientes para a individualização inequívoca dos usuários de seus serviços pelo prazo de 1 (um) ano. BRASIL. Projeto de Lei n.º 4.939/20.

[10] LEONARDI, Marcel. Responsabilidade Civil dos Provedores de Serviços de Internet. 1. ed. São Paulo: Editora Juarez de Oliveira, 2005, p. 20.

[11] *Ibidem*, p. 22.

c) Provedores de Aplicações da Internet

Conforme Frederico Ceroy, são empresas, organizações ou pessoas naturais que forneçam qualquer tipo de aplicações e funções dentro do espaço das redes[12]. Empresas de serviços de *e-mail*, aplicativos de mensagens e armazenamento em nuvem encontram-se nesta categoria. Esta forma de provedor também é referida e subdividida por Marcel Leonardi e pela Lei n.º 12.965/14 em três outras:

c.1) Provedores de Correio Eletrônico

São as pessoas jurídicas que oferecem os serviços de correio eletrônico que, por conseguinte, oferecerão as funcionalidades típicas do que se entende por *e-mail*, como endereço de webmail e espaço de armazenagem de conteúdo enviado e recebido[13]. Em destaque, no Brasil, estão o *Gmail*, da Google; *Outlook*, da Microsoft e *iCloud*, da Apple. Por vezes provedores de acesso à internet também oferecem seus próprios serviços de correio eletrônico, como exemplo a Uol e o Terra.

c.2) Provedores de Hospedagem (*Hosting Provider*)

São as pessoas jurídicas que garantem e oferecem o uso de seus servidores para prestação de serviços de armazenamento e compartilhamento de dados de todas as espécies[14]. Dentre segmentos conhecidos, estão os de armazenagem em nuvem – como *Google Drive*, da Google; *OneDrive*, da Microsoft e a *Dropbox* – e de hospedagem das demais aplicações que necessitam guardar dados, podendo ser websites, como *Wix* e *GoDaddy*.

c.3) Provedores de Informação

Toda pessoa natural ou jurídica que produz diretamente material para ser divulgado na internet por meio dos provedores de conteúdo, portanto são os criadores intelectuais da informação[15]. Neste aspecto, todo usuário das redes é um provedor de

[12] CEROY, Frederico Meinberg. Os conceitos de provedores no Marco Civil da Internet. 20 de setembro de 2020. Migalhas. Disponível em: https://www.migalhas.com.br/depeso/211753/os-conceitos-de-provedores-no-marco-civil-da-internet.
[13] LEONARDI, Marcel. Responsabilidade Civil dos Provedores de Serviços de Internet. 1. ed. São Paulo: Editora Juarez de Oliveira, 2005, p. 26.
[14] *Ibidem*, p. 27.
[15] *Ibidem*, p. 30.

informação, dentre bons exemplos da nova era estão os criadores em plataformas como YouTube, além de outras redes sociais como Facebook, Instagram, TikTok etc.

c.4) Provedores de Conteúdo

Toda pessoa natural ou jurídica que divulga na internet os conteúdos criados pelos provedores de informação[16], sendo, desta forma, as plataformas que permitem a divulgação, como as empresas YouTube, Facebook e até *blogs* particulares.

2.2.2 Tecnologias de comunicações de dados telefônicos, telemáticos e informáticos

O conjunto dessas camadas de provedores é permeado pelas tecnologias atuais predominantes nas redes de telecomunicações. Para o setor da telefonia móvel são utilizadas as chamadas tecnologias padrão de rádio de 2ª geração, como GSM, GPRS e EDGE que tem por intuito uma maior cobertura de recepção e emissão de sinal, via estações de rádio base, em detrimento de uma alta taxa de transmissão de dados[17]. Isto é, são tecnologias que possuem maior alcance face as de gerações posteriores, diferentemente das tecnologias de posterior geração. Tanto EDGE quanto GPRS são modernizações que tem por base o sistema GSM.

Ainda no Brasil, a empresa Vivo emprega o padrão CDMA[18], com tecnologia diversa das demais, mas também utilizada na troca de telefonemas e SMS. Até anos anteriores o método de cobrança da utilização das tecnologias GSM, assim como subsequentes, e CDMA dava-se por quantidade de ligações realizadas ou pela quantidade de SMS enviados.

Com o avanço técnico das últimas décadas, outros padrões começaram a ser lançados, o advento da terceira (3G), quarta (4G) e quinta (5G) gerações de redes móveis incorporaram, quase que indispensavelmente, sua ligação com a internet, que, ao contrário das anteriores, poderiam ou não perpassar pelo ambiente da rede

---

[16] *Ibidem*.
[17] SANTOS, Ricardo Di Lucia. Redes GSM, GPRS, EDGE e UMTS. UFRJ, 2008. Disponível em https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2008_2/ricardo/4.html.
[18] Redação Minha Operadora. Vivo religa sua rede CDMA. Minha Operadora, 22 de janeiro de 2013. Disponível em: https://www.minhaoperadora.com.br/2013/01/vivo-religa-sua-rede-cdma.html.

mundial de computadores. Todos os recursos anteriormente vistos são considerados como meios de acesso direto e indireto à internet, assim como outras vias como, por exemplo, as conexões discadas (*dial-up*), a banda larga, o *Wi-Fi* e via satélite[19].

Nota-se que todos estes padrões de telefonia são híbridos, podendo ou não serem usados paralelamente à internet, e são acolhidos implicitamente pela Lei n.º 9.472[20], de 1997, conhecida por Lei das Telecomunicações, e por ela disciplinadas e reguladas.

É, aliás, necessário saber que as tecnologias padrões de segunda e terceira gerações estão na iminência de seu desuso, uma vez que as de gerações posteriores já estão atingindo patamares de incrementação a ponto de que, em uma década, poderão cobrir todo o território nacional. Indo nessa revolução, algumas empresas, como a Claro, pretendem abandonar tais tecnologias ainda nesta década[21].

2.3 Inviolabilidade do sigilo de dados

A inviolabilidade ao sigilo de dados é tema de caráter constitucional, estando disposto no inciso XII[22] do artigo 5º da Constituição Federal Brasileira. Trata-se de garantia constitucional expressa junto a sua exceção.

Em seu decurso histórico, esta proteção jurídica evoluiu ao longo do tempo à medida que o uso de tecnologias e meios de coleta, armazenamento e compartilhamento de dados pessoais se tornaram mais modernos.

---

[19] RAMOS JUNIOR, Durval. Conheça os vários tipos de conexão. Tecmundo, 20 de janeiro de 2010. Disponível em: https://www.tecmundo.com.br/banda-larga/3489-conheca-os-varios-tipos-de-conexao.htm.

[20] BRASIL, Lei n.º 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm.

[21] GOGONI, Ronaldo. Os riscos da rede 2G e por que desligá-la não é tão simples. Meiobit, 2022. Disponível em https://meiobit.com/456885/redes-2g-ataques-desligamento-nada-simples/.

[22] Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. BRASIL. Constituição Federal de 1988. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

No Direito Internacional, tal garantia de resguardo do sigilo fora reconhecido em 1948 pela Declaração Universal de Direitos do Homem, em seu artigo 12[23]. Posteriormente, em 1981, o Conselho da Europa adotou em seu texto da Convenção n.º 108, a proteção no tratamento de dados em sistemas automatizados, trazendo consigo, a preocupação crescente com a privacidade e a proteção de dados pessoais perante a expansão irrefreável no uso de computadores e dispositivos eletrônicos.[24]

Desde então, muitos países adotaram leis de privacidade para proteger os dados pessoais de seus cidadãos, incluindo a União Europeia, culminando com a as disposições inseridas no Regulamento Geral sobre a Proteção de Dados, o Regulamento n.º 2016/679 da União Europeia, assinado em 2016.

No Brasil, a Lei Geral de Proteção de Dados, Lei n.º 13.709, de 14 de agosto de 2018, teve sua entrada em vigor o ano de 2020, tornando-se um dos mais avançados marcos regulatórios de proteção de dados pessoais em todo o mundo. A LGPD é aplicável a todas as empresas que coletam, armazenam ou tratam dados pessoais de cidadãos brasileiros, independentemente de sua localização geográfica. Nestes quesitos, também há nela expressa as mesmas garantias de defesa à privacidade e ao sigilo de dados, como escrito nos incisos I e IV[25] de seu art. 2º.

Como conceito, a inviolabilidade do sigilo de dados é uma garantia jurídica que protege a privacidade e a confidencialidade dos dados pessoais de uma pessoa. Ela significa que esses dados não podem ser coletados, armazenados, usados, divulgados ou compartilhados sem o consentimento da pessoa em questão ou sem uma base legal válida.

---

[23] Artigo 12°. Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei. ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos, 1948. Disponível em: https://www.oas.org/dil/port/1948%20Declaração%20Universal%20dos%20Direitos%20Humanos.pdf.

[24] Visa «garantir [...] a todas as pessoas singulares [...] o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal». EUROPA. Convenção n.º 108 do Conselho da Europa de 1981. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf.

[25] Art. 2º. A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; [...] IV - a inviolabilidade da intimidade, da honra e da imagem. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

De outro lado, para exceção prevista constitucionalmente ainda no mesmo inciso, o Min. Alexandre de Moraes sucintamente explica o caráter limitado que qualquer garantia ou direito, estando ele exposto a sua relativização:

> Os direitos e garantias fundamentais consagrados pela Constituição Federal, portanto, não são ilimitados, uma vez que encontram seus limites nos demais direitos igualmente consagrados pela Carta Magna (Princípio da relatividade ou convivência das liberdades públicas).[26]

Sendo, também, o exato entendimento por parte do Min. Celso de Mello, sintetizado dentro do julgamento da Mandado de Segurança n.º 23.452/RJ[27], diante o Tribunal Pleno, em 16 de setembro de 1999:

> 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, ainda que excepcionalmente, a adoção, por parte dos órgãos estatais, de medidas restritivas das prerrogativas individuais ou coletivas, desde que respeitados os termos estabelecidos pela própria Constituição. O estatuto constitucional das liberdades públicas, ao delinear o regime jurídico a que estas estão sujeitas - e considerado o substrato ético que as informa - permite que sobre elas incidam limitações de ordem jurídica, destinadas, de um lado, a proteger a integridade do interesse social e, de outro, a assegurar a coexistência harmoniosa das liberdades, pois nenhum direito ou garantia pode ser exercido em detrimento da ordem pública ou com desrespeito aos direitos e garantias de terceiros.

Desta forma, não resta dúvidas de que o afastamento do sigilo de dados de um indivíduo é conduzido pela Constituição Federal e têm reflexos, explícitos e implícitos, em toda a legislação que discorre sobre este tema. Para tal ponderação acerca da quebra de sigilo de dados, Marcelo Novelino nos evidência uma definição clara:

> A quebra do sigilo de dados consiste no acesso a informações privadas referentes a transações financeiras (dados bancários), ou prestadas ao fisco por contribuintes (dados fiscais), ou constantes dos registros das operadoras de telefonia (dados telefônicos) ou, ainda, contidas em arquivos eletrônicos (dados informáticos).[28]

Carece dizer que, igualmente, a inviolabilidade do sigilo de dados é de mesmo modo protegida pelo Marco Civil da Internet, a Lei n.º 12.965, de 2014, que estabelece

---

[26] MORAES, Alexandre de. Direito Constitucional. 24. ed. São Paulo: Editora Atlas, 2009, p. 32.
[27] BRASIL. Supremo Tribunal Federal. MS n.º 23.452/RJ. Rel. Min. Celso de Mello, julgado em 12/09/1999, DJ de 12/05/2000. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=85966.
[28] NOVELINO, Marcelo. Curso de Direito Constitucional. 11. ed. Salvador: JusPodivm, 2016, p. 340.

regras para o tratamento de dados pessoais e impõe penalidades para quem descumpri-las.

2.4 A Lei n.º 9.296/1996 e o Marco Civil da Internet

O Marco Civil da Internet, Lei n.º 12.965, de 2014, é a legislação que versa e regulamenta o ambiente da internet no país e estabelece princípios, garantias, direitos e deveres para o uso da rede. Os pontos basilares de sua redação incluem a proteção da privacidade dos usuários da internet, a liberdade de expressão, o direito à informação, o acesso à rede e a preservação da neutralidade da rede, distribuídos ao longo dos incisos I ao IV[29] do artigo 3º.

Em seu artigo 5º, fez muito bem o legislador no sentido de definir claramente alguns conceitos inclusos na redação, significando os termos “internet”, “terminal”, “endereço de IP”, “administrador de sistema autônomo”, “conexão à internet”, “registro de conexão”, “aplicações de internet e registros de acesso a aplicações na internet”, dispostos respectivamente de seu inciso I ao VIII[30].

No tocante a este trabalho, vê-se importante citar os demais artigos da Lei a qual referem-se aos direitos à privacidade e à proteção de dados. Em seu artigo 7º é mencionado que os usuários da internet terão assegurados sua intimidade e vida

[29] 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. BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Brasília, DF. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

[30] 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. *Ibidem*.

privada, inciso I, o seu sigilo no fluxo de comunicações no ambiente de rede, inciso II, bem como suas comunicações privadas nela armazenados, inciso III[31]. Este artigo tem por objetivo defender o cliente pelo prisma de seus direitos e garantias.

De imediato, a Lei visou em seus arts. 10 e 11[32] versar sobre os deveres dos provedores de internet, aquelas empresas que provêm o acesso à internet, para com seus usuários e para com o Estado brasileiro. Deverão tais provedores ter um registro mínimo como explanado em lei com os usuários, devendo tratar seus dados de maneira resguardarem o sigilo de seus clientes na medida que não proporcionem a anonimidade total em rede com o fim de, se necessário, prestar contas com o poder público assim que acionados.

Por seu turno, a Lei n.º 9.296, de 24 de julho de 1996, conhecida por Lei das Interceptações Telefônicas teve por objetivo especificar a exceção trazida pelo inciso XII do artigo 5º da Constituição Federal no que se refere a necessidade da quebra de sigilo dos dados em ocasiões que interessem nos âmbitos investigatório e processual penal. A lei em epígrafe ficou responsável por regrar, a título de exemplo, a medida de interceptação telefônica decorrente da medida de afastamento do sigilo dos dados.

A diferenciação tanto da quebra de sigilo de dados quanto da interceptação telefônica causa certa dificuldade. No sentido de distingui-las rapidamente, deve-se tratar o afastamento de sigilo como medida *lato sensu* que visa a relativização do direito à proteção do sigilo, buscando alcançar quaisquer conteúdos privados disponíveis para acesso em inúmeras instituições, podendo ser o sigilo bancário, fiscal, financeiro ou telemático. Já a interceptação telefônica é o meio de obtenção de prova específico que pode decorrer do afastamento do sigilo de dados.

---

[31] Art. 7º. O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial. *Ibidem*.

[32] 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. [...] Art. 11. 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, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. *Ibidem*.

Consequentemente, percebe-se ser a Lei n.º 9.296/96 um possível instrumento que abarque as exceções nítidas trazidas pelo próprio Marco Civil da Internet em suas ressalvas. Todavia ainda é incerto que a Lei das Interceptações abranja todas as novas funcionalidades oriundas dos novos tempos, tais como no caso de acesso aos conteúdos armazenados em *e-mails* e em nuvem.

Neste ponto, o Tribunal de Justiça do Distrito Federal e Territórios, ao julgar mandado de segurança de processo transitando ainda em segredo, exibiu em uma parte de sua ementa o entendimento de que os dados em repouso não são abrangidos pela Lei em questão, como diz o relator, o Des. João Timóteo de Oliveira: “os dados armazenados em nuvem não evidenciam uma comunicação de dados, mas representam o armazenamento de dados em um provedor de serviços na nuvem (*cloud storage*)”[33].

Em vista disso, percebe-se que ambas as leis terão papel complementar, em que a Lei de Interceptação Telefônica agirá sobre temas de natureza comunicativa e o Marco Civil da Internet *per si* oferecerá fundamentação suficiente e necessária em matéria de conteúdo e dados armazenados.

2.5 Comunicações e dados em aplicativos de comunicação

Face à miríade proporcionada perante os novos recursos de comunicação via rede mundial de computadores, é necessário referenciar algumas das hodiernas plataformas de serviços de transmissão de dados muito comuns na sociedade brasileira. Contudo, antes disso, vê-se indispensável buscar uma definição de dados para fins de melhor análise.

Em definição, dado significa qualquer tipo de informação cuja unidade é mensurada a partir de *bits* e é armazenada na memória de um *hardware* para este fim, no caso de qualquer aplicativo de mensagem, dados são todos os conteúdos ali

[33] DISTRITO FEDERAL. Dados em Nuvem - Inaplicabilidade da lei 9.296/96. 04 de fevereiro de 2021, TJDFT. Disponível em: https://www.tjdft.jus.br/consultas/jurisprudencia/decisoes-em-evidencia/4-2-2021-2013-dados-em-nuvem-2013-inaplicabilidade-da-lei-9-296-96-2013-tjdft.

trocados. Já o metadado é a informação que diz respeito à natureza do dado, como o tamanho, formato e horário em que ele foi processado[34].

Uma vez conceituada a unidade fundamental da informação, deve-se fazer um breve apanhado das aplicabilidades mais correntes na esfera informacional. São indispensáveis no cotidiano a utilização de serviços como *e-mails*, envio e recebimento de mensagens instantâneas, de redes sociais e de armazenamento de dados de forma remota, aplicações estas que compõem maior parte do que se entende por serviços de comunicação e armazenamento.

Os aplicativos de mensagens instantâneas têm papel preponderante na era digital, com eles atualmente é possível que dois usuários possam comunicar entre si através de mensagens de texto, imagens ou vídeos via *chats* privados. Não suficiente, tais programas contam com recursos como grupos – a qual três ou mais pessoas tem a possibilidade de escrever simultaneamente umas com as outras – bem como chamadas telefônicas e de videoconferências em tempo real para se conversarem.

O aplicativo *WhatsApp*, pertencente ao Grupo Meta, é o meio de comunicação mais utilizado pelo cidadão brasileiro[35], trazendo todas as aplicabilidades acima descritas com o benefício da criptografia ponta a ponta que os garante total privacidade cibernética. Em menor escala há outras plataformas de características próximas como o *Telegram* e o *Signal*. Há, igualmente, recursos semelhantes no âmbito das redes sociais, como é o caso do Messenger, introduzido dentro das plataformas do Facebook e Instagram.[36]

De outro lado, advinda de tecnologia bem anterior, encontram-se os serviços de *e-mail* – capitaneados no mercado brasileiro pelo *Gmail*, *Outlook* e *iCloud*, pertencentes, respectivamente, pela Google LLC, pela Microsoft Corporation e pela Apple Inc. Tais plataformas tem por objetivo oferecerem um sistema de correio

---

[34] CHAPPLE, Mike. *What Is Metadata?* ThoughtCo. 18 de novembro de 2021. Tradução nossa. Disponível em: https://www.thoughtco.com/metadata-definition-and-examples-1019177.
[35] LOUREIRO, Rodrigo. Pesquisa revela os aplicativos de mensagens mais utilizados no Brasil. Revista Exame, 04 de setembro de 2021. Disponível em: https://exame.com/tecnologia/pesquisa-revela-os-aplicativos-de-mensagens-mais-utilizados-no-brasil/.
[36] HESSE, Brendan. *The Best WhatsApp Alternatives*. LifeHacker, 07 de janeiro de 2021. Disponível em: https://lifehacker.com/the-best-whatsapp-alternatives-1832064581.

eletrônico aos seus clientes, podendo trocar mensagens contendo textos e os mais diversos tipos de arquivos.[37]

Junto a estes serviços também estão as plataformas de armazenamento e compartilhamento de arquivos na nuvem, como o *iCloud*, *Google Drive*, *Dropbox* e *Microsoft OneDrive*. São serviços que permitem que se armazene, sincronize e compartilhe arquivos em servidores remotos, salvando-os fora da memória de computadores ou de dispositivos móveis, tornando-os acessíveis de qualquer lugar desde que haja conexão à internet.[38]

Todos estes sistemas informatizados utilizam-se do espaço da rede mundial de computadores para suas trocas de dados e metadados e a maioria já conta com serviços de criptografia ponta a ponta. Este último recurso é trazido em razão da alta demanda por segurança em redes e atualmente é abrangido na maioria dos serviços antes citados, podendo ser padrão ou recurso secundário dentro dos aplicativos.

2.6 Tecnologia de criptografia ponta a ponta e o direito à proteção de dados

A privacidade e a intimidade são direitos fundamentais dos mais caros ao Estado Democrático de Direito, tanto que figuram ao topo do rol do artigo 5º da Constituição Federal de 1988, neste caso em seu inciso X[39], sendo direitos que resguardam na totalidade a esfera da vida privada do indivíduo.

Na visão que parece melhor apetecer à Paulo Gustavo Gonet Branco, ao se falar do direito à privacidade, pode-se entendê-lo como direito mais amplo que visa dar proteção a totalidade das relações e pensamentos de um indivíduo, sejam elas familiares, comerciais ou professionais. Com relação ao direito da intimidade, seria a

---

[37] BEAL, Vangie. *Email Services*. Webopedia, 05 de janeiro de 2011. Disponível em https://www.webopedia.com/definitions/email-services/. Tradução nossa.

[38] ROSENBERG, Jothy; MATEOS, Arthur. The Cloud at Your Service. 1. ed. Connecticut: Manning Publications, 2011, p. 1. Tradução nossa.

[39] Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. BRASIL. Constituição Federal de 1988. Brasília, DF.

proteção de um conjunto mais restrito destes pensamentos e relações interpessoais – como com familiares e amigos – mais profundas do homem[40].

De forma mais rigorosa e no mesmo sentido, Marcelo Novelino divide a privacidade e a intimidade como gênero e espécie, respectivamente:

> Para proteger a privacidade (gênero), permitindo ao indivíduo conduzir a própria vida da maneira que julgar mais conveniente, sem intromissão da curiosidade alheia, a Constituição assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem (espécies). A intensidade da proteção deve variar conforme a área da personalidade afetada. Quanto mais próxima das experiências definidoras da identidade do indivíduo, maior deve ser o peso conferido ao direito à privacidade.[41]

Pela diferenciação feita anteriormente, conclui-se ser a privacidade um gênero que abarca as demais espécies, que são subsequentes ao inciso X, sendo elas a intimidade, a vida privada, a honra e a imagem.

Com vistas assegurar o direito à intimidade e a privacidade, um novo direito – e consequentemente uma série de regulamentações nascem –, mais recentemente, à luz da Constituição Cidadã, desta vez dissertando a respeito dos atuais meios digitais pelos quais os direitos supracitados podem ser colocados em risco. O aparecimento da internet, o sistema global de redes de computadores mais utilizado, traz inéditas necessidades de inovação legislativa com fim de garantir os demais direitos.

Em 2022, a Constituição Federal acrescentava o seu inciso LXXIX[42] do artigo 5º, por meio da Emenda Constitucional n.º 115, apresentando agora o direito à proteção dos dados pessoais.

Tal inovação de direitos nada mais é que a constante adaptabilidade e evolução que deve o Direito deverá ter e sofrer em face as novas mudanças socioculturais dos novos tempos, como bem Fernando Bobbio indagou – naquele momento discutia

---

[40] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 16. ed. São Paulo: Saraiva Educação, 2021, p. 547.
[41] NOVELINO, Marcelo. Curso de Direito Constitucional. 11. ed. Salvador: JusPodivm, 2016, p. 337.
[42] Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. BRASIL. Constituição Federal de 1988. Brasília, DF.

acerca da inovação dos direitos relativos ao meio-ambiente – na introdução à sua obra *A Era do Direito*:

> Mais uma prova, se isso ainda fosse necessário, de que os direitos não nascem todos de uma vez. Nascem quando devem ou podem nascer. Nascem quando o aumento do poder do homem sobre o homem — que acompanha inevitavelmente o progresso técnico, isto é, o progresso da capacidade do homem de dominar a natureza e os outros homens — ou cria novas ameaças à liberdade do indivíduo ou permite novos remédios para as suas indigências: ameaças que são enfrentadas através de demandas de limitações do poder; remédios que são providenciados através da exigência de que o mesmo poder intervenha de modo protetor.[43]

Fora da esfera estatal, por sua vez, as grandes empresas do ramo de tecnologia, chamadas de *Big Techs*, que compõem maior parte do mercado e a concorrência no tocante aos meios de comunicação via internet, também procuraram as mais diversas soluções para o resguardo das informações de seus usuários.

A resposta encontrada para maioria dos casos foi o uso de ferramentas de criptografia, que mais recentemente trouxe a popularização do recurso da criptografia ponta a ponta, um tipo específico das criptografias assimétricas.

A criptografia assimétrica utiliza-se de um mecanismo da mescla de dois tipos de chaves, uma chave privada e uma pública[44], esta mistura faz com que apenas o usuário emissor e o usuário receptor tenham acesso ao conteúdo de tais mensagens, fazendo com que a prestadora dos serviços de envio de mensagens torne-se totalmente alheia ao seu conteúdo.

A criptografia ponta a ponta (*end-to-end encryption* ou *E2EE* em inglês) é uma técnica de criptografia assimétrica que garante privacidade e segurança de comunicações eletrônicas, como mensagens de texto, chamadas de voz e compartilhamento de arquivos[45].

Com este recurso, as informações são cifradas no dispositivo de origem antes de serem transmitidas para o destinatário, e só podem ser decifradas no dispositivo

---

[43] BOBBIO, Norberto. A Era dos Direitos. Tradução Carlos Nelson Coutinho; apresentação de Celso Lafer. Nova ed. Rio de Janeiro: Elsevier, 2004, p. 9.

[44] STALLINGS, William. Criptografia e segurança de redes: princípios e práticas. Tradução de Daniel Vieira, 6. ed. São Paulo: Pearson Education do Brasil, 2015, p. 200.

[45] COUTINHO, Mariana. O que é criptografia de ponta-a-ponta? Entenda o recurso de privacidade. Techtudo, 12 de junho de 2019. Disponível em: https://www.techtudo.com.br/noticias/2019/06/o-que-e-criptografia-de-ponta-a-ponta-entenda-o-recurso-de-privacidade.ghtml.

do destinatário. Isso significa que, mesmo que as informações sejam interceptadas durante a transmissão, elas não podem ser lidas ou compreendidas sem a chave de decifração.

A criptografia ponta a ponta é uma forma efetiva de proteger as informações contra acessos não autorizados, vazamentos de dados e outros tipos de ameaças à privacidade. Ela é amplamente utilizada em aplicativos de mensagens e chamadas, como o *WhatsApp*, o *Signal* e o *Telegram*, e em serviços de armazenamento de dados na nuvem, como o *Google Drive* e o *Dropbox*.

3. MEIOS DE OBTENÇÃO DA PROVA TELEMÁTICA NO PROCESSO PENAL BRASILEIRO E NO PROJETO DE LEI N.º 4.939/20

3.1 A interceptação telemática e a Lei n.º 9.296/1996

A Lei n.º 9.296/96 tem por papel fundamental dispor e elencar todo um ferramental investigativo com vistas à obtenção de provas na esfera dos procedimentos telefônicos-telemáticos, sendo assim, já em seu parágrafo único, do artigo primeiro[46], preconiza uma equiparação entre os sistemas telemáticos e informáticos.

No que tange ao procedimento da interceptação telemática, o órgão investigador, em regra o Ministério Público e as Polícias Judiciárias[47], peticiona ao Poder Judiciário para que os envolvidos, devidamente identificados, em crimes tenham sua comunicação via telefone interceptada. Embora o artigo ainda cite que a interceptação possa ser determinada de ofício pelo magistrado, desde a impetração da Ação Direta de Inconstitucionalidade n.º 3.450, ainda a ser julgada pelo Supremo Tribunal Federal, resta uma resposta definitiva quanto ao juiz poder fazê-la autonomamente.

Como a interceptação telefônica é polissêmica, pode facilmente ser confundida com outras ferramentas investigativas, então cabe distinguir alguns conceitos já pacificados de outros ainda controversos. Por isso listaremos a seguir, o mais resumidamente possível, os conceitos mais importantes na literatura das provas telemáticas.

---

[46] Art. 1º. A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática. BRASIL. Lei n.º 9.296, de 24 de julho de 1996.

[47] Art. 3°. A interceptação das comunicações telefônicas poderá ser determinada pelo juiz, de ofício ou a requerimento: I - da autoridade policial, na investigação criminal; II - do representante do Ministério Público, na investigação criminal e na instrução processual penal. *Ibidem*.

a) Interceptação Telefônica *lato sensu*:

A interceptação telefônica em sentido amplo abarca tanto a interceptação telefônica *stricto sensu* quanto a escuta telefônica. Esta diferenciação ocorre com certos doutrinadores, como é o caso do professor Fernando Capez:

> Tanto a interceptação stricto sensu quanto a escuta telefônica inserem-se na expressão "interceptação", prevista no art. 5o, XII, da CF; logo, submetem-se às exigências da Lei n. 9.296/96. Diferente é o caso em que o próprio interlocutor grava a conversa. Neste, não existe a figura do terceiro, portanto não se pode falar em interceptação.[48]

De forma semelhante entende Luiz Francisco Torquato Avolio:

> Juridicamente, as interceptações, lato sensu, podem ser entendidas como ato de interferência nas comunicações telefônicas, quer para impedi-las – com consequências penais –, quer para delas apenas tomar conhecimento – nesse caso, também com reflexos no processo.[49]

Seguidamente, Torquato também restringirá o termo interceptação telefônica *lato sensu* no sentido de excluir a modalidade de gravação realizada pelo próprio interlocutor como parte dessa categoria[50].

b) Escuta Telefônica

A escuta telefônica, por sua vez, é o acompanhamento do conteúdo de chamadas e mensagens no qual um dos interlocutores da conversa possui ciência de que está sendo escutado[51][52]. Tal medida é mais comum em crimes de estelionato e sequestro.

c) Gravação Telefônica

Também chamada de gravação clandestina, é amplamente entendida pela doutrina como a gravação realizada por um dos interlocutores, podendo, ou não, que

---

[48] CAPEZ, Fernando. Curso de Direito Penal, v. 4, Legislação Penal Especial. 13. ed. São Paulo: Saraiva Jur, p. 528.
[49] AVOLIO, Luiz Francisco Torquato. Provas Ilícitas: Interceptações telefônicas, ambientais e gravações clandestinas. 6. ed. São Paulo: Editara Revista dos Tribunais, 2015, p. 104.
[50] *Ibidem*. p. 108.
[51] LIMA, Renato Brasileiro de. Legislação Criminal Especial Comentada. 8. ed. Salvador: JusPodivm, 2020, p. 515.
[52] AVOLIO, Luiz Francisco Torquato. Provas Ilícitas: Interceptações telefônicas, ambientais e gravações clandestinas. 6. ed. São Paulo: Editara Revista dos Tribunais, 2015, p. 108.

o outro tenha consciência de que está sendo gravado[53][54]. Embora denominada como clandestina, certas hipóteses garantem sua licitude no processo penal, como para fins de legítima defesa.

d) Grampo Telefônico

O grampo telefônico é, na realidade, um jargão popular que engloba todos os métodos pelos quais há o acompanhamento de chamadas, sendo eles legais ou ilegais, ou seja, não possui significado específico. Esta expressão é alheia ao ordenamento jurídico brasileiro, sendo mais famosa entre a imprensa brasileira[55].

e) Comunicação Ambiental

A expressão comunicação ambiental é uma definição que irá reger o significado da palavra “ambiental” expressa no nome dos demais métodos de obtenção de prova. Comunicação ambiental é toda a comunicação realizada ao ambiente aberto, sem que haja a necessidade de que a comunicação tenha de perpassar por qualquer meio artificial de transmissão ou gravação, seja este meio analógico ou digital.

f) Interceptação Ambiental x Captação Ambiental

Termo polissêmico que pode tanto remeter à captação clandestina de comunicação ambiental[56], quanto o método autorizado pelo magistrado de obtenção de prova aproveitando-se de sinais eletromagnéticos, ópticos ou acústicos. Este último, captação ambiental, é o termo em que há maior precisão, estando previsto no inciso II[57] do art. 3º da Lei de Organizações Criminosas vigente no Brasil.

---

[53] LIMA, Renato Brasileiro de. Legislação Criminal Especial Comentada. 8. ed. Salvador: JusPodivm, 2020, p. 515.
[54] AVOLIO, Luiz Francisco Torquato. Provas Ilícitas: Interceptações telefônicas, ambientais e gravações clandestinas. 6. ed. São Paulo: Editara Revista dos Tribunais, 2015, p. 114.
[55] Perguntas e Respostas: Grampos telefônicos. Veja, 05 de dezembro de 2008. Disponível em: https://web.archive.org/web/20121227133554/http://veja.abril.com.br/idade/exclusivo/perguntas_respostas/grampos-telefonicos/escuta-telefonica-espionagem-investigacao-lei-policia-cpi.shtml.
[56] LIMA, Renato Brasileiro de. Legislação Criminal Especial Comentada. 8. ed. Salvador: JusPodivm, 2020, p. 515.
[57] 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: [...] II - captação ambiental de sinais eletromagnéticos, ópticos ou acústicos. BRASIL, Lei n.º 12.850, de 2 de agosto de 2013. Brasília, DF. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.

De acordo com Luiz Flávio Gomes e Marcelo Rodrigues da Silva, por seu turno, distingue-se captação ambiental de interceptação ambiental por esta ser alheia ao conhecimento de ambos os interlocutores e por aquela ser executada por um dos interlocutores que realiza a própria gravação[58], significando de igual forma a gravação ambiental para Renato Brasileiro. No Inquérito n.º 2.424/RJ, com relatoria do Min. Cezar Peluso há a menção da interceptação junto à captação ambiental:

> PROVA. Criminal. Escuta ambiental. Captação e interceptação de sinais eletromagnéticos, óticos ou acústicos. Meio probatório legalmente admitido. Fatos que configurariam crimes praticados por quadrilha ou bando ou organização criminosa. Autorização judicial circunstanciada. Previsão normativa expressa do procedimento. Preliminar repelida. Inteligência dos arts. 1º e 2º, IV, da Lei nº 9.034/95, com a redação da Lei nº 10.217/95. Para fins de persecução criminal de ilícitos praticados por quadrilha, bando, organização ou associação criminosa de qualquer tipo, são permitidos a captação e a interceptação de sinais eletromagnéticos, óticos e acústicos, bem como seu registro e análise, mediante circunstanciada autorização judicial. (Inq. n.º 2.424/RJ, Relator o Ministro Cezar Peluso, Tribunal Pleno, DJe de 26/3/10).[59]

A ambiguidade pode ser percebida também ainda de antes do advento da recente Lei das Organizações Criminosas, como demonstra a ementa anteriormente citada. Trata-se, desta forma, de conceitos ainda em discussão quanto ao seu significado mais rigoroso.

g) Escuta Ambiental

A escuta ambiental tem seu conceito bem definido, sendo ela a captação de comunicação em ambiente aberto, realizada por um terceiro, o qual um dos interlocutores possui ciência de que tem sua comunicação sendo acompanhada[60].

h) Método de Espelhamento

Método o qual, da apreensão de telefone celular, o investigador obtém acesso ao aplicativo de mensagem do aparelho e o espelha utilizando o recurso *web* do aplicativo para que assim possa acompanhar as mensagens trocadas. No RHC n.º

---

[58] GOMES, Luiz Flávio; SILVA, Marcelo Rodrigues da. Organizações Criminosas e Técnicas Especiais de Investigação. 1. ed. Salvador: JusPodivm, 2015, p. 413.

[59] BRASIL. Supremo Tribunal Federal. INQ 2.424-4/RJ. Rel. Min. Cezar Peluso. Julgado em 25/04/2007. DJ de 24/08/2007. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=481962.

[60] LIMA, Renato Brasileiro de. Legislação Criminal Especial Comentada. 8. ed. Salvador: JusPodivm, 2020, p. 515.

99.735/SC, de relatoria da Min. Laurita Vaz, julgado em 27/11/2018, é mostrada a postura atual do Superior Tribunal de Justiça quanto a este método.

> 2. O espelhamento das mensagens do WhatsApp ocorre em sítio eletrônico disponibilizado pela própria empresa, denominado WhatsApp Web. Na referida plataforma, é gerado um tipo específico de código de barras, conhecido como Código QR (Quick Response), o qual só pode ser lido pelo celular do usuário que pretende usufruir do serviço. Daí a necessidade de apreensão, ainda que por breve período de tempo, do aparelho telefônico que se pretende monitorar.[61]

Tal procedimento, como se percebe, fora proibido pela jurisprudência, entendendo o tribunal que o órgão investigador terá a possibilidade de agir ativamente ao escrever e enviar mensagens pelo investigado.

i) Interceptação Telefônica *stricto sensu*:

A interceptação telefônica é o acompanhamento do conteúdo de chamadas e mensagens, por um período predefinido, o qual ambos os interlocutores da conversa não possuem ciência de que estão sendo observados por um investigador. Neste caso o perscrutador não possui capacidade de interferência sobre o conteúdo das conversas[62][63].

A interceptação das comunicações telefônicas em sentido estrito é uma das ferramentas mais utilizadas no âmbito do processo investigativo e do processo penal em que há a interceptação, realizada por um terceiro que neste caso do órgão investigador, de todas as ligações telefônicas e mensagens do tipo SMS de um determinado terminal telefônico por um prazo definido de 15 (quinze) dias, renováveis por mais 15 (quinze) dias se comprovada a indispensabilidade do meio de prova, como sucintamente aponta o artigo 5º da Lei de Interceptação Telefônica[64].

---

[61] BRASIL. Superior Tribunal de Justiça. RHC n.º 99.735/SC. Rel. Min. Laurita Vaz, julgado em 27/11/2018, DJe de 12/12/2018. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1777437&num_registro=201801533498&data=20181212&peticao_numero=-1&formato=PDF.

[62] LIMA, Renato Brasileiro de. Legislação Criminal Especial Comentada. 8. ed. JusPodivm, 2020, p. 515.

[63] AVOLIO, Luiz Francisco Torquato. Provas Ilícitas: Interceptações telefônicas, ambientais e gravações clandestinas. 6. ed. São Paulo: Editara Revista dos Tribunais, 2015, p. 106.

[64] Art. 5°. A decisão será fundamentada, sob pena de nulidade, indicando também a forma de execução da diligência, que não poderá exceder o prazo de quinze dias, renovável por igual tempo uma vez comprovada a indispensabilidade do meio de prova. BRASIL. Lei n.º 9.296, de 14 de julho de 1996.

Nesse interim o investigador terá acesso a todas as conversas e mensagens que o investigado tenha contatado ou sido contatado sem que haja qualquer tipo ou possibilidade de interferência advinda do perscrutante, bem como ciência de que o conteúdo do investigado esteja sendo ouvido.

Deve-se frisar que o instrumento da interceptação telefônica é último recurso, pois carece de imprescindibilidade, isto é, deve ser demonstrado que não há mais outros meios para obtenção de prova, e deve ter fundamentação específica, tanto no pedido cautelar, quanto na fundamentação da decisão proferida. Essa característica de *ultima ratio* encontra-se expressa no inciso II[65] do artigo 2º.

3.2 A busca e apreensão de/em dispositivos telemáticos de comunicação e de transmissão e dados no PL n.º 4.939/20

A busca e apreensão é medida cautelar prevista no Código de Processo Penal e tem por objetivo a coleta de objetos relacionados a um crime investigado. A diligência encontra-se regrada pelos artigos 240 ao 250 do Código de Processo Penal, de 1941, tendo ali elencadas seu objeto, seus requisitos e seu procedimento. Como medida cautelar, tem por objetivo a coleta de elementos relacionados a um crime investigado, sendo realizada, precipuamente, pela autoridade policial, devendo ser autorizada por um juiz, que avaliará se há indícios suficientes de que os objetos ou as informações procuradas são relevantes para o andamento da investigação.

O Projeto de Lei n.º 4.939/20 aduz esta modalidade de meio de obtenção de prova com nova roupagem em seu inciso I[66] do artigo 9º, com fim de uma mais efetiva sistematização para tal procedimento.

Em primeiro momento, cabe distinguir o conceito de busca de apreensão. A busca é a diligência a qual procura-se objetos ou pessoas, enquanto a apreensão é a

[65] Art. 2º. Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses: [...] II - a prova puder ser feita por outros meios disponíveis. *Ibidem*.
[66] Art. 9º. Constituem meios de obtenção da prova digital, na forma da Lei: I – a busca e apreensão de dispositivos eletrônicos, sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica, e o tratamento de seu conteúdo. BRASIL. PL n.º 4.939, de 2020.

providência tomada no que diz respeito a pôr sob custódia estes objetos ou pessoas[67]. A busca é dividida em duas espécies: a domiciliar, quando há o adentramento em domicílio, igualmente protegida pelo inciso X do artigo 5º da Constituição Federal, e tem por finalidade a busca de pessoas e objetos, por seu turno, a busca pessoal é aquela realizada no corpo humano ou em seus objetos íntimos quando fundada suspeita para colheita de qualquer elemento de convicção[68].

Entendendo-se estas partes, percebe-se ser uma medida invasiva que só pode ser empregada se houver uma fundada suspeita de que determinado local ou pessoa guarda elementos importantes para a investigação, como preveem os parágrafos primeiro e segundo do artigo 240 do Código de Processo Penal[69]. Além disso, a busca deve ser realizada de forma adequada, sem prejudicar direitos dos investigados ou de terceiros envolvidos.

Seguidamente, no artigo 243[70] serão colocados os requisitos do mandado, devendo indicar, o mais precisamente, lugar ou pessoa, motivos e fins de tal diligência, bem como subscrição e assinatura dos servidores competentes.

No atinente à apreensão de dispositivo telemático, como computadores, notebooks, celulares e demais dispositivos eletrônicos, a autoridade competente, como Delegado ou Promotor, submeterá os aparelhos à perícia a fim de coletar vestígios do crime. Nesta etapa é realizada a perícia digital, podendo ser feita por um agente estatal específico, o perito em informática, ou por empresa especializada no acesso destes dispositivos.

Em etapa de expedição de mandado de busca, passou a ser mais comum, com vistas a recrudescer as fundamentações, a autoridade pedir em conjunto com a busca

---

[67] LIMA, Renato Brasileiro de. Código Processual Penal Comentado. 2. ed. Salvador: JusPodivm, 2017, p. 681.
[68] *Ibidem*. p. 682.
[69] Art. 240. A busca será domiciliar ou pessoal. § 1º Proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem. [...] § 2º Proceder-se-á à busca pessoal quando houver fundada suspeita de que alguém oculte consigo arma proibida ou objetos mencionados nas letras b a f e letra h do parágrafo anterior. BRASIL, Decreto Lei n.º 3.689, de 03 de outubro de 1941, Código de Processo Penal. Brasília, DF. Disponível em: http://www.planalto.gov.br/CCIVIL/Decreto-Lei/Del3689.htm.
[70] Art. 243. O mandado de busca deverá: I - indicar, o mais precisamente possível, a casa em que será realizada a diligência e o nome do respectivo proprietário ou morador; ou, no caso de busca pessoal, o nome da pessoa que terá de sofrê-la ou os sinais que a identifiquem; II - mencionar o motivo e os fins da diligência e III - ser subscrito pelo escrivão e assinado pela autoridade que o fizer expedir. *Ibidem*.

e apreensão a quebra de sigilo para acesso aos dados informáticos, como bem explica Márcio Mesquita:

> A experiência prática do foro tem revelado que tanto o Delegado de Polícia Federal quanto o representante do Ministério Público Federal têm formulado, juntamente com o requerimento de expedição de mandado de busca e apreensão, também requerimento de autorização de acesso ao conteúdo das mídias digitais apreendidas, ou até mesmo de quebra de sigilo para acesso a tais conteúdos.[71]

Todavia, de acordo com o Superior Tribunal de Justiça, em sede do RHC n.º 75.800/PR, cujo relator era o Min. Felix Fischer, não haveria a necessidade de se pedir além da própria busca e apreensão dos aparelhos eletrônicos, como bem expõe o item quatro da ementa:

> IV - Na pressuposição da ordem de apreensão de aparelho celular ou smartphone está o acesso aos dados que neles estejam armazenados, sob pena de a busca e apreensão resultar em medida írrita, dado que o aparelho desprovido de conteúdo simplesmente não ostenta virtualidade de ser utilizado como prova criminal.[72]

A perícia digital é, destarte, um conjunto de técnicas utilizadas para coletar, analisar e preservar informações armazenadas em dispositivos eletrônicos. Os casos de apreensão de *smartphones*, bem como posterior perícia, são recorrentes em situações de investigações criminais. Os técnicos ao terem acesso aos dados recuperados, coletarão relevantes elementos para a investigação, como mensagens de texto, chamadas e registros telefônicos, fotos, vídeos e dados de localização[73].

Ao se extrair o material digital de todos os dispositivos apreendidos, dever-se-á prestar atenção no aspecto da integridade da prova, isto é, se a fonte da prova não sofreu qualquer adulteração e no aspecto da autenticidade da prova, que é a confiabilidade do material colhido da prova. Baseando-se em Pozo Pérez, Gustavo Badaró sintetiza quanto à pertinência destes itens no âmbito do procedimento da cadeia de custódia:

---

[71] MESQUITA, Márcio Satalino. Crimes Cibernéticos: Investigação e provas. 1. Ed. EMAG TRF-3, 2017, p. 200.

[72] BRASIL. Superior Tribunal de Justiça. RHC n.º 75.800/PR, Rel. Min. Felix Fischer, julgado em 15/09/2016, DJe de 26/09/2016, p. 1. Disponível em: https://www.conjur.com.br/dl/busca-apreensao-celular-autoriza-acesso.pdf.

[73] LOPES, Diogo. Tudo sobre perícia em celulares e o papel do perito em celular. Ipericias, 09 de março de 2021. Disponível em https://lpericias.com.br/tudo-sobre-pericia-em-celulares-e-o-papel-do-perito-em-celular/.

> Trata-se, portanto, de um procedimento de documentação ininterrupta, desde o encontro da fonte de prova, até a sua juntada no processo, certificando onde, como e sob a custódia de quais pessoas e órgãos foram mantidos tais traços, vestígios ou coisas que interessam à reconstrução histórica dos fatos no processo, com a finalidade de garantia de sua identidade, integridade e autenticidade.[74]

Outrossim, parte deste procedimento já estava recepcionado pelo artigo 11[75] da Lei n.º 11.419, de 2006, que dispôs acerca da informatização do processo penal, o qual trouxe o entendimento de que há uma equiparação de iguais entre documento original digital e documento cópia digital juntado ao processo.

Desta feita, em resumo, a busca e apreensão de dispositivos telemáticos de comunicação e de transmissão e dados deverá seguir um rito próprio, diferente das demais provas periciais, no momento de seu pedido, sua diligência na busca e apreensão, seu afastamento de sigilo, sua perícia e sua inserção como conteúdo probatório dentro do processo investigativo e penal, que seguirão novas diretrizes dentro da nova era digital.

3.3 Coleta remota de comunicações e dados telemáticos em repouso acessados à distância no PL n.º 4.939/20

Ao discorrer sobre a coleta remota de comunicações e dados telemáticos em repouso acessados à distância, se está tratando de um dos meios de obtenção de prova digital sugeridos no inciso II[76] do art. 9º do Projeto de Lei n.º 4.939/20. Primeiramente, faz pertinente a definição do significado de “dados em repouso” contida na própria protolegislação supracitada em seu artigo 3º, inciso VII[77], que diz respeito aos dados armazenados em dispositivo eletrônico ou em sistema informático.

---

[74] BADARÓ, Gustavo Henrique Righi Ivahy. Processo Penal. 9. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 696. *E-book*.

[75] Art. 11. Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais. BRASIL. Lei n.º 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm.

[76] Art. 9º. Constituem meios de obtenção da prova digital, na forma da Lei: [...] II – a coleta remota, oculta ou não, de dados em repouso acessados à distância. BRASIL. PL n.º 4.939, de 2020.

[77] Art. 3º. Para feitos desta Lei considera-se: [...] VII - Dados em repouso: dados que se encontram armazenados em um dispositivo eletrônico ou sistema informático. *Ibidem*.

Deve-se ter em mente de que o objeto deste meio de obtenção de prova é todo o material contido apenas em provedores de serviços de armazenamento, que poderão ser, por exemplo, empresas que operam com serviços de *e-mails*, armazenamento em nuvem e até conteúdo ocultos e não ocultos no âmbito das redes sociais.

Esse meio de coleta remota permite que os dados de comunicação e telemáticos sejam acessados e coletados de dispositivos eletrônicos à distância, sem a necessidade de ter acesso físico ao aparelho ou estar próximo dele. Portanto, a medida ocupa-se de coletar todos os dados que se encontrem estáticos em serviços de armazenagem, isto é, que não em fluxo de comunicação.

Em face do procedimento em si, quando fundada suspeita de que um ilícito fora ou está em prática por determinado indivíduo, tendo aqui em mãos elementos mínimos de identificação – como nome, endereço de *e-mail*, número telefônico ou *URL* da rede social –, o órgão investigador peticiona ao Poder Judiciário pelo afastamento do sigilo sobre os dados em repouso. Convém expressar que a medida de coleta remota de dados em repouso pretende resgatar elementos de convicção de um crime já consumado, mesmo que permaneça sendo perpetrado, *i.e.*, inserido no pedido deverá haver o ínterim em que o crime fora praticado.

O *Habeas Corpus* n.º 315.220/RS, julgado pelo Superior Tribunal de Justiça, de relatoria da Min. Maria Thereza de Assis Moura, é paradigmático no que se refere ao procedimento da coleta de dados remotos em repouso. Em sede do remédio constitucional citado, há a discussão tanto com relação às exigências necessárias do pedido de quebra do sigilo, quanto de um possível prazo máximo para a posterior coleta de *e-mails*, como bem resume o Min. Rogerio Schietti Cruz:

> A Ministra Maria Thereza de Assis Moura, relatora, considerando o fato de a constrição da comunicação eletrônica ter abrangido período superior a dez anos, de 2004 a 2014, "sem que se declinasse adequadamente a necessidade da medida extrema ou mesmo os motivos para o lapso temporal abrangido, a refugar o brocardo da proporcionalidade", concedeu a ordem, "a fim de declarar nula apenas a evidência resultante do afastamento dos sigilos de seus respectivos correios eletrônicos, determinando-se que seja

> desentranhado, envelopado, lacrado e entregue aos respectivos indivíduos o material decorrente da medida".[78]

Em caso de autorização judicial positiva do afastamento de sigilo, caberá aos perquiridores entrarem em contato com a plataforma que detém os dados, enviando uma petição dentro de Medida Cautelar Criminal junto de cópia da decisão fundamentada. Como aqui se refere às grandes empresas da seara da tecnologia, que quase em sua totalidade possuem sede no Brasil, há quadros responsáveis nestas empresas que conseguem, por sua vez, prover as informações, desde que não criptografadas de ponta a ponta, solicitadas pelo investigador.

Em exemplo, pode-se citar o caso da Google Brasil, que disponibiliza a plataforma *Google LERS*[79] (*Law Enforcement Online Requests*), onde o investigador oficial terá seu cadastro e acesso as informações para posterior coleta e cotejamento. Em consequência a este pedido, dependerá de quanto o indivíduo observado utilizou-se das mais variadas ferramentas disponíveis pela prestadora Google, quanto mais serviços usados, maior é a carga de dados que ir-se-á receber de resposta. Sistemas semelhantes também estão disponibilizados por empresas como o Grupo Meta[80], Amazon[81], WhatsApp[82], Microsoft[83], entre outras mais.

3.4 Interceptação telemática em transmissão no PL n.º 4.939/20

De igual modo, ao se dissertar sobre a obtenção de prova em fluxo de transmissão, se está tratando de um dos meios de obtenção de prova digital sugeridos no inciso III[84] do art. 9º do Projeto de Lei n.º 4.939/20. Previamente, tem-se de referir

---

[78] BRASIL. Superior Tribunal de Justiça. Habeas Corpus n.º 315.220/RS. Rel. Min. Maria Thereza de Assis Moura, julgado em 15/09/2015, DJe de 09/10/2015, p. 31-32. Disponível em https://www.conjur.com.br/dl/hc-315220-quebra-sigilo-telematico-dez.pdf.

[79] Sistema de Solicitação de Aplicação da Lei. Google. Disponível em https://lers.google.com/signup_v2/landing.

[80] Informações sobre aplicação da lei. Grupo Meta. Disponível em: https://www.facebook.com/help/instagram/494561080557017/?helpref=uf_share.

[81] *Law Enforcement Requests Tracker*. Amazon Inc. Disponível em: https://ler.amazon.com/us.

[82] Solicitações Online para Autoridades Públicas. WhatsApp LLC. Disponível em: https://www.whatsapp.com/records/login/?locale=pt_BR&lang=pt_br.

[83] *Law Enforcement Requests Report*. Microsoft Corporation. Disponível em: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report.

[84] Art. 9º. Constituem meios de obtenção da prova digital, na forma da Lei: [...] III – a interceptação telemática de dados em transmissão. BRASIL. Câmara dos Deputados. PL n.º 4.939, de 2020.

que o PL estabelece o conceito de “dados em transmissão”, presente em seu art. 3º, inciso VIII[85], que dirá respeito sobre os dados em movimento, ou seja, em tráfego.

É essencial considerar que a interceptação telemática em transmissão já havia sido anteriormente acolhida pela Lei de Interceptação Telefônica, dado que ainda em seu parágrafo único, do artigo 1º, estendia os poderes da lei para além do simples contexto telefônico. O projeto legislativo em discussão ainda traz um breve regramento a respeito dessa modalidade em seu artigo 10[86], carregando, subsidiariamente, o procedimento realizado na Lei n.º 9.296/96.

Este meio de interceptação telemática se assemelharia demasiado ao que já existe, então, desde a década de noventa. Todavia é totalmente benéfico o entrelaçamento do projeto com a lei, posto que há caracteres suplementares de uma com a outra, sendo que a proposta esclarece conceitos das tecnologias mais recentes.

No tocante ao procedimento, será aplicada a regulamentação da Lei de Interceptação, isto é, cumprindo-se os requisitos necessários à medida, como justificada suspeita de que o indivíduo esteja perpetrando um ilícito e tendo aqui em mãos elementos mínimos de sua identificação para este caso – tal como nome e número telefônico –, o órgão investigador peticiona ao Poder Judiciário pelo afastamento do sigilo sobre os dados em transmissão. Diferentemente da coleta remota de dados em repouso, nesta situação só serão abertos os dados que passarem em comunicação pelo prazo estipulado, não havendo abertura do sigilo de antes ou de depois.

Diante de decisão concordante pelo magistrado, a interceptação entrará em vigor pelo prazo de sessenta dias, cabendo mesma renovação, de acordo com o §1º[87]

---

[85] Art. 3º. Para feitos desta Lei considera-se: [...] VI - Dados em transmissão: dados encapsulados em pacotes trafegando por redes segundo protocolos determinados. *Ibidem*.

[86] Art. 10. A interceptação telemática poderá ser destinada aos provedores ou serviços de infraestrutura, de conexão ou aplicação, bem como aos dispositivos eletrônicos ou sistemas informáticos particulares, devendo ser individualizadas as redes de dados e os protocolos de internet envolvidos. *Ibidem*.

[87] Art. 13. A ordem judicial para obtenção da prova digital para fins de investigação e processo penal descreverá os fatos investigados com a indicação da materialidade e possível autoria delitiva, indicando ainda os motivos, a necessidade e os fins da diligência, estabelecendo os limites da atividade a ser empreendida e o prazo para seu cumprimento. § 1º Em caso de monitoramento do fluxo de dados, o prazo da medida não poderá exceder a 60 (sessenta) dias, permitidas prorrogações por igual período, desde que continuem presentes os pressupostos autorizadores da diligência, até o máximo de 360 (trezentos e sessenta) dias, salvo quando se tratar de crime permanente, enquanto não cessar a permanência. *Ibidem*.

do art. 13, e o investigador terá a oportunidade de verificar a transmissão de informações em tempo real. A ideia do Projeto de Lei é de pôr os provedores de aplicação na internet nos mesmos moldes que são cumpridos pelas operadoras de telefonia.

Desta forma as empresas ou aplicações de mensageiro instantâneo, como *WhatsApp*, *Telegram* e *Messenger*, deverão lançar novas funcionalidades que permitam as autoridades públicas o acesso das transmissões de texto, áudio e vídeo quando conveniente ao poder estatal.

3.5 Coleta por acesso forçado de sistema telemático no PL n.º 4.939/20

Por último, a coleta por acesso forçado do sistema telemático é o meio de obtenção de prova telemática derradeiro, acolhido no inciso IV[88] do artigo 9º do PL n.º 4.939/20. Sua definição está bem estabelecida no art. 12[89] e mostra uma via possível na eventualidade da ordem judicial ser frustrada por algum motivo. Sendo, desta forma, um expediente a ser usado caso a busca e apreensão em dispositivo eletrônico, a coleta de dados em repouso acessados à distância ou a interceptação telemática em transmissão não obterem êxito em suas diligências em face da desobediência do provedor.

Este meio de obtenção de prova seria, de fato, uma das inovações trazidas ao ordenamento jurídico brasileiro, todavia deve ser mais refinado com a finalidade de não mitigar em demasia os direitos constitucionais à privacidade e à intimidade. Uma das hipóteses que o texto permite aventar é no tocante a utilização de softwares de espionagem, ou *spywares*, que tem por objetivo, segundo John Aycock, coletar registros de dados, capturar imagens da tela do dispositivo eletrônico, gravar áudio e imagem por meio dos microfones e webcams conectadas ou introduzidas ao aparelho,

---

[88] Art. 9º. Constituem meios de obtenção da prova digital, na forma da Lei: [...] IV – a coleta por acesso forçado de sistema informático ou de redes de dados. *Ibidem*.

[89] Art. 12. A coleta por acesso forçado a dispositivo eletrônico, sistema informático ou redes de dados, ocorrerá somente após prévia desobediência de ordem judicial determinando a entrega da prova pretendida ou quando impossível identificar o controlador ou provedor em território nacional, e compreenderá os métodos de segurança ofensiva ou qualquer outra forma que possibilite a exploração, isolamento e tomada de controle. *Ibidem*.

ter acesso às conversas e *e-mails* gravados e em tráfego e observar todas as mais variadas atividades realizadas no aparelho[90].

Embora programas do gênero possam funcionar nos setores das agências de inteligência e dos demais órgãos de defesa nacional, transpô-los à seara da Justiça poderá acarretar diversas consequências. A organização Coalização Direitos nas Redes demonstrou alguns receios que o método em supramencionado pode trazer, são três deles: (i) o aumento incontrolável do armazenamento de dados em futuras investigações, (ii) o atenuamento das garantias presentes nas outras formas de coleta de provas digitais e (iii) a legitimação da atividade *hacker* executada pelo Estado[91].

No cenário internacional, a legislação espanhola já permite medida de obtenção de prova por meio destes *spywares*, constando no artigo 588, inciso VII, alínea *a*[92], do Código de Processo Penal do Estado da Espanha, ou *Ley de Enjuiciamiento Criminal* em espanhol. Embora extremamente invasivo para os padrões legais brasileiros, em um de seus itens, de igual alínea, há a suavização uma vez que é indispensável a descrição dentro da ordem judicial de qual *software* será utilizado em determinada operação[93].

Se porventura a coleta por acesso forçado for admitida ao sistema legal brasileiro, dever-se-á buscar empresas internacionais de cibersegurança que ofereçam este tipo de atividade com fim estabelecer convênios e acordos para disponibilização, ou programação, de aplicativos com esta função. Já é de amplo conhecimento algumas grandes empresas que produzem oficialmente *softwares* de vigilância, como a empresa israelense NSO Group Technologies, fabricante do

---

[90] AYCOCK, John. *Spyware and Adware*. 1. ed. Estados Unidos: Springer, 2011, p. 02.

[91] Reforma do Código de Processo Penal pode aumentar vigilância e precisa de equilíbrio em questões de tecnologia. Coalizão Direitos na Rede, 20 de maio de 2021. Disponível em: https://direitosnarede.org.br/2021/05/20/reforma-do-codigo-de-processo-penal-pode-aumentar-vigilancia-e-precisa-de-equilibrio-em-questoes-de-tecnologia/.

[92] Art. 588, VII, a, item 1. O juiz competente poderá autorizar a utilização de dados de identificação e códigos, assim com a instalação de software, que permitam, de forma remota e telemática, o exame a distância sem o conhecimento de seu titular, ou usuário, do conteúdo de um computador, dispositivo eletrônico, sistema informático, sistema de armazenamento massivo de dados informacionais ou base de dados, sempre que se busque a investigação de um dos crimes seguintes. ESPANHA. Código de Processo Penal Espanhol. Tradução nossa. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036.

[93] Art. 588, VII, a, item 2. A autorização judicial que autoriza o registro deverá especificar: [...] b) O alcance dela, a forma que se procederá no acesso e apreensão de dados ou arquivos informáticos relevantes para o caso e o programa meio pelo qual se executará a vigilância da informação. Tradução nossa. *Ibidem*.

controverso programa Pegasus[94], bem como a empresa, também israelense, Cellebrite Digital Intelligence, que presta, entre outras atividades, serviços de desbloqueio de celulares. Esta última, inclusive, está em uso no Brasil por diversas instituições, como no caso do assassinato de Henry Borel, onde a Polícia Civil do Estado do Rio de Janeiro dispôs desta ferramenta para desbloqueio e extração de dados celulares dos investigados pelo homicídio[95].

Ressalta-se que o ordenamento jurídico permite a compra e aluguel de serviços e equipamentos de investigação para algumas das modalidades de obtenção de prova, inclusive com dispensa de licitação, desde 2015[96] quando fora acrescentado o parágrafo 1º[97] ao art. 3º da Lei de Organizações Criminosas.

Por fim, durante a fase de instrução haverá a possibilidade do enfrentamento proporcionado pela ampla defesa e contraditório entre o Ministério Público e o denunciado permitirá a oportunidade de questionamento quanto ao método de obtenção empregado mediante certo programa de investigação.

3.6 Admissibilidade e utilização da prova telemática colhida ilicitamente

Uma vez que as inovações da nova era digital são implacáveis, no sentindo que civilização humana caminha cada vez mais adentro de sua virtualização, tem-se a prova telemática, ou digital, como provável protagonista no circuito da persecução penal, desta forma ela também passará pelo devido escrutínio tal qual as demais espécies de prova.

---

[94] CARVALHO, Caio. O que é o *spyware* Pegasus? Canaltech, 25 de setembro de 2021. Disponível em: https://canaltech.com.br/seguranca/o-que-e-o-spyware-pegasus/.

[95] FANTINATO, Giovanna. Cellebrite: conheça o software usado na investigação do caso Henry. Tecmundo, 12 de abril de 2021. Disponível em https://www.tecmundo.com.br/software/215422-cellebrite-conheca-software-usado-investigacao-caso-henry.htm.

[96] GOMES, Luiz Flávio; SILVA, Marcelo Rodrigues da. Organizações Criminosas e Técnicas Especiais de Investigação. 1. ed. Salvador: JusPodivm, 2015, p. 418.

[97] 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: [...] § 1º Havendo necessidade justificada de manter sigilo sobre a capacidade investigatória, poderá ser dispensada licitação para contratação de serviços técnicos especializados, aquisição ou locação de equipamentos destinados à polícia judiciária para o rastreamento e obtenção de provas previstas nos incisos II e V. BRASIL. Lei n.º 12.850, de 2 de agosto de 2013, Brasília, DF.

O processo penal, ao longo do período da redemocratização, passou a acolher mais recentemente o entendimento de que não deveria de se admitir prova obtida ilicitamente, uma vez que estabeleceria, no âmago do sistema brasileiro, um hábito infrator à norma jurídica[98], o que veio a ser assentado no inciso LVI[99] do artigo 5º da Constituição de 1988 e posteriormente cristalizado no artigo 157[100] do CPP, estendendo sua vedação às provas derivadas das ilícitas, como é recebido no primeiro trecho do parágrafo primeiro[101]. Apesar disso, após nova redação dada pela Lei n.º 11.690, de 2008, ao artigo, o mesmo dispositivo traz a partir da segunda fração do primeiro parágrafo[102] a ressalva proveniente de prova colhida por fonte independente.

O Brasil, desta forma, veio a se filiar a regra geral de que não se aceitará nem as provas colhidas ilicitamente, nem as provas derivadas da original ilícita, tal doutrina é chamada por teoria do fruto da árvore envenenada, também denominada por *the fruits of the poisonous tree*, em inglês, tendo sido proveniente do caso *Silverthorne Lumber & Co. v. United States*, de 1920[103]. Aury Lopes Jr. utiliza-se do exemplo específico das escutas e da violação das correspondências eletrônicas para demonstrar o caminho lógico da contaminação da prova derivada:

> Exemplo típico é a apreensão de objetos utilizados para a prática de um crime (armas, carros etc.) ou mesmo que constituam o corpo de delito, e que tenham sido obtidos a partir da escuta telefônica ilegal ou através da violação de correspondência eletrônica. Mesmo que a busca e apreensão seja regular, com o mandado respectivo, é um ato derivado do anterior, ilícito. Portanto, contaminado está.[104]

Já a Teoria da Fonte Independente, como dito antes, prevista nos dois primeiros parágrafos do art. 157, é uma das doutrinas também aplicadas no processo penal brasileiro, a qual estabelece que a prova ilícita obtida por um agente interessado

---

[98] MOREIRA, José Carlos Barbosa. Temas de Direito Processual. 6. ed. São Paulo: Editora Saraiva, 1997, p. 109.
[99] [...] LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos. BRASIL. Constituição Federal de 1988. Brasília, DF.
[100] Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais. BRASIL. Código de Processo Penal, Decreto Lei n.º 3.689, de 03 de outubro de 1941, Brasília, DF.
[101] §1º. São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras. *Ibidem*.
[102] [...] ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras. § 2º Considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova. *Ibidem*.
[103] DEZEM, Guilherme Madeira. Da Prova Penal. 1. ed. São Paulo: Millenium, 2008, p. 134.
[104] LOPES JUNIOR, Aury. Direito Processual Penal. 17. ed. São Paulo: Saraiva, 2020, p. 639. *E-book*.

pode ser considerada válida se a mesma informação tiver sido obtida independentemente por meios lícitos. Como Nestor Távora e Rosmar Rodrigues Alencar sintetizam:

> Se existirem provas outras no processo, independentes de uma determinada prova ilícita produzida, não há de se falar em contaminação, nem em aplicação da teoria dos frutos da árvore envenenada, pois, em não havendo vinculação nem relação de dependência, a prova ilícita não terá o condão de contaminar as demais.[105]

Em outras palavras, se a prova foi obtida por uma fonte independente, que não está relacionada com a prova ilícita, esta pode ser considerada válida no processo penal, mesmo que a prova ilícita seja excluída.

Além da circunstância anteriormente citada, há outra particularidade aceita pela ordem legal brasileira, trata-se da teoria do encontro fortuito de provas. Tal doutrina é comumente usada em situações em que, durante uma investigação criminal, ao se empregar métodos invasivos de obtenção de provas, como busca e apreensão, interceptação telefônica ou quebra de demais tipos de sigilo, é possível que indivíduos ou objetos que não alvos originais sejam alcançados. Isso ocorre porque estes métodos violam o sigilo da pessoa investigada e, em decorrência disso, torna impossível limitar a extensão do que será identificado como elemento de prova pelo agente interceptador.

Este é o fenômeno denominado de serendipidade, que busca abranger, de igual forma, a possibilidade de que outros interlocutores ainda não focados por uma investigação possam ser nela incluídos em face de elementos incriminadores. A utilização de prova telemática, para esta hipótese, também é permitida no processo penal nacional, como explica Luiz Flávio Gomes e Silvio Maciel:

> Mas no curso da captação da comunicação telefônica ou telemática podem surgir outros fatos penalmente relevantes, distintos da “situação objeto da investigação”. Esses fatos podem envolver o investigado ou outras pessoas. De outro lado, podem aparecer outros envolvidos, com o mesmo fato investigado ou com outros fatos, diferentes do que motivou a decretação da interceptação. É nisso que reside o fenômeno da serendipidade, que significa procurar algo e encontrar coisa distinta (buscar uma coisa e descobrir outra,

[105] TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. Curso de Direito Processual Penal. 12. ed. Salvador: JusPodivm, 2017, p. 632.

> estar em busca de um fato ou uma pessoa e descobrir outro ou outra por acaso).[106]

Desta forma, como forma de evitar o uso do *male captum, bene retentum*, consequência da teoria da proporcionalidade, de forma indiscriminada, o Direito nacional admitiu por estes dois caminhos como exceção, com fim de afastar os excessos que possam sobrevir do comportamento antijurídico da coleta de provas por meios ilícitos. Sendo, portanto, afastadas as palavras do processualista José Carlos Barbosa Moreira, de que sempre haverá cabimento em discussão do caso em particular: "a gravidade do caso, a índole da relação jurídica controvertida, a dificuldade para o litigante demonstrar a veracidade de suas alegações mediante procedimentos perfeitamente ortodoxos, o vulto do dano causado e outras circunstâncias" (MOREIRA, 1997, p. 109).

3.6.1 A Jurisprudência do Superior Tribunal de Justiça

Na década de 1990, entendia o Superior Tribunal de Justiça pela utilização do princípio da razoabilidade. Tal entendimento pôde ser visto no julgar do *Habeas Corpus* n.º 3.982/RJ[107], cujo relator, o Min. Adhemar Maciel, invocou o princípio constitucional da razoabilidade a fim de afastar o caráter absoluto da garantia constitucional do inc. LVI:

> Constitucional e Processo Penal. Habeas Corpus. Escuta telefônica com ordem judicial. Réu condenado por formação de quadrilha armada, que se acha cumprindo pena em penitenciária, não tem como invocar direitos fundamentais próprios do homem livre para trancar ação penal (corrupção ativa) ou destruir gravação feita pela polícia. O inciso LVI do artigo 5º da Constituição, que fala 'são inadmissíveis as provas obtidas por meio ilícito', não tem conotação absoluta. Há sempre um substrato ético a orientar o exegeta na busca de valores maiores na construção da sociedade. A própria Constituição Federal Brasileira, que é dirigente e programática, oferece ao juiz, através da 'atualização constitucional (verfassungsaktualisierung), base para o entendimento de que a cláusula constitucional invocada é relativa. A jurisprudência norte-americana, mencionada em precedente do Supremo Tribunal Federal, não é tranqüila. Sempre é invocável o princípio da 'Razoabilidade' (Reasonableness). O 'princípio da exclusão das provas ilicitamente obtidas' (Exclusionary Rule) também lá pede temperamentos.

---

[106] GOMES, Luiz Flávio; CUNHA, Rogério Sanches. Legislação Criminal Especial, v. 6. 6. ed. São Paulo: Revista dos Tribunais, 2010, p. 591.

[107] Revista n.º 4 de Direito do Ministério Público do Estado do Rio de Janeiro. 1. ed. Rio de Janeiro: Órgão Cultural do MPRJ, 1996. p. 306. Disponível em: https://www.mprj.mp.br/servicos/revista-do-mp/revista-04.

> Ordem denegada. (STJ, HC n.º 3.982/RJ, 6ª Turma, Rel. Min. Adhemar Maciel, Julgado em 05/12/1995)

O caso em tela trata de um *habeas corpus* impetrado pelo preso Waldemir Paes Garcia, um bicheiro da cidade do Rio de Janeiro que fora preso em 1992 junto a outros treze por ação da juíza Denise Frossard[108], mostra-se também interessante por se discutir o instrumento da escuta telefônica em ano anterior a entrada em vigor da Lei de Interceptações Telefônicas, de 1996.

Em seu voto, o Min. Adhemar Maciel ameniza tanto o princípio da exclusão das provas obtidas ilicitamente, quanto a doutrina dos frutos da árvore envenenada por meio do princípio da razoabilidade, uma vez que parte das provas teriam sido colhidas em cárcere, por meio de escuta autorizada judicialmente, sendo, desta forma, o requerente uma pessoa não livre que não deve usufruir de mesma intensidade de garantias e direitos constitucionais que o homem livre. É de se notar que em algumas passagens do acórdão há a argumentação de que houve carga probatória suficiente distinta da escuta, por isso há certa imprecisão do julgar para responder, de forma categórica, no que concerne a questão da eficácia de tal ato processual.

Todavia, o entendimento mais atual do Superior Tribunal de Justiça opta, claramente, pela inadmissibilidade da utilização de prova colhida ilicitamente, como é apresentado no acórdão do RHC n.º 89.981/MG[109], com relatoria do Min. Reynaldo Soares da Fonseca.

> PENAL E PROCESSO PENAL. RECURSO EM HABEAS CORPUS. FURTO E QUADRILHA. APARELHO TELEFÔNICO APREENDIDO. VISTORIA REALIZADA PELA POLÍCIA MILITAR SEM AUTORIZAÇÃO JUDICIAL OU DO PRÓPRIO INVESTIGADO. VERIFICAÇÃO DE MENSAGENS ARQUIVADAS. VIOLAÇÃO DA INTIMIDADE. PROVA ILÍCITA. ART. 157 DO CPP. RECURSO EM HABEAS CORPUS PROVIDO.
>
> 1. Embora a situação retratada nos autos não esteja protegida pela Lei n. 9.296/1996 nem pela Lei n. 12.965/2014, haja vista não se tratar de quebra sigilo telefônico por meio de interceptação telefônica, ou seja, embora não se trate violação da garantia de inviolabilidade das comunicações, prevista no

[108] OTÁVIO, Francisco. Tribunal de Justiça condenou bicheiros do Rio por quadrilha. Extra, 21 de outubro de 2012. Disponível em: https://extra.globo.com/noticias/brasil/tribunal-de-justica-condenou-bicheiros-do-rio-por-quadrilha-6474081.html.

[109] BRASIL. Superior Tribunal de Justiça. RHC 89.981/MG. Rel. Min. Reynaldo Soares da Fonseca, julgado em 05/12/2017, DJe de 13/12/2017. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1663002&num_registro=201702509663&data=20171213&formato=PDF.

> art. 5º, inciso XII, da CF, houve sim violação dos dados armazenados no celular do recorrente (mensagens de texto arquivadas - WhatsApp).
>
> 2. No caso, deveria a autoridade policial, após a apreensão do telefone, ter requerido judicialmente a quebra do sigilo dos dados armazenados, haja vista a garantia, igualmente constitucional, à inviolabilidade da intimidade e da vida privada, prevista no art. 5º, inciso X, da CF. Dessa forma, a análise dos dados telefônicos constante dos aparelhos dos investigados, sem sua prévia autorização ou de prévia autorização judicial devidamente motivada, revela a ilicitude da prova, nos termos do art. 157 do CPP. Precedentes do STJ.
>
> 3. Recurso em habeas corpus provido, para reconhecer a ilicitude da colheita de dados do aparelho telefônico dos investigados, sem autorização judicial, devendo mencionadas provas, bem como as derivadas, serem desentranhadas dos autos. (STJ, HC n.º 89.981/MG, 5ª Turma, Rel. Min. Reynaldo Soares da Fonseca, Julgado em 05/12/2017)

O caso versa a respeito do manuseio de provas resgatadas em telefone celular pela Polícia Civil do Estado de Minas Gerais após diligência de busca e apreensão. Teria a autoridade policial não se atentado a uma requisição pelo afastamento de sigilo dos dados armazenados no dispositivo, tendo, portanto, acesso a conversas pelo aplicativo WhatsApp. Em uma rápida e sintética decisão, a 5ª Turma entendeu pela não admissibilidade da prova, bem como pelo seu desentranhamento dos autos.

3.6.2 A Jurisprudência do Supremo Tribunal Federal

Mais constante é a compreensão vinda do Supremo Tribunal Federal em ser inflexível quanto ao uso da prova contaminada, como mostra a deliberação do ano de 2001 do *habeas* n.º 80.949/RJ[110], de relatoria do Min. Sepúlveda Pertence:

> EMENTA: I. Habeas corpus: cabimento: prova ilícita. 1. Admissibilidade, em tese, do habeas corpus para impugnar a inserção de provas ilícitas em procedimento penal e postular o seu desentranhamento: sempre que, da imputação, possa advir condenação a pena privativa de liberdade: precedentes do Supremo Tribunal. II. Provas ilícitas: sua inadmissibilidade no processo (CF, art. 5º, LVI): considerações gerais.
>
> 2. Da explícita proscrição da prova ilícita, sem distinções quanto ao crime objeto do processo (CF, art. 5º, LVI), resulta a prevalência da garantia nela estabelecida sobre o interesse na busca, a qualquer custo, da verdade real no processo: conseqüente impertinência de apelar-se ao princípio da proporcionalidade - à luz de teorias estrangeiras inadequadas à ordem

[110] BRASIL. Supremo Tribunal Federal. HC 80.949-9/RJ. Rel. Min. Sepúlveda Pertence, julgado em 30/10/2001, DJ de 14/12/2001. Disponível em https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=78579.

> constitucional brasileira - para sobrepor, à vedação constitucional da admissão da prova ilícita, considerações sobre a gravidade da infração penal objeto da investigação ou da imputação. III. Gravação clandestina de "conversa informal" do indiciado com policiais.
>
> 3. Ilicitude decorrente - quando não da evidência de estar o suspeito, na ocasião, ilegalmente preso ou da falta de prova idônea do seu assentimento à gravação ambiental - de constituir, dita "conversa informal", modalidade de "interrogatório" sub-reptício, o qual - além de realizar-se sem as formalidades legais do interrogatório no inquérito policial (C.Pr.Pen., art. 6º, V) -, se faz sem que o indiciado seja advertido do seu direito ao silêncio.
>
> 4. O privilégio contra a auto-incriminação - nemo tenetur se detegere -, erigido em garantia fundamental pela Constituição - além da inconstitucionalidade superveniente da parte final do art. 186 C.Pr.Pen. - importou compelir o inquiridor, na polícia ou em juízo, ao dever de advertir o interrogado do seu direito ao silêncio: a falta da advertência - e da sua documentação formal - faz ilícita a prova que, contra si mesmo, forneça o indiciado ou acusado no interrogatório formal e, com mais razão, em "conversa informal" gravada, clandestinamente ou não. IV. Escuta gravada da comunicação telefônica com terceiro, que conteria evidência de quadrilha que integrariam: ilicitude, nas circunstâncias, com relação a ambos os interlocutores.
>
> 5. A hipótese não configura a gravação da conversa telefônica própria por um dos interlocutores - cujo uso como prova o STF, em dadas circunstâncias, tem julgado lícito - mas, sim, escuta e gravação por terceiro de comunicação telefônica alheia, ainda que com a ciência ou mesmo a cooperação de um dos interlocutores: essa última, dada a intervenção de terceiro, se compreende no âmbito da garantia constitucional do sigilo das comunicações telefônicas e o seu registro só se admitirá como prova, se realizada mediante prévia e regular autorização judicial.
>
> 6. A prova obtida mediante a escuta gravada por terceiro de conversa telefônica alheia é patentemente ilícita em relação ao interlocutor insciente da intromissão indevida, não importando o conteúdo do diálogo assim captado.
>
> 7. A ilicitude da escuta e gravação não autorizadas de conversa alheia não aproveita, em princípio, ao interlocutor que, ciente, haja aquiescido na operação; aproveita-lhe, no entanto, se, ilegalmente preso na ocasião, o seu aparente assentimento na empreitada policial, ainda que existente, não seria válido.
>
> 8. A extensão ao interlocutor ciente da exclusão processual do registro da escuta telefônica clandestina - ainda quando livre o seu assentimento nela - em princípio, parece inevitável, se a participação de ambos os interlocutores no fato probando for incindível ou mesmo necessária à composição do tipo criminal cogitado, qual, na espécie, o de quadrilha. V. Prova ilícita e contaminação de provas derivadas (fruits of the poisonous tree). 9. A imprecisão do pedido genérico de exclusão de provas derivadas daquelas cuja ilicitude se declara e o estágio do procedimento (ainda em curso o inquérito policial) levam, no ponto, ao indeferimento do pedido. (STF, HC n.º 80.949/RJ, 1ª Turma, Rel. Min. Sepúlveda Pertence, DJU de 14/12/2001)

Neste paradigmático acórdão, é afastada de forma veemente a máxima *male captum, bene retentum*, principalmente de material colhido pelo Estado, em vistas de

conter abusos latentes de autoridades policiais. Neste aspecto o Tribunal preza pela repreensão a quaisquer atos semelhantes advindos da máquina estatal, considerando um mínimo ético que deverá ser trilhado para que se atinja uma pena[111]. Também houve a recepção à aplicação rigorosa da doutrina dos frutos da árvore envenenada, em desconformidade com o entendimento dado pelo Ministro Adhemar Maciel, do Superior Tribunal de Justiça no *Habeas Corpus* n.º 3.982/RJ. Desta forma, o ordenamento jurídico brasileiro vigente, seja por força de Lei, seja pela interpretação jurisprudencial, considera não somente pela inadmissibilidade e utilização da prova telemática colhida ilicitamente, como de todas as provas.

3.7 A insuficiência normativa e as soluções para modalidade de mensagens de aplicativos e o Projeto de Lei n.º 4.939/20 da Câmara dos Deputados

Não resta dúvidas de que o Projeto de Lei que tramita no Congresso Nacional é instrumento que poderá ter grande importância no atinente às investigações e às persecuções penais, uma vez que estabelece muitos conceitos de fenômenos da era digital de forma clara e apresenta um rol de meios de obtenção de provas na seara do direito informático, trazendo algumas novidades como a coleta de dados por acesso remoto forçado.

Este projeto, se aprovado, pretenderá ser uma lei que, além de sua matéria, promoverá uma ligação entre algumas legislações esparsas, como é o caso do Marco Civil da Internet, dado que o projeto objetiva ser um Marco Penal da Internet e da Lei de Interceptações Telefônicas, ao complementar métodos investigativos contemplados na Lei n.º 9.296/96. Em simultaneidade, o PL irá adicionar um novo rol de cibercrimes, bem como regular os métodos e procedimentos novos à instância processual trazendo, portanto, inovações também para o Direito Penal.

Já explicado e esmiuçado o que o Projeto de Lei trata, resta agora tentar apontar melhorias que trarão maior segurança jurídica quando tais medidas forem efetivas. Para tal, vê-se interessante complementar alguns pontos do PL n.º 4.939/20, serão eles: (i) providenciar mais algumas conceituações alheias à Lei brasileira e (ii)

[111] ANDRADE, Manuel da Costa. Sobre as Proibições de Prova em Processo Penal. Editora Coimbra, 1992, p. 15.

um incremento à medida de coleta por acesso forçado, pretendida no art. 12 do projeto.

O primeiro passo para melhoria deverá ser feito no espaço destinado à lista de significados presentes em seu artigo 3º, lugar em que há a significação de treze conceitos pertinentes ao assunto abordado, todavia ainda persiste a ausência de conceitos que não foram mencionados nem no PL, nem nas demais legislações correntes, são eles: uma classificação mínima acerca dos tipos de provedores a fim de construir necessárias separações de responsabilidades na esfera penal; o conceito de “dados”, juntamente ao inc. XIII que define “metadados”, e, por final, um conceito claro à palavra “telemático”.

No que se refere à nova modalidade de obtenção de provas apresentada pelo artigo 12, a coleta por acesso forçado, precisará ter seu procedimento devidamente regrado, por tender a ser um dos métodos mais invasivos de devassa no ordenamento penal brasileiro. Os moldes do sistema legal espanhol apresentam uma interessante saída ao pôr requisitos específicos ao uso de aplicativos de vigilância, contudo terá de se demandar, com a finalidade de assegurar a justiça, por programas que não propiciem a interferência ativa dos investigadores, além de possibilitarem uma extração de dados sem que haja quebra na integridade e autenticidade do conteúdo retirado.

Em último lugar, há a incumbência de se dar início a uma discussão séria à criptografia, em especial a ponta a ponta, entre o Estado brasileiro com as plataformas que oferecem este recurso, dado que a tecnologia é hostil aos meios de coleta de prova abrangidos pelo PL n.º 4.939/20. Atualmente tanto aplicativos de mensageiros instantâneos quanto serviços de armazenamento em nuvem, incluindo serviços de *e-mail*, ofertam este recurso.

Sem que haja uma solução protagonizada pelo governo brasileiro, a maioria dos meios de obtenção de prova do projeto estarão obsoletos no instante que a lei for promulgada. Sabe-se que o Brasil é um dos países mais importantes na área de mineração de dados, essa mineração é uma das principais atividades que sustentam buscadores, navegadores e redes sociais, que tem a oportunidade de coletar

informações referentes aos hábitos dos usuários para o aprimoramento de seus algoritmos que tem por finalidade maximizar o consumo[112].

O Brasil é o quinto país mais conectado com a Internet do mundo[113] e o segundo mercado mais importante para empresa WhatsApp, ao ter cerca de 119 milhões de usuários em sua rede[114], o país poderá se valer desta realidade para tratar sobre uma saída em que tais empresas, não só a WhatsApp, possam colaborar com o Poder Público.

[112] LISBOA, Alveni. Como o WhatsApp ganha dinheiro? Canaltech, 08 de maio de 2022. Disponível em: https://canaltech.com.br/apps/como-o-whatsapp-ganha-dinheiro-215340/.
[113] Redação Finanças. Brasil é o quinto país que mais acessa internet no mundo. Yahoo Finanças, 14 de outubro de 2022. Disponível em: https://br.financas.yahoo.com/noticias/brasil-e-o-quinto-pais-com-mais-internautas-no-mundo-140153847.html.
[114] WhatsApp Users in Select Countries, 2020 & 2021. Insider Intelligence, 01 de junho de 2021. Disponível em: https://www.insiderintelligence.com/chart/249914/whatsapp-users-select-countries-2020-2021-millions.

CONSIDERAÇÕES FINAIS

O Projeto de Lei n.º 4.939/20 pretende-se ser um novo regramento que possa guiar o Direito Penal e o Direito Processual Penal na esfera digital, agregando-se, desta forma, à Lei de Interceptação Telefônica e ao Marco Civil da Internet, buscando dar coesão entre ordenamento jurídico e as novas tecnologias em vigor na sociedade moderna.

Eleva-se, portanto, a um elo que se manifesta em face à revolução tecnológica, uma vez que a indústria da telecomunicação oferece progressivamente mais instrumentos para o uso cotidiano do cidadão comum. À medida que um número de pessoas maior usufrui mais das redes em detrimento de tecnologias anteriores, urge-se a necessidade de uma regulação mais adequada a estes novos meios.

Com esse propósito, o PL visa querer regular tanto no espectro do direito material, quanto no espectro do direito processual. No atinente a este último, o a proposta consolida as técnicas especiais de investigação já existentes na Lei das Interceptações, como o caso da interceptação telemática em transmissão e no Código de Processo Penal, na hipótese da busca e apreensão de dispositivos telemáticos de comunicação e de transmissão e dados.

Outrossim, tenderá, ao mesmo tempo, tornar-se fonte primária a outras técnicas de investigação corriqueiras sustentadas com base na exceção da inviolabilidade do sigilo de dados na circunstância da coleta remota de comunicações e dados telemáticos em repouso acessados à distância. Ademais será inovadora na situação da coleta por acesso forçado de sistema telemático, forma de apuração totalmente alheia à legislação brasileira.

Contudo, nenhum dos meios de obtenção de prova serão úteis se não houver diálogo entre o governo brasileiro e as atuais empresas de tecnologia no assunto da crescente evolução dos recursos de criptografia, uma vez que este se torna um adversário desafiador frente a todos os métodos previstos no projeto. Para tal, em caso de negativa disposição das empresas em resolver estes impasses, precisará o governo, por meio de seus legisladores, executores e julgadores, encontrar alguma

maneira de submeter essas empresas ao regime jurídico brasileiro, sob pena de não poderem mais atuar no mercado brasileiro.

REFERÊNCIAS

ANDRADE, Manuel da Costa. **Sobre as Proibições de Prova em Processo Penal**. 1. ed. Portugal: Editora Coimbra, 1992.

AVOLIO, Luiz Francisco Torquato. **Provas Ilícitas: Interceptações telefônicas, ambientais e gravações clandestinas**. 6. ed. São Paulo: Editara Revista dos Tribunais, 2015.

AYCOCK, John. **Spyware and Adware**. 1. ed. Estados Unidos: Springer, 2011.
BADARÓ, Gustavo Henrique Righi Ivahy. **Processo Penal**. 9. ed. São Paulo: Thomson Reuters Brasil, 2021. *E-book*.

BEAL, Vangie. **Email Services**. Webopedia, 05 de janeiro de 2011. Disponível em https://www.webopedia.com/definitions/email-services/. Acesso em 09 fev. 2023.

BOBBIO, Norberto. **A Era dos Direitos**. Tradução Carlos Nelson Coutinho; apresentação de Celso Lafer. Nova ed. Rio de Janeiro: Elsevier, 2004.

BRASIL. **Constituição Federal de 1988**. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 09 fev. 2023.

BRASIL. **Decreto Lei n.º 3.689, de 03 de outubro de 1941**. Código de Processo Penal. Brasília, DF. Disponível em: http://www.planalto.gov.br/CCIVIL/Decreto-Lei/Del3689.htm. Acesso em 09 fev. 2023.

BRASIL. **Lei n.º 9.296, de 24 de julho de 1996**. Brasília, DF. Dispõe sobre a interceptação telefônica e outras medidas. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 27 mar. 2023.

BRASIL. **Lei n.º 9.472, de 16 de julho de 1997**. Brasília, DF. Dispõe sobre a organização dos serviços de telecomunicações. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Acesso em 08 fev. 2023.

BRASIL. **Lei n.º 11.419, de 19 de dezembro de 2006**, que dispõe sobre a informatização do processo judicial, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em 27 fev. 2023.

BRASIL. **Lei n.º 12.850, de 2 de agosto de 2013**. Brasília, DF. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em 09 fev. 2023.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Brasília, DF. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 08 fev. 2023.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 13 fev. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei n.º 4.939/20**. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1936366&filename=PL%204939/2020. Acesso em 08 fev. 2023.

BRASIL. Superior Tribunal de Justiça. **HC 315.220/RS**. Rel. Min. Maria Thereza de Assis Moura, julgado em 15/09/2015, DJe de 09/10/2015, p. 31-32. Disponível em https://www.conjur.com.br/dl/hc-315220-quebra-sigilo-telematico-dez.pdf. Acesso em 23 mar. 2023.

BRASIL. Superior Tribunal de Justiça. **RHC 75.800/PR**. Rel. Min. Felix Fischer, julgado em 15/09/2016, DJe de 26/09/2016. Disponível em: https://www.conjur.com.br/dl/busca-apreensao-celular-autoriza-acesso.pdf. Acesso em 23 mar. 2023.

BRASIL. Superior Tribunal de Justiça. **RHC 89.981/MG**. Rel. Min. Reynaldo Soares da Fonseca, julgado em 05/12/2017, DJe de 13/12/2017. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1663002&num_registro=201702509663&data=20171213&formato=PDF. Acesso em 23 mar. 2023.

BRASIL. Supremo Tribunal Federal. **HC 80.949-9/RJ**. Rel. Min. Sepúlveda Pertence, julgado em 30/10/2001, DJ de 14/12/2001. Disponível em https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=78579. Acesso em 06 mar. 2023.

BRASIL. Supremo Tribunal Federal. **INQ 2.424-4/RJ**. Rel. Min. Cezar Peluso. Julgado em 25/04/2007. DJ de 24/08/2007. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=481962. Acesso em 27 mar. 2023.

BRASIL. Supremo Tribunal Federal. **MS 23.452/RJ**. Rel. Min. Celso de Mello. Julgado em 16/09/1999, DJ de 12/05/2000. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=85966. Acesso em 06 mar. 2023.

CAPEZ, Fernando. **Curso de Direito Penal, v. 4, Legislação Penal Especial**. 13. ed. São Paulo: Saraiva Jur.

CARVALHO, Caio. **O que é o spyware Pegasus?** Canaltech, 25 de setembro de 2021. Disponível em: https://canaltech.com.br/seguranca/o-que-e-o-spyware-pegasus/. Acesso em 02 mar. 2023.

CEROY, Frederico Meinberg. **Os conceitos de provedores no Marco Civil da Internet**. 20 de setembro de 2020. Migalhas. Disponível em: https://www.migalhas.com.br/depeso/211753/os-conceitos-de-provedores-no-marco-civil-da-internet. Acesso em 23 fev. 2023.

CHAPPLE, Mike. **What Is Metadata?** ThoughtCo, 18 de novembro de 2021. Tradução nossa. Disponível em: https://www.thoughtco.com/metadata-definition-and-examples-1019177. Acesso em 09 fev. 2023.

COSTA JÚNIOR, Ivan Jezler. **Prova Penal Digital: Tempo, Risco e Busca Telemática**. 1. ed. Florianópolis: Tirant lo Blanch, 2019. *E-book*.

COUTINHO, Mariana. **O que é criptografia de ponta-a-ponta? Entenda o recurso de privacidade**. Techtudo, 12 de junho de 2019. Disponível em: https://www.techtudo.com.br/noticias/2019/06/o-que-e-criptografia-de-ponta-a-ponta-entenda-o-recurso-de-privacidade.ghtml. Acesso em 09 fev. 2023.

DEZEM, Guilherme Madeira. **Da Prova Penal**. 1. ed. São Paulo: Millenium, 2008.

DISTRITO FEDERAL. **Dados em Nuvem - Inaplicabilidade da lei 9.296/96**. 04 de fevereiro de 2021, TJDFT. Disponível em: https://www.tjdft.jus.br/consultas/jurisprudencia/decisoes-em-evidencia/4-2-2021-2013-dados-em-nuvem-2013-inaplicabilidade-da-lei-9-296-96-2013-tjdft. Acesso em 13 fev. 2023.

DORE, Eder. **O que é Telemática?** Maplink, 16 de março de 2020. Disponível em: https://maplink.global/blog/o-que-e-telematica/. Acesso em: 07 fev. 2023.

ESPANHA. **Código de Processo Penal Espanhol**. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036. Acesso em 01 mar. 2023.

EUROPA. **Convenção n.º 108 do Conselho da Europa de 1981**. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf. Acesso em 08 fev. 2023.

FANTINATO, Giovanna. **Cellebrite: conheça o software usado na investigação do caso Henry**. Tecmundo, 12 de abril de 2021. Disponível em https://www.tecmundo.com.br/software/215422-cellebrite-conheca-software-usado-investigacao-caso-henry.htm. Acesso em 02 mar. 2023.

GOGONI, Ronaldo. **Os riscos da rede 2G e por que desligá-la não é tão simples**. 2022. Disponível em https://meiobit.com/456885/redes-2g-ataques-desligamento-nada-simples/. Acesso em 08 fev. 2023.

GOMES, Luiz Flávio; CUNHA, Rogério Sanches. **Legislação Criminal Especial, v. 6**. 6. ed. São Paulo: Revista dos Tribunais, 2010.

GOMES, Luiz Flávio; SILVA, Marcelo Rodrigues da. **Organizações Criminosas e Técnicas Especiais de Investigação**. 1. ed. Salvador: JusPodivm, 2015.

GOMES FILHO, Antonio Magalhães. **Estudos em Homenagem à Professora Ada Pellegrini Grinover: notas sobre a terminologia da prova (reflexos no processo penal brasileiro)**. 1. ed. São Paulo: DPJ, 2005.

HESSE, Brendan. **The Best WhatsApp Alternatives**. LifeHacker, 07 de janeiro de 2021. Disponível em: https://lifehacker.com/the-best-whatsapp-alternatives-1832064581. Acesso em 09 fev. 2023.

Informações sobre aplicação da lei. Grupo Meta. Disponível em: https://www.facebook.com/help/instagram/494561080557017/?helpref=uf_share. Acesso em 23 fev. 2023.

Law Enforcement Requests Report. Microsoft Corporation. Disponível em: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report. Acesso em 23 fev. 2023.

Law Enforcement Requests Tracker. Amazon Inc. Disponível em: https://ler.amazon.com/us. Acesso em 23 fev. 2023.

LEONARDI, Marcel. **Responsabilidade Civil dos Provedores de Serviços de Internet**. 1. ed. São Paulo: Editora Juarez de Oliveira, 2005.

LIMA, Renato Brasileiro de. **Código Processual Penal Comentado**. 2. ed. Salvador: JusPodivm, 2017.

LIMA, Renato Brasileiro de. **Legislação Criminal Especial Comentada**. 8. ed. Salvador: JusPodivm, 2020.

LISBOA, Alveni. **Como o WhatsApp ganha dinheiro?** Canaltech, 08 de maio de 2022. Disponível em: https://canaltech.com.br/apps/como-o-whatsapp-ganha-dinheiro-215340/. Acesso em 12 abr. 2023.

LOPES, Diogo. **Tudo sobre perícia em celulares e o papel do perito em celular**. Ipericias, 09 de março de 2021. Disponível em https://lpericias.com.br/tudo-sobre-pericia-em-celulares-e-o-papel-do-perito-em-celular/. Acesso em 09 fev. 2023.

LOPES JUNIOR, Aury. **Direito Processual Penal**. 17. ed. São Paulo: Saraiva, 2020. *E-book*.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 16. ed. São Paulo: Saraiva Educação, 2021.

MESQUITA, Márcio Satalino. **Crimes Cibernéticos: Investigação e provas**. 1. Ed. EMAG TRF-3, 2017.

MORAES, Alexandre de. **Direito Constitucional**. 24. ed. São Paulo: Editora Atlas, 2009.

MOREIRA, José Carlos Barbosa. **Temas de Direito Processual**. 6. ed. São Paulo: Editora Saraiva, 1997.

NOVELINO, Marcelo. **Curso de Direito Constitucional**. 11. ed. Salvador: JusPodivm, 2016.

NUCCI, Guilherme de Souza. **Prova no Processo Penal**. 4. ed. Rio de Janeiro: Forense, 2015. *E-book*.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**, 1948. Disponível em: https://www.oas.org/dil/port/1948%20Declaração%20Universal%20dos%20Direitos%20Humanos.pdf. Acesso em 08 fev. 2023.

OTÁVIO, Francisco. **Tribunal de Justiça condenou bicheiros do Rio por quadrilha**. Extra, 21 de outubro de 2012. Disponível em: https://extra.globo.com/noticias/brasil/tribunal-de-justica-condenou-bicheiros-do-rio-por-quadrilha-6474081.html. Acesso em 27 mar. 2023.

Perguntas e Respostas: Grampos telefônicos. Veja, 05 de dezembro de 2008. Disponível em: https://web.archive.org/web/20121227133554/http://veja.abril.com.br/idade/exclusivo/perguntas_respostas/grampos-telefonicos/escuta-telefonica-espionagem-investigacao-lei-policia-cpi.shtml. Acesso em 23 mar. 2023.

RAMOS JUNIOR, Durval. **Conheça os vários tipos de conexão**. 20 de janeiro de 2010. Disponível em: https://www.tecmundo.com.br/banda-larga/3489-conheca-os-varios-tipos-de-conexao.htm. Acesso em 08 fev. 2023.

Redação Finanças. **Brasil é o quinto país que mais acessa internet no mundo**. Yahoo Finanças, 14 de outubro de 2022. Disponível em: https://br.financas.yahoo.com/noticias/brasil-e-o-quinto-pais-com-mais-internautas-no-mundo-140153847.html. Acesso em 12 abr. 2023.

Redação Minha Operadora. **Vivo religa sua rede CDMA**. 22 de janeiro de 2013. Disponível em: https://www.minhaoperadora.com.br/2013/01/vivo-religa-sua-rede-cdma.html. Acesso em 08 fev. 2023.

Reforma do Código de Processo Penal pode aumentar vigilância e precisa de equilíbrio em questões de tecnologia. Coalizão Direitos na Rede, 20 de maio de 2021. Disponível em: https://direitosnarede.org.br/2021/05/20/reforma-do-codigo-de-processo-penal-pode-aumentar-vigilancia-e-precisa-de-equilibrio-em-questoes-de-tecnologia/. Acesso em 01 mar. 2023.

RODRIGUES, Benjamin Silva. **Da prova penal: v. IV - Da prova-electrónico-digital e da criminalidade informático-digital**. 1. ed. Lisboa: Rei dos Livros, 2011.
ROSENBERG, Jothy; MATEOS, Arthur. **The Cloud at Your Service**. 1. ed. Connecticut: Manning Publications, 2011.

SANTOS, Ricardo Di Lucia. **Redes GSM, GPRS, EDGE e UMTS**. UFRJ, 2008. Disponível em: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2008_2/ricardo/4.html. Acesso em 08 fev. 2023.

Sistema de Solicitação de Aplicação da Lei. Google. Disponível em: https://lers.google.com/signup_v2/landing. Acesso em 27 fev. 2023.

Solicitações Online para Autoridades Públicas. WhatsApp LLC. Disponível em: https://www.whatsapp.com/records/login/?locale=pt_BR&lang=pt_br. Acesso em 23 fev. 2023.

STALLINGS, William. **Criptografia e segurança de redes: princípios e práticas**. Tradução de Daniel Vieira, 6. ed. São Paulo: Pearson Education do Brasil, 2015.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**. 12. ed. Salvador: JusPodivm, 2017.

WhatsApp Users in Select Countries, 2020 & 2021. Insider Intelligence, 01 de junho de 2021. Disponível em: https://www.insiderintelligence.com/chart/249914/whatsapp-users-select-countries-2020-2021-millions. Acesso em 12 abr. 2023.

ANEXO A – Projeto de Lei n.º 4.949/20

CÂMARA DOS DEPUTADOS
Gabinete do Deputado Federal **HUGO LEAL** – PSD/RJ

PROJETO DE LEI Nº , de 2020.

(Do Senhor Hugo Leal).

Dispõe sobre as diretrizes do direito da Tecnologia da Informação e as normas de obtenção e admissibilidade de provas digitais na investigação e no processo, além de outras providências.

O Congresso Nacional decreta**:**

CAPÍTULO I
Das Disposições Gerais.

Art. 1º Esta Lei estabelece princípios e diretrizes na aplicabilidade do Direito da Tecnologia da Informação, bem como normas de obtenção e admissibilidade de provas digitais na investigação e no processo, definindo crimes e penas.

Parágrafo único: As normas contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

Art. 2º - Esta Lei será pautada pelos seguintes fundamentos:

I - Direito fundamental à proteção de dados, assegurando-se o seu uso de forma adequada, necessária e proporcional;

II - A garantia de acesso dos legítimos interessados à prova digital sob controle ou disponibilidade de terceiros;

III - Respeito à soberania nacional;

IV - A cooperação jurídica internacional;

V - Garantia de autenticidade e da integridade da informação;

VI - A Preservação da Empresa e sua função social;

VII - Transparência dos meios de tratamento da informação.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 3º Para feitos desta Lei considera-se:

I - Dispositivo eletrônico: Qualquer equipamento, instrumento ou componente que dependa para seu funcionamento dos princípios da eletrônica e use a manipulação do fluxo de elétrons para seu funcionamento.

II - Sistema Informático: Conjunto de dispositivos eletrônicos inter-relacionados que coletam, processam, armazenam e distribuem informações.

III - Protocolos de rede: Regras sobre como ocorrerá a comunicação entre dispositivos eletrônicos segundo padrões pré-determinados.

IV - Redes de Dados: Conjunto de dois ou mais dispositivos eletrônicos interligados por um sistema informático e guiados por protocolos de rede para compartilhar entre si informação e serviços.

V - Pacotes de dados: Estrutura unitária de transmissão de informação em uma rede de dados.

VI - Dados em transmissão: dados encapsulados em pacotes trafegando por redes segundo protocolos determinados.

VII - Dados em repouso: dados que se encontram armazenados em um dispositivo eletrônico ou sistema informático.

VIII - Prova nato-digital: informação gerada originariamente em meio eletrônico.

IX - Prova digitalizada: informação originariamente suportada por meio físico e posteriormente migrada para armazenamento em meio eletrônico, na forma da Lei.

X - Integridade da prova: certeza de que a informação que a constitui se mantém inalterada após o seu tratamento.

XI - Autenticidade da prova: certeza da sua origem, contexto ou autoria.

XII - Interceptação: coleta de dados em transmissão através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros.

XIII - Metadados: qualquer informação sobre outra informação armazenada em meio eletrônico que identifique ou revele a origem, datas e horários relevantes e qualquer outra circunstância relativa ao contexto da evidência digital.

Art. 4º Considera-se prova digital toda informação armazenada ou transmitida em meio eletrônico que tenha valor probatório.

Parágrafo Único - À prova digital aplicam-se subsidiariamente as disposições relativas às provas em geral.

Art. 5º A admissibilidade da prova nato-digital ou digitalizada na investigação e no processo exigirá a disponibilidade dos metadados e a descrição dos procedimentos de custódia e tratamento suficientes para a verificação da sua autenticidade e integridade.

Parágrafo Único: Caso a prova digital seja produto de tratamento de dados por aplicação de operação matemática ou estatística, de modo automatizado ou não, devem estar transparentes os parâmetros e métodos empregados, de modo a ser possível a sua repetição e reprodutibilidade.

Art. 6º Poderão os legítimos interessados, para o fim da investigação ou instrução processual, requerer ordem judicial para guarda e acesso a prova digital sob controle de terceiros, observados os requisitos de necessidade, adequação e proporcionalidade.

§ 1º O requerimento deve individualizar usuários, provedores, dispositivos eletrônicos ou sistemas informáticos, temporalidades,

redes de dados e protocolos de rede próprios ao contexto do legítimo interesse manifestado, não podendo ter caráter genérico.

§ 2º Os dados encaminhados, transmitidos ou em suporte físico, pelos controladores ou provedores em cumprimento de ordem judicial ou requisição da autoridade policial e do Ministério Público devem estar em formato interoperável e com garantia de autenticidade e integridade.

Art. 7º Os provedores de infraestrutura, conexão e aplicação deverão manter, além das informações de guarda legal previstas em lei, os registros de dados necessários e suficientes para a individualização inequívoca dos usuários de seus serviços pelo prazo de 1 (um) ano.

Art. 8º Se houver receio de que a prova digital possa perder-se, alterar-se ou deixar de estar disponível, poderá o juiz, a requerimento do legítimo interessado, ordenar a quem tenha disponibilidade, controle ou opere os dados, que os guarde pelo prazo de até 1 (um) ano, podendo este prazo ser renovado, observadas a necessidade, adequação e proporcionalidade.

CAPÍTULO II
DA PROVA DIGITAL NA INVESTIGAÇÃO E NO PROCESSO PENAL
Seção I
Dos Meios de obtenção.

Art. 9º Constituem meios de obtenção da prova digital, na forma da Lei:

I – a busca e apreensão de dispositivos eletrônicos, sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica, e o tratamento de seu conteúdo.

II – a coleta remota, oculta ou não, de dados em repouso acessados à distância.

III – a interceptação telemática de dados em transmissão.

IV – a coleta por acesso forçado de sistema informático ou de redes de dados.

V – o tratamento de dados disponibilizados em fontes abertas, independentemente de autorização judicial.

Seção II
Interceptação Telemática

Art. 10 A interceptação telemática poderá ser destinada aos provedores ou serviços de infraestrutura, de conexão ou aplicação, bem como aos dispositivos eletrônicos ou sistemas informáticos particulares, devendo ser individualizadas as redes de dados e os protocolos de internet envolvidos.

Parágrafo Único. A interceptação telemática seguirá subsidiariamente o procedimento estabelecido para a interceptação telefônica.

Seção III
Requisição itinerante

Art. 11 O provedor de infraestrutura, de conexão ou de aplicação em face da qual tenha sido expedida a diligência, constatando que a medida deve ser cumprida por outro provedor, remeterá a requisição a este em caráter itinerante, a fim de se praticar o ato, independentemente de nova ordem, comunicando-se à autoridade judicial ou ao órgão de investigação em 24 (vinte e quatro) horas.

Parágrafo Único. Os provedores em face da qual tenha sido ordenada a diligência indicará à autoridade judiciária e ao órgão de investigação em 24 (vinte e quatro) horas os outros provedores através das quais tenha tido conhecimento da ocorrência de tráfego de dados pertinentes ao alvo da interceptação, com o fim de identificar todas os provedores envolvidos.

Seção IV
Coleta por Acesso Forçado

Art. 12 A coleta por acesso forçado a dispositivo eletrônico, sistema informático ou redes de dados, ocorrerá somente após prévia desobediência de ordem judicial determinando a entrega da prova pretendida ou quando impossível identificar o controlador ou provedor em território nacional, e compreenderá os métodos de

segurança ofensiva ou qualquer outra forma que possibilite a exploração, isolamento e tomada de controle.

Seção V
Decisão judicial e prazo

Art. 13 A ordem judicial para obtenção da prova digital para fins de investigação e processo penal descreverá os fatos investigados com a indicação da materialidade e possível autoria delitiva, indicando ainda os motivos, a necessidade e os fins da diligência, estabelecendo os limites da atividade a ser empreendida e o prazo para seu cumprimento.

§ 1º Em caso de monitoramento do fluxo de dados, o prazo da medida não poderá exceder a 60 (sessenta) dias, permitidas prorrogações por igual período, desde que continuem presentes os pressupostos autorizadores da diligência, até o máximo de 360 (trezentos e sessenta) dias, salvo quando se tratar de crime permanente, enquanto não cessar a permanência.

§ 2º A obtenção da prova digital pode se dirigir a uma terceira pessoa, desde que haja indícios de que o investigado utilize o dispositivo eletrônico, ou quaisquer outros meios de armazenamento de informação eletrônica, com ou sem o conhecimento do proprietário.

§ 3º O órgão de investigação ou o Ministério Público poderá requisitar a guarda da prova digital sem acesso ao conteúdo pelo prazo de 1 (um) ano, independentemente de autorização judicial, quando houver perigo na demora, devendo comunicar a medida ao juiz competente em até 24 (vinte e quatro) horas, para validação da medida.

Seção VI
Mandado judicial

Art. 14 A decisão judicial será instrumentalizada por mandado judicial, dirigido aos seus executores e às pessoas físicas ou jurídicas que irão sofrê-la, suficientemente instruído com informações sobre os fatos sob investigação, a pessoa física ou jurídica alvo da diligência, se possível, os dispositivos eletrônicos,

sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica, se for o caso, os provedores ou serviços de infraestrutura, de conexão ou de aplicação, potencialmente atingidos, o objeto da medida, os procedimentos autorizados a serem efetuados, os limites da apreensão e o prazo para cumprimento.

Parágrafo Único Será expedido mandado de intimação aos interessados, nos termos do caput, logo após o fim do cumprimento da medida, desde que não prejudique a operação.

Seção VII
Termo Circunstanciado

Art. 15 Ao fim da diligência para obtenção da prova digital, o órgão de investigação lavrará auto circunstanciado, com declaração do lugar, dia e hora em que se realizou, com menção das pessoas que a sofreram e das que nela tomaram parte ou a tenham assistido, com as respectivas identidades, bem como de todos os incidentes ocorridos durante a sua execução, especificando-se os procedimentos adotados e equipamentos utilizados.

Art. 16 Caso a diligência para obtenção da prova digital seja positiva, constará do auto circunstanciado a relação e descrição das coisas e dos dados apreendidos, bem como dos métodos de preservação de sua autenticidade e integridade.

Art. 17 O cumprimento da diligência será comunicado à autoridade judicial competente, no prazo de 72 (setenta e duas) horas, informando-se do seu resultado e do encaminhamento conferido aos objetos coletados e apresentando-se cópia do auto circunstanciado.

Seção VIII
Cadeia de Custódia Específica

Art. 18 Além do auto circunstanciado, será elaborado o registro da custódia do que foi apreendido na diligência, indicando os custodiantes e as transferências havidas, bem como as demais operações realizadas em cada momento da cadeia.

Art. 19 Os meios de obtenção da prova digital serão implementados por perito oficial ou assistente técnico da área de informática, que deverão proceder conforme as boas práticas aplicáveis aos procedimentos a serem desenvolvidos, cuidando para que se preserve a integridade, a completude, a autenticidade, a auditabilidade e a reprodutibilidade dos métodos de análise.

§ 1º A realização da obtenção garantirá, independentemente de norma técnica:

I - ambiente controlado com redução de contaminação;

II - espelhamento técnico em duas cópias, com o máximo de metadados e a descrição completa de procedimentos, datas, horários ou outras circunstâncias de contexto aplicáveis;

III - preservação imediata após o ato de espelhamento com emprego de recurso confiável que garanta a integridade da prova.

§ 2º A autoridade judicial, mediante requerimento do órgão de investigação ou do interessado, requisitará aos controladores o encaminhamento de dados pessoais associados à prova digital obtida e que sejam complementares e suficientes para a sua análise contextual.

Art. 20 Uma cópia dos dados resultantes da diligência, feita por espelhamento, será encaminhada e armazenada pela autoridade judicial competente, para eventual confronto. As análises, as pesquisas e os exames periciais devem ser realizados sobre cópia de trabalho.

Art. 21 Salvo expressa determinação judicial em contrário ou impossibilidade de cumprimento da medida desta forma, a apreensão da prova digital ocorrerá por espelhamento, não se fazendo a apreensão de dispositivos eletrônicos, sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica.

Seção IX
Restituição de dispositivos eletrônicos ou sistemas informáticos

Art. 22 Em caso de impossibilidade de apreensão por espelhamento, será garantida aos titulares ou agentes de tratamento atingidos pela apreensão dos dispositivos eletrônicos, sistemas informáticos ou outros meios de armazenamento de informação eletrônica cópia dos dados coletados. A apreensão não poderá superar 60 (sessenta) dias, salvo por motivo relevante.

Seção X
Sigilo profissional e religioso

Art. 23 Os meios de obtenção da prova digital observarão o sigilo em razão de função, ministério, ofício ou profissão, incluindo, mas não se limitando, o sigilo médico, religioso e o sigilo da relação advogado e cliente, ressalvados os casos em que o exercício da atividade represente ou preste-se a encobrir a atuação delitiva.

Seção XI
Dados íntimos e restrições de acesso à informação

Art. 24 Os dados pessoais sensíveis, íntimos ou sigilosos do investigado, acusado ou pessoas a ele relacionadas, que sejam relevantes ao caso, mas que não digam respeito aos demais sujeitos processuais, serão apartados em autos próprios, mantendo-se acessíveis apenas aos interessados, vedada a alteração do espelhamento.

§ 1º Decorridos 05 (cinco) anos do cumprimento integral da sentença condenatória ou em caso de absolvição ou de decretação de extinção de punibilidade, os dados mencionados no caput serão indisponibilizados, desde que não haja interesse público na preservação ou que não tenham relevância ou pertinência processual, devendo ser intimados os interessados e atualizada a garantia de integridade e anterioridade dos dados remanescentes.

§ 2º Os dados que se enquadrem nas restrições de acesso à informação, nos termos da Lei, serão apartados em autos próprios e encaminhados em 24 (vinte e quatro) horas à autoridade competente, vedada a alteração do espelhamento.

Seção XII
Encontro fortuito e serendipidade

Art. 25 Se, na coleta da prova digital judicialmente autorizada, houver o encontro fortuito de dados relacionados a fatos diversos, estes deverão ser remetidos como notícia crime ao órgão de investigação.

Seção XIII
Infiltração virtual

Art. 26 A infiltração de agentes de investigação em redes de dados, conectadas entre si ou não, com o fim de investigar crimes punidos com pena privativa de liberdade máxima igual ou superior a 4 (quatro) anos, obedecerá às seguintes regras:

I – será precedida de autorização judicial, mediante requerimento do Ministério Público, órgão de investigação ou representação de delegado de polícia, que conterá a demonstração de sua necessidade, o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a individualização dessas pessoas;

II – não poderá exceder o prazo de 60 (sessenta) dias, sem prejuízo de eventuais renovações, desde que o total não exceda a 360 (trezentos e sessenta) dias e seja demonstrada sua efetiva necessidade, salvo quando se tratar de crime permanente, enquanto não cessar a permanência.

§ 1º A autoridade judicial, o órgão de investigação e o Ministério Público poderão requisitar relatórios parciais da operação de infiltração a qualquer tempo.

§ 2º A tramitação da medida será em autos apartados, cujo acesso somente será dado ao juiz, ao membro do Ministério Público, ao órgão de investigação e à autoridade policial, que podem indicar formalmente no máximo dois auxiliares para colaborarem.

Art. 27 É atípica a conduta do agente que oculta a sua identidade para, por meio da internet, colher indícios de autoria e materialidade dos crimes investigados.

Parágrafo Único. Não é punível, no âmbito da infiltração, a prática de crime pelo agente infiltrado no curso da investigação, quando inexigível conduta diversa.

Art. 28 Os órgãos de registro e cadastro público e privado poderão incluir nos bancos de dados próprios, mediante procedimento sigiloso e requisição da autoridade judicial, as informações necessárias à efetividade da identidade fictícia criada.

Art. 29 Concluída a investigação, todos os atos eletrônicos praticados durante a operação deverão ser registrados e armazenado, devendo ser encaminhados ao juiz e ao Ministério Público, juntamente com relatório circunstanciado.

Parágrafo Único. Os atos eletrônicos registrados citados no caput deste artigo serão reunidos nos autos apartados e vinculados ao processo judicial juntamente com a investigação criminal, assegurando-se a preservação da identidade do agente infiltrado e, se necessário, das pessoas envolvidas.

Seção XIV
Ação disfarçada

Art. 30 É admissível a medida de ação disfarçada de agentes de investigação ou, excepcionalmente, de particular no curso da investigação relativa aos crimes cometidos por meio eletrônico, ainda que parcialmente, quando presentes elementos probatórios razoáveis de conduta criminal preexistente e em andamento, independentemente de autorização judicial.

Parágrafo Único. À ação disfarçada aplicam-se as disposições relativas à infiltração policial, no que for cabível.

CAPÍTULO III
DOS CRIMES E DAS PENAS
Seção I
Falsidade informática

Art. 31 Falsificar, omitir, introduzir, modificar ou suprimir dados informáticos ou por qualquer outra forma interferir em um tratamento de dados, produzindo informação ou seu registro

documental ilícito, no todo ou em parte, para que seja considerado ou utilizado para finalidade juridicamente relevante.

Pena - reclusão, de três a oito anos, e multa.

§ 1º Se a informação é gerada originalmente por pessoa jurídica de direito público interno ou estrangeiro.

Pena - reclusão, de quatro a doze anos, e multa.

§ 2º Se o intuito for a obtenção de vantagem econômica indevida:

Pena - reclusão, de quatro a dez anos, e multa.

§ 3º Elaborar, produzir, importar, distribuir, vender ou possuir para fins comerciais qualquer dispositivo eletrônico, sistema informático ou código malicioso que permita o acesso a meio de pagamento.

Pena - reclusão, de quatro a doze anos, e multa.

§ 4º Se o agente é funcionário público e comete o crime prevalecendo-se do cargo.

Pena - reclusão, de quatro a doze anos, e multa.

Seção II
Dano informático

Art. 32 Indisponibilizar, alterar, destruir, danificar, suprimir ou tornar não acessíveis permanentemente sistemas informáticos, programas de computador, rede de dados ou dados armazenados em meio eletrônico sob controle ou operação de terceiros, no todo ou em parte, ou por qualquer forma lhes afetar disponibilidade, sem permissão legal ou para tanto estar autorizado.

Pena - reclusão, de dois a seis anos, e multa.

§ 1º Incorre na mesma pena quem indevidamente elaborar, produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir em redes de dados, dispositivos eletrônicos ou sistemas informáticos, programas de computador ou código malicioso destinado a produzir as condutas não autorizadas no caput.

§ 2º Se o dano atingir de forma grave ou por tempo relevante um dispositivo eletrônico, rede de dados ou sistema informático que apoie uma atividade destinada a assegurar funções sociais críticas, especialmente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.

Pena – 3 a 6 anos.

§ 3º Se o agente é funcionário público e comete o crime prevalecendo-se do cargo.

Pena - reclusão, de quatro a doze anos, e multa.

Seção III
Sabotagem informática

Art. 33 Entravar, impedir, interromper ou perturbar o funcionamento de um dispositivo eletrônico, sistema informático ou rede de dados, através da introdução de código malicioso, programa de computador ou qualquer outra forma de interferência, capaz de causar deterioração, danificação, alteração, indisponibilização ou impedimento do acesso, sem permissão legal ou sem para tanto estar autorizado.

Pena - reclusão, de um a cinco anos, e multa.

§ 1º Incorre na mesma pena quem ilicitamente elaborar, produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir em dispositivo eletrônico, sistemas informáticos ou rede de dados, programa de computador ou código malicioso destinado a produzir as condutas não autorizadas no caput.

2º Se a sabotagem atingir de forma grave ou por tempo relevante um dispositivo eletrônico, rede de dados ou sistema informático que apoie uma atividade destinada a assegurar funções sociais críticas, especialmente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.

Pena - reclusão, de dois a seis anos, e multa.

Seção IV
Acesso ilícito

Art. 34 Aceder de qualquer modo a um dispositivo, sistema informático ou redes de dados sem permissão legal ou sem para tanto estar autorizado.

Pena - detenção, de seis meses a dois anos, e multa.

§ 1º Se o agente é funcionário público e comete o crime prevalecendo-se do cargo.

Pena - 1 a 3 anos

§ 2º. 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.

§ 3º Incorre na mesma pena quem elaborar, produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir ilicitamente programa de computador ou código malicioso em sistemas informáticos, dispositivos eletrônicos ou redes de dados, a fim de produzir as condutas não autorizadas descritas no caput.

§ 4º Se, através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei.

Pena - reclusão, de dois a seis anos, e multa.

Seção V
Interceptação ilícita

Art. 35. Coletar, interceptar, capturar ou obter, através de meios técnicos, dados em transmissão sem permissão legal ou sem para tanto estar autorizado.

Pena - reclusão, de dois a quatro anos, e multa.

§ 1º Incorre na mesma pena quem ilicitamente elaborar, produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir em dispositivo eletrônico, sistemas informáticos ou rede de dados, programas de computador ou código malicioso destinado a produzir as condutas não autorizadas no caput.

CAPÍTULO III
DISPOSIÇÕES FINAIS

Art. 36. O Decreto-Lei 2.848/40 (Código Penal) passa a vigorar com as seguintes alterações.

"Art.
325.....
.....

.....
.....

I - permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas banco de dados da Administração Pública." (NR)

Art. 37. Revogam-se os artigos 154-A e 313-A do Decreto-Lei 2.848/40.

Art. 38. Esta Lei entra em vigor 60 dias após a data de sua publicação.