A COLETA DA PROVA NOS ILÍCITOS DIGITAIS

Neide Aparecida Ribeiro

EDITORA UNITINS

A COLETA DA PROVA NOS ILÍCITOS DIGITAIS

Neide Aparecida Ribeiro

EDITORA UNITINS

R484c Ribeiro, Neide Aparecida.
A coleta da prova nos ilícitos digitais [recurso eletrônico] / Neide Aparecida Ribeiro.
Palmas, TO: UNITINS, 2026.
128f.: il.color.; PDF.
ISBN: 978-85-5554-362-3
DOI: 10.36725/978-85-5554-362-3
1. Coleta. 2. Prova. 3. Ilícito. 4. Digitais. 5. Segurança. /Sistema de Informação. I. Universidade Estadual do Tocantins. II. Título.

CDD: 005.8

Ficha catalográfica elaborada pela Bibliotecária Ysabella Canindé Guerreiro Macêdo CRB-2/ 1191

Contato
Editora Unitins

(63) 3901-4176
108 Sul, Alameda 11, Lote 03
CEP.: 77.020-122 - Palmas - Tocantins

APRESENTAÇÃO

Com o surgimento da internet, transformaram-se radicalmente a comunicação e as interações sociais, conectando pessoas e instituições globalmente de maneira antes inimaginável. Essa revolução cibernética, inicialmente percebida apenas por suas facilidades e utilidades, logo revelou um lado sombrio: o uso da rede mundial de computadores para a prática de ilícitos.

A relação entre Direito e tecnologia tornou-se intrínseca e complexa, exigindo um estudo interdisciplinar aprofundado. Com a proliferação de computadores e smartphones, surgiram condutas ilícitas digitais que expõem a fragilidade do sistema legal e a falta de segurança na rede. A gravidade desses atos é amplificada pelo anonimato que o ambiente virtual proporciona, dificultando a identificação dos agressores e, consequentemente, a lavratura de autos de prisão em flagrante. No entanto, a internet não é espaço sem lei.

Nesse cenário desafiador, a presente obra se dedica à análise da coleta da prova dos ilícitos penais praticados na rede mundial de computadores e outras mídias. Para tanto, traça-se um breve histórico da evolução tecnológica até o surgimento da internet, como uma vasta comunidade virtual de troca de informações entre computadores fisicamente distantes, interconectados por sofisticados meios de telecomunicações.

Aborda-se a preocupante realidade de que, muitas vezes, as instituições do sistema de justiça criminal combatem esses ilícitos apenas parcialmente. Casos de violação de registros de dados bancários, por exemplo, mostram que a preferência por ressarcir clientes em vez de notificar as autoridades impede a devida apuração e a identificação de materialidade e autoria. A complexidade da coleta de provas em crimes digitais é agravada pela escassez de uma legislação brasileira robusta e pela falta de critérios eficientes que deem suporte às autoridades. O Código de Processo Penal, datado de 1941, não previa a realidade da internet, difundida no Brasil apenas em 1995.

Ainda que a Lei n. 9.296/1996 (Lei de Interceptação Telefônica) e o art. 5º, XII, da Constituição Federal apresentem dilemas interpretativos sobre a interceptação de sistemas telemáticos e de informática, a investigação tem buscado outros meios de prova para combater a impunidade. Além disso, leis mais recentes, como a Lei Carolina Dieckmann (Lei n. 12.737/2012) e o Marco Civil da Internet (Lei n. 12.965/2014), oferecem novas perspectivas de política criminal e ampliam a reflexão sobre a produção probatória na criminalidade virtual.

A obra explora o tema da coleta de provas em ilícitos digitais, unindo as áreas técnica da informática e jurídica da prova. A primeira parte detalha a evolução tecnológica e o surgimento da internet, conceituando rede e sua arquitetura, além de abordar vulnerabilidade e segurança online, tipologias de crimes digitais (próprios e impróprios), técnicas dos atacantes e protagonismo da criptografia. O papel dos agentes envolvidos na parede digital, autores e vítimas, encerra essa seção.

Também analisa a prova como um meio processual adequado para dar subsídio à acusação e demonstrar a materialidade do delito e, principalmente, comprovar autoria. Sem provas digitais robustas e válidas, a atuação do Ministério Público fica comprometida, podendo resultar em impunidade dos criminosos.

Este trabalho é, portanto, de suma importância, não apenas para a comunidade acadêmica de docentes e discentes, mas para todos os profissionais que lidam com a disseminação de informações por meio da tecnologia. Diante do crescimento vertiginoso da internet e da complexidade dos ilícitos nela praticados, a análise da coleta da prova nos crimes digitais é relevante para que autoridades possam atuar de forma eficaz na busca por justiça e segurança no ambiente virtual.

Palmas, 20 de dezembro de 2025

A Autora

PREFÁCIO

A emergência da rede mundial de computadores, a Internet, desencadeou uma transformação radical nas interações sociais e na comunicação global, conectando indivíduos e instituições em um ecossistema antes inimaginável. No entanto, essa revolução cibernética logo expôs um lado sombrio, caracterizado pelo uso da rede para a prática crescente de ilícitos.

A obra que ora se apresenta ao leitor representa um marco significativo na análise jurídica dos desafios impostos pela criminalidade digital à persecução penal brasileira. Neide Aparecida Ribeiro enfrenta, com rigor científico e profundidade doutrinária, um dos temas mais complexos e contemporâneos do Direito Processual Penal: a coleta da prova nos ilícitos cometidos por meio ou contra sistemas informáticos.

A revolução tecnológica que transformou radicalmente as comunicações humanas trouxe consigo não apenas facilidades inimagináveis, mas também um cenário de vulnerabilidades e práticas delitivas que desafiam as estruturas normativas tradicionais. Como bem observou Vladimir Aras na epígrafe desta obra, "o virtual e o real são apenas figuras de linguagem" recordando-nos que tudo o que ocorre no ciberespaço acontece na dimensão humana e dela depende. Essa premissa filosófica fundamenta toda a construção teórica aqui apresentada: crimes digitais não constituem uma categoria ontologicamente distinta dos delitos tradicionais, mas exigem adaptações procedimentais e interpretativas que respeitem tanto a eficácia da persecução penal quanto as garantias fundamentais.

O anacronismo entre a legislação processual penal brasileira — cuja origem remonta a 1941 — e a realidade da internet, difundida no país apenas em 1995, expõe uma lacuna normativa que a autora examina com notável competência. O descompasso é ainda mais evidente quando se considera que o Código de Processo Penal foi elaborado décadas antes do surgimento do primeiro *e-mail*, da *world wide web* e dos dispositivos móveis que hoje constituem instrumentos centrais tanto para a comunicação lícita quanto para a prática delitiva.

A problemática central enfrentada nesta obra — a (im)possibilidade de interceptação telemática e de dados em sistemas de informática à luz do art. 5º, XII, da Constituição Federal e da Lei nº 9.296/1996 — revela tensões hermenêuticas que permeiam a doutrina e a jurisprudência brasileiras. A autora não se furta ao debate, apresentando com clareza as correntes interpretativas que ora defendem a aplicação analógica da Lei de Interceptações Telefônicas aos sistemas telemáticos, ora sustentam a vedação constitucional expressa a tais medidas.

A interdisciplinaridade que permeia toda a investigação constitui um dos méritos mais expressivos desta obra. Ao combinar conhecimentos técnicos da área de informática com a dogmática processual penal, a autora demonstra que a compreensão adequada dos ilícitos digitais e dos meios probatórios correspondentes exige domínio tanto da linguagem jurídica quanto da arquitetura tecnológica subjacente. A explanação sobre a evolução histórica da computação, a estrutura da internet, os protocolos TCP/IP, os sistemas de endereçamento e as vulnerabilidades da rede oferece ao leitor — mesmo aquele não familiarizado com a tecnologia — subsídios imprescindíveis para a análise jurídica subsequente.

Particular relevância assume a análise das providências acauteladoras de prova. A autora demonstra conhecimento da teoria geral das cautelares processuais penais ao examinar institutos como a busca e apreensão, as prisões processuais e a cadeia de custódia aplicados aos crimes digitais. A inclusão dos arts. 158-A a 158-E no Código de Processo Penal, disciplinando a cadeia de custódia, representa avanço significativo para a preservação da integridade da prova digital — elemento de fragilidade reconhecida em face da volatilidade e da possibilidade de adulteração dos dados eletrônicos.

A classificação dos crimes digitais em próprios e impróprios, amplamente debatida na doutrina brasileira e internacional, recebe tratamento didático e esclarecedor. Enquanto os crimes próprios têm na tecnologia não apenas um meio, mas a própria essência da conduta típica — como a pirataria de *software*, o envio de vírus ou a violação de e-mail —, os crimes impróprios utilizam o ambiente digital como instrumento para a prática de tipos penais preexistentes, como estelionato, crimes contra a dignidade sexual e contra a honra.

A análise dos sujeitos envolvidos na "parede digital" — atacantes e vítimas — revela preocupação criminológica que transcende a mera dogmática penal. A autora reconhece que o anonimato proporcionado pelo ambiente virtual não apenas dificulta a identificação dos autores, mas também altera a dinâmica da vitimização e influencia a sensação de impunidade que estimula a prática delitiva. Essa compreensão sociológica do fenômeno criminal digital enriquece sobremaneira a obra e demonstra maturidade científica.

No que concerne à teoria geral da prova, a obra oferece síntese precisa dos conceitos fundamentais — fontes, meios, procedimento probatório, ônus da prova e licitude —, sempre com o olhar voltado às especificidades da prova digital. A distinção entre provas ilícitas e ilegítimas, tema de controvérsia doutrinária intensificada após a reforma do art. 157 do CPP pela Lei nº 11.690/2008, é abordada com clareza, ressaltando-se que a proteção constitucional contra a utilização de provas obtidas por meios ilícitos representa garantia fundamental do acusado, jamais podendo ser relativizada em nome da eficiência punitiva.

A perícia nos ilícitos digitais, tratada no capítulo final, constitui o cerne operacional de toda a problemática probatória. A autora demonstra conhecimento técnico ao descrever os procedimentos adequados de preservação do local digital, duplicação de mídias, análise forense de sistemas, recuperação de dados apagados e elaboração de laudos periciais. A metodologia descrita encontra amparo tanto na doutrina criminalística quanto nas normas técnicas da ABNT, revelando preocupação com a cientificidade e a confiabilidade da prova pericial digital.

A responsabilidade dos provedores de internet — tema que ganhou nova dimensão após o Marco Civil da Internet (Lei nº 12.965/2014) e as recentes decisões do Supremo Tribunal Federal sobre o art. 19 da referida lei — recebe tratamento atualizado e crítico. A autora reconhece que os provedores, enquanto intermediários técnicos, não podem ser responsabilizados diretamente por todo conteúdo ilícito veiculado por terceiros, mas têm o dever legal de colaborar com as autoridades mediante ordem judicial, fornecendo dados cadastrais e registros de conexão que podem ser decisivos para a identificação de autores de crimes digitais.

Esta obra surge em momento histórico particularmente relevante. O Brasil tem enfrentado crescimento exponencial de crimes digitais — segundo dados recentes, ocupa posição de destaque entre os países mais atacados ciberneticamente no mundo[1]. Simultaneamente, a legislação penal e processual penal brasileira ainda apresenta lacunas significativas, não obstante os avanços representados pela Lei Carolina Dieckmann (Lei nº 12.737/2012), pelo Marco Civil da Internet (Lei nº 12.965/2014) e pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

A Professora Neide Aparecida Ribeiro, com sua experiência acadêmica e sensibilidade para temas de fronteira entre Direito e Tecnologia, oferece à comunidade jurídica, acadêmica e aos operadores do sistema de justiça criminal obra de consulta obrigatória. Não se trata de um manual técnico, mas de reflexão crítica sobre os limites constitucionais da persecução penal, o equilíbrio entre segurança pública e direitos fundamentais, e a necessidade de atualização constante do Direito diante das transformações tecnológicas.

Aos estudantes de Direito, a obra oferece introdução sólida e abrangente aos crimes digitais e à prova digital. Aos advogados, defensores públicos, promotores de justiça e magistrados, fornece subsídios teóricos e práticos para a atuação em casos envolvendo criminalidade digital. Aos delegados de polícia e peritos criminais, apresenta orientações procedimentais fundamentadas juridicamente. A toda a sociedade, revela que a internet não é território sem lei, mas espaço que exige compreensão sofisticada da interação entre normas jurídicas e realidade tecnológica.

A leitura desta obra é, portanto, não apenas recomendável, mas necessária a todos aqueles que desejam compreender os desafios contemporâneos da persecução penal em ambiente digital, sempre com o compromisso ético e constitucional de preservar tanto a efetividade da Justiça quanto a dignidade da pessoa humana e seus direitos fundamentais.

Dra. Jéssica Painkow Rosa Cavalcante

Doutora em Direito Público pela Universidade do Vale do Rio dos Sinos (UNISINOS) e mestra em Direitos Humanos pela Universidade Federal de Goiás (UFG). Atualmente, é pesquisadora de pós-doutorado no Programa de Pós-Graduação Interdisciplinar em Direitos Humanos da UFG (PPGIDH/UFG). Possui bacharelado em Direito pela Pontifícia Universidade Católica de Goiás (PUC-GO), licenciatura em Ciências Sociais e Letras, além de especializações em Direito Agrário e Agronegócio (FACAB) e em Direito Civil e Processo Civil (UCAM). É professora do curso de Direito da Universidade Estadual do Tocantins (UNITINS), no Câmpus Dianópolis-TO, e advogada registrada na OAB-TO, atuando como Membro Titular do Tribunal de Ética e Disciplina da OAB-TO. É representante institucional do Instituto dos Advogados Brasileiros (IAB) pelo Estado do Tocantins e membro do Comitê Estadual de Educação em Direitos Humanos - TO.

E-mails: jessicapainkow@hotmail.com | jessica.pr@unitins.br

1 Os levantamentos mais recentes convergem para um panorama claro: o Brasil ocupa posição de liderança na América Latina em incidentes cibernéticos, destacando-se especialmente em ataques do tipo DDoS e ransomware, que o colocam entre os países mais visados da região (NETSCOUT, 2025; CHECK POINT RESEARCH, 2024). No cenário global, o país também figura com destaque — tanto como origem quanto como alvo — em campanhas de malware e ataques coordenados, conforme apontam relatórios da Qrator Labs e da IBM X-Force (QRATOR LABS, 2025; IBM, 2025). Soma-se a isso o monitoramento contínuo realizado pelo CERT.br, vinculado ao NIC.br, que evidencia um volume expressivo e diversificado de incidentes notificados anualmente no território nacional (CERT.br, 2025). Ver: CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Estatísticas de incidentes registrados pelo CERT.br. São Paulo: NIC.br, 2025. Disponível em: https://stats.cert.br/. Acesso em: 23 out. 2025; CHECK POINT RESEARCH. Cyber Security Report 2024. 2024. Disponível em: https://www.checkpoint.com/resources/report-3854/report--cyber-security-report-2024. Acesso em: 23 out. 2025; IBM. X-Force Threat Intelligence Index 2025. Nova York: IBM, 2025. Disponível em: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index. Acesso em: 23 out. 2025; NETSCOUT. DDoS Threat Intelligence Report 2025.1. 2025. Disponível em: https://tiinside.com.br/05/09/2025/com-brasil-na-lideranca-de-ataques-ciberneticos-na-america-latina-relatorio-da-netscout-revela-que-ataques-ddos-dominam-o-mercado/. Acesso em: 23 out. 2025; e, QRATOR LABS. AI-powered DDoS attacks are becoming a reality. Londres: ITPro, 2025. Disponível em: https://www.itpro.com/security/cyber-attacks/cyber-experts-have-been-warning-about-ai-powered-ddos-attacks-now-theyre-becoming-a-reality. Acesso em: 23 out. 2025.

ABREVIATURAS

- a. – Ano
- a.C. – Antes de Cristo
- ABC – *Atanasoff Berry Computer*
- ABRANET – Associação Brasileira dos Provedores de Acesso, Serviços e informações
- ADSL – *Assymmetric Digital Subscriber Line*
- Ampl. – Ampliada
- AOL – América *On Line*
- APCF – Associação dos Peritos Criminais Federais
- ARPA – *Advanced Research Projects Agency*
- ARPANET – *Advanced Reserch Project Agency Network*
- Art. – Artigo
- Atual. – Atualizada
- BB – Banco do Brasil
- Bol. – Boletim
- BR – Brasil
- Brfree – grátis no Brasil
- ccTLD – *Coutry Code Top Level Domain*
- CD – *Compact Disk*
- CD-ROM – *Compact Disk, Read Only Memory*
- CEF – Caixa Econômica Federal
- CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
- CF – Constituição Federal
- CGI – Comitê Gestor da *Internet*
- Cis – Circuitos Integrados
- CNN – *Cable News Network*
- COBOL – *Common Business Oriented Language*
- COEP – Comitê de Ética em Pesquisa
- COM – Organizações Comerciais
- CP – Código Penal

- CPD – Central de Processamento de Dados
- CPF – Cadastro de Pessoas Físicas
- CPP – Código de Processo Penal
- CPU – Unidade Central de Processamento
- d.C. – Depois de Cristo
- Des. – Desembargador
- DF – Distrito Federal
- DJU – Diário da Justiça da União
- DoD – Departamento de Defesa Americano
- DNS – *Domain Name System*
- DoS – *Denial of Service*
- DPCRIM – Divisão de Pesquisa, Padrões e Dados Criminalísticos
- DPER – Divisão de Perícias
- Dr. – Doutor
- DSL – *Digital Subscribers Liners*
- DVDs – *Digital Versatile Disks*
- ed. – Edição
- EDSAC – *Electronic Delay Storage Automatic Calculator ou Computer*
- EDU – Organizações Educacionais
- EDVAC – *Electronic Discret Variable Automatic Computer*
- EMBRAPA – Empresa Brasileira de Pesquisa Agropecuária
- EMBRATEL – Empresa Brasileira de Telecomunicações
- ENIAC – *Electronic Numeric Integrator and Calculator*
- EUA – Estados Unidos da América
- EXE – *Execute*
- f. – Folha
- FBI – *Federal Bureau of Investigation*
- FEBRABAN – Federação Brasileira de Bancos
- Fig. – Figura
- FISA – *Federazione Italiana Soft Air*
- FTP – Protocolo de Transferência de Arquivos
- GO – Goiás

- GOV – Organizações Governamentais
- H – Horas
- HC – *Habeas Corpus*
- HDs – *Hard Disks*
- HTTP – *Hypertext Transfer Protocol*
- Hz – *Hertz*
- IAB – *Internet Architeture Board*
- IBccrim – Instituto Brasileiro de Ciências Criminais
- IBGE – Instituto Brasileiro de Geografia e Estatística
- IBM – *IBM Corporation*
- ICANN – *Internet Corporation for Assigned Names and Numbers*
- il. – Ilustrada
- INC – Instituto Nacional de Criminalística
- INPI – Instituto Nacional de Propriedade Industrial
- Intelig – Inteligência
- IP – *Internet Protocol*
- IR – Imposto de Renda
- ISP's – *Internet Service Providers*
- IT – Itália
- Km – Kilômetro
- LAN – *Local Area Network*
- LP – Linha Privativa de Dados
- LSI – *Large Scale Integrator*
- MC – Ministério das Comunicações
- MCT – Ministério da Ciência e Tecnologia
- MG – Minas Gerais
- MIL – Organizações Militares
- MILNET – Rede Militar
- Min. – Ministro
- MIRC – Micreiro da *Internet Relay Chat*
- MIT – *Massachusetts Institute of Tecnology*
- MITS – *Micro Instrumentation Telemetry Systems*

- MP – Medida Provisória
- MP3 – *Motion Picture Expert Group-Layer* 3
- MS – Mandado de Segurança
- MSN – *Messenger*
- n. – Número
- NASA – *National Aeronautics and Space Administration*
- NC – Nota Conjunta
- NIC – Núcleo de Informação e Coordenação
- NSF – *National Science Foundation*
- NSFNET – *National Science Foundation Network*
- ob. – Obra
- OECD – Organização de Cooperação e Desenvolvimento Econômico
- ONU – Organização das Nações Unidas
- ORG – Outras Organizações
- org. - Organizador
- p. – Página
- FAPESP – Fundação de Amparo à Pesquisa do Estado de São Paulo
- PASI – Provedor de Acesso a Serviços da *Internet*
- PCs – Microcomputadores de clientes
- PD – Processamento de Dados
- PF – Polícia Federal
- PL – Projeto de Lei
- Prof. – Professor
- PTP – *Protocol Transfer Protocol*
- RAM – *Read And Memorize*
- Rel. – Relator
- rev. – Revista
- RHC – Recurso em *Habeas Corpus*
- RNP – Rede Nacional de Pesquisa
- ROM – *Read Only Memory*
- SEPINF – Serviços de Perícias em Informática
- SI – Sistema de Informação

- SPC – Serviço de Proteção ao Crédito
- SRF – Secretaria da Receita federal
- STF – Supremo Tribunal Federal
- STFC – Operadora de Telefonia
- STJ – Superior Tribunal de Justiça
- TCP – *Transport Control Protocol*
- TCP/IP – *Transport Control Protocol* da *Internet Protocol*
- Telecom – Telecomunicação
- TI – Tecnologia de Informação
- TJRS – Tribunal de Justiça do Rio Grande do Sul
- TLD – *Top Level Damain*
- TV – Televisão
- UFG – Universidade Federal de Goiás
- UK - Inglaterra
- ULSI – *Utra Large Scale of Integration*
- UNCITRAL – *United Nations Commission on International Trade Law*
- UNICAMP – Universidade de Campinas
- UNIVAC – *Universal Automatic Computer*
- UOL – Universo *On Line*
- USP – Universidade de São Paulo
- v. – Volume
- VLSI – *Very Large Scale Integrator*
- WAN – *Wide Area Network*
- WI-FI – *Wireless Fidelity*
- WWW – *World Wide Web*

"O virtual e o real são apenas figuras de linguagem (um falso dilema), não definindo, de fato, dois mundos diferentes, não dependentes. Em verdade, tudo o que se passa no ciberespaço acontece na dimensão humana e depende dela." (Vladimir Aras).

SUMÁRIO

INTRODUÇÃO

Com o advento da rede mundial de computadores *(Internet),* um dos fatores preponderantes a ser ressaltado é a modificação da comunicação entre pessoas e instituições sociais.

A relação estreita entre Direito e tecnologia, em razão do uso de computadores e aparelhos celulares, resultou em várias situações novas que requerem uma atenção especial de um estudo interdisciplinar das duas áreas de forma interativa.

A revolução cibernética trouxe muitos atrativos para a humanidade. Góis Júnior (2002) explica que a sedução pelas máquinas foi tão grande que, em um primeiro momento, somente se prestou atenção às facilidades e utilidades provenientes desse aparato tecnológico.

Para Góis Júnior (2002), o fascínio era tanto, que era difícil prever que alguém pudesse se valer do uso de computador para práticas nefastas. Entretanto, em um segundo momento, com o uso de um dos principais aplicativos dos computadores, a *Internet*, as pessoas se valeram desse instrumento para praticar ilícitos, motivo de preocupação da área jurídica.

Nesta obra, e dada a complexidade do tema, a tônica será a análise da coleta da prova dos ilícitos penais praticados na rede mundial de computadores e outras mídias, após a demonstração de um breve histórico da evolução tecnológica até o aparecimento da *Internet*.

Para Pimentel (2000), a *Internet* pode ser definida como ligação de dois computadores por meio de cabos e *softwares*, os quais permitem a troca de informações com apenas dois computadores ligados. É uma sociedade nova que forma uma comunidade virtual, estendendo-se de um extremo ao outro do mundo. É como uma modalidade de troca de informações entre computadores situados em ambientes diferentes e distantes fisicamente, interconectados através dos sofisticados meios oferecidos pela engenharia de telecomunicações.

Com a difusão das redes, surgiu uma infinidade de atividades ainda não conhecidas, em que os usuários utilizam os computadores e outros aparatos tecnológicos, como os *smartphones,* e praticam condutas que podem ser enquadradas como ilícitos digitais.

A fragilidade do sistema legal e a gravidade dos atos que podem ser realizados por meio da *Internet* traduzem falta de segurança ao acessar a rede e prática crescente de inúmeras condutas praticadas em virtude do avanço tecnológico globalizado.

O anonimato é outro fator preocupante, porque a autoridade policial tem dificuldades em identificar o atacante virtual em razão da reduzida possibilidade de se lavrar o auto de prisão em flagrante. A pessoa que introduz ou desvia informações, ou simplesmente ingressa em endereços eletrônicos apenas por curiosidade, imagina que está protegida pela falta de identificação. Ou seja, o agressor pode ser qualquer pessoa e pode estar em qualquer lugar.

Por outro lado, as instituições do sistema de justiça criminal têm combatido, parcialmente, tais ilícitos. Redes bancárias, quando têm os registros de dados violados, como o consequente desvio de somas de dinheiro de correntistas para pessoas estranhas ao conhecimento do banco, às vezes, preferem

ressarcir os clientes a notificar o fato à autoridade policial. Quando essa é a postura do banco, impede o endereçamento ao destinatário da notícia do fato ao Ministério Público, tanto quanto aos elementos essenciais, indícios ou provas, que podem indicar materialidade e autoria.

Verifica-se, na prática, a complexidade da coleta da prova nos crimes digitais, uma vez que o domínio da informática e do uso da internet se espalha no planeta, tornando-se extremamente difícil sua localização, em face de o Brasil ter uma legislação precária em estabelecer critérios eficientes para viabilizar o trabalho das autoridades do sistema de justiça criminal.

O Decreto-Lei n. 3.689, de 3 de outubro de 1941, conhecido como Código de Processo Penal, não especifica como coletar as provas em ilícitos dessa natureza. A Lei n. 9.296, de 24 de julho de 1996, dispõe sobre a interceptação telefônica e telemática em confronto com o inciso XII do art. 5º da Constituição Federal, que admite a interceptação, referindo-se expressamente sobre a interceptação telefônica. No entanto, as investigações têm avançado com o uso da tecnologia para que tais crimes não fiquem impunes.

Da leitura das hipóteses elencadas pelo legislador, surgem duas situações: se a *Internet* estiver incluída como uma espécie de comunicação, enquadra-se no tipo genérico de interceptação de comunicações telefônicas de qualquer natureza, entre as quais a previsão da possibilidade de interceptação do fluxo de comunicações em sistemas de informática e telemática, na previsão do *caput* do art. 1º e parágrafo único, da Lei n. 9.296/1996, podendo ser realizada caso tenham sido preenchidos todos os requisitos legais.

Porém, o inciso XII do art. 5º da Constituição Federal, em sua forma literal, veda expressamente que a interceptação de sistemas telemáticos e de informática seja realizada, obstando, assim, a coleta da prova nos ilícitos digitais. Dessa maneira, a problemática pode ser apresentada na forma de (im)possibilidade de se realizar a interceptação dos sistemas informáticos e telemáticos, em especial de ilícitos praticados na *Internet,* para instruir investigação criminal, de acordo com o art. 1º da Lei nº 9.296/1996, tendo como impedimento o inciso XII do art. 5º da Constituição Federal. Resta, portanto, a investigação de outros meios de prova previsto no estatuto processual penal que podem possibilitar a elaboração do laudo pericial nos ilícitos digitais.

Há, todavia, a Lei nº 12.737, de 30 de novembro de 2012, conhecida como Lei Carolina Dieckmann, e o Marco Civil da Internet, Lei nº 12.695, de 23 de abril de 2014, que trazem outras perspectivas de política criminal que serão tratadas nesta obra, ampliando a reflexão sobre a produção probatória específica na criminalidade virtual.

O tema é atual e relevante e poderá interessar à comunidade acadêmica formada de docentes e discentes, além de alcançar outras áreas de atuação profissional, dada a disseminação das informações por meio da tecnologia, em especial do crescimento vertiginoso da rede mundial de computadores, a *Internet*, em que se faz necessário o estudo da coleta da prova nos ilícitos praticados na rede.

Isso se explica porque o Código de Processo Penal não previu sobre a coleta da prova nos ilícitos informáticos, uma vez que o diploma legal data de 1940, e a *Internet* ter sido difundida no Brasil 55 anos

depois, em 1995. Outras legislações esparsas não são suficientes para dar suporte a quem investiga os ilícitos digitais aos demais sujeitos do sistema de justiça criminal.

O trabalho versa sobre a coleta da prova nos ilícitos digitais envolvendo a área técnica da informática, da *Internet* e jurídica da prova em duas partes. A primeira parte da obra foi dividida em três capítulos.

O capítulo I, trata da evolução tecnológica e do surgimento do computador, trazendo a síntese da evolução da tecnologia até o aparecimento e uso da *Internet.* A *Internet* foi conceituada, e a arquitetura da rede mundial de computadores, a aplicação da *Internet* no mundo contemporâneo e a administração da *Internet* no Brasil foram explicadas ao leitor.

O capítulo II explica a vulnerabilidade e a segurança na *Internet.* Para melhor compreensão do assunto, foram estudadas as principais condutas tidas como ilícitas quando praticadas com o uso do computador e pelo computador. Para tanto, apresentou-se o conceito clássico de crime, para posteriormente adentrar no conceito dos crimes praticados na rede, dividindo-os em crimes próprios e impróprios. Para complementar, foram descritas as principais técnicas utilizadas pelos atacantes digitais e a preocupação do uso da segurança nas operações realizadas via *Internet,* como, por exemplo, a criptografia.

No capítulo III, foram analisados os agentes envolvidos na parede digital, as diversas tipologias de autores de fatos dessa natureza e os tipos de vítimas, encerrando-se a primeira parte. A prova foi abordada em sentido amplo no processo penal, sem intuito de esgotar o tema, apenas focando nas fontes e nos meios de prova, do princípio do ônus *probandi* no direito pátrio, do procedimento probatório e da licitude das provas.

Na segunda parte, priorizou-se o estudo da prova coletada em ilícitos praticados na grande teia mundial, a qual tem conexão direta com a primeira parte, uma vez que trata dos diversos meios de provas utilizadas no âmbito da investigação e da instrução criminal.

O capítulo IV trabalhou as medidas acauteladoras de prova com digressão nas medidas cautelares reais e pessoais que tenham relação com o *periculum in mora* e *fumus boni juris*, estreitamente ligadas aos crimes cibernéticos, em face da rapidez do desaparecimento das informações que devem ser capturadas pela polícia judiciária.

No capítulo V, a problemática da (im)possibilidade de se fazer a interceptação telefônica, telemática e de dados na rede mundial de computadores foi enfrentada com digressão nas correntes que abordaram o assunto. Estudaram-se o sigilo de dados, da informática e da telemática, o sigilo bancário, a responsabilidade das empresas provedoras de acesso à *Internet, e* a admissão do *e-mail* como prova. Finalmente, concluiu-se com a análise da elaboração do laudo pericial tendo outros meios de prova como ponto de partida no ambiente virtual.

Portanto, ao final da leitura deste trabalho, espera-se que o leitor possa averiguar a importância do tema devido ao crescente número de fatos envolvendo o ambiente virtual e a necessidade de as autoridades terem meios eficazes para coletar apropriadamente a prova oriunda de ilícitos digitais.

1. EVOLUÇÃO TECNOLÓGICA: DO SURGIMENTO DO COMPUTADOR AO USO DA INTERNET

Antes de adiantar o tema abordado, faz-se necessária uma análise sobre a tecnologia, abrangendo o surgimento do computador e o uso da *Internet.* Meirelles (1994) explica que o marco inicial data de 2000 a.C., com o uso do ábaco pelos povos da babilônia e ainda utilizados por chineses e japoneses.

Para Rosa (2002), o período da evolução cibernética pode ser dividido em quatro gerações, iniciando-se com os povos primitivos na contagem dos animais feita pelos pastores gregos e egípcios. No entanto, o primeiro registro pode ser considerado desde 2500 a.C. com a versão primitiva do Ábaco, utilizado pelos egípcios e romanos, no Oriente Médio, para fazer transações representadas por pedras de calcário, chamadas de *Calculi*, considerada um dos primeiros dispositivos mecânicos da computação.

Entretanto, para melhor compreensão da evolução e do surgimento da *Internet*, é preciso mencionar outros fatores que contribuíram para o desenvolvimento da informática (Silva, 2003).

Jonh Napier, matemático escocês, inventou em 1614 a tábua ou ossos de Napier, feitos de marfim, dispositivo utilizado para desenvolver operações de multiplicações matemáticas, chamado de Círculos de Proporção. A invenção de Napier contribuiu para o aparecimento da régua de cálculo de William Oughtred, em 1621, considerada como marco analógico da computação (Meirelles, 1994). Em 1642, foi inventada a primeira calculadora mecânica com capacidade de fazer as operações de somar e subtrair (Costa, 2003).

No entanto, foi o matemático alemão Gottfried Wilhelm von Leibniz quem, em 1677, aperfeiçoou a máquina para ter capacidade de multiplicar e dividir com números de oito algarismos (Meirelles, 1994; Rosa, 2002).

Meirelles (1994) relata que, em 1801, Joseph Marie Jacquard inventou um tear mecânico com capacidade de desenhar padrões dos tecidos em um cartão perfurado, que foi a primeira representação de um programa para o primeiro processador. O francês Charles Thomas de Colmar, em 1820, criou a primeira máquina de calcular, com a simplificação da ideia de Leibniz, denominada de *Arithmometers.*

O inglês Charles Babbage, em 1835, inventou outra máquina, denominada de Máquina Analítica, que utilizava cartões perfurados, não conseguindo levar sua invenção adiante por escassez de recursos financeiros. Todavia, foi Lady Ada Augusta Byron, Condessa de Lovelace, matemática, considerada a primeira programadora da humanidade, quem trabalhou com Babbage e desenvolveu as séries de instruções para serem utilizadas na máquina, considerada como a precursora do *software* (Silva, 2003).

Em 1854, com a publicação da obra *An Investigastion of the Laws* of *Thought,* do inglês George Boole, houve um avanço com o estudo dos princípios binários utilizados anos depois no estudo das operações computacionais internas, chamadas de Álgebra *Booleana* ou álgebra de *Boole* (Meirelles, 1994).

Herman Hollerith inventou uma máquina de calcular que fez a contagem em seis semanas e a análise estatística em dois anos e meio nos resultados do censo de 1890 nos Estados Unidos. Contraste positivo com o censo anterior, que demorou onze anos para ser concluído, tendo contribuído, inclusive,

para a criação da Companhia de Máquinas Tabuladoras (*Tabulating Machine Company*), dirigida em 1911 por Thomas Watson, chamada posteriormente de *International Business Machines Corporation*, conhecida mundialmente como *IBM* (Silva, 2003).

Outra máquina de calcular mecânica importante que merece ser citada foi criada por William S. Burroughs, em 1886, diferente das anteriores porque imprimia parcelas e resultados. Foi comercializada em 1890, pela *American Arithmometer Company*, empresa fundada por ele, tendo transformado em *Burroughs Company*, que se uniu à empresa UNIVAC, hoje *UNISYS Corporation* (Meirelles, 1994).

Os autores não são unânimes em dizer sobre a data exata do surgimento do primeiro computador no mundo. Em 1931, Vannevar Bush criou o primeiro computador analógico, no *Massachussets Institute of Tecnologic* (MIT), em Bostom, usado para fazer equações diferenciais simples, com analisador diferencial mecânico (Meirelles, 1994).

Em 1942, a Marinha Americana juntamente com a Universidade de Harvard e a IBM idealizaram o MARK I, um computador gigantesco que ocupava um espaço de 120 m2, com componentes eletromecânicos. Esse computador foi idealizado por Howard Aiken, em 1937, sendo o primeiro projeto que a história noticia, apresentado em 1944 com uma estrutura densa e pesada, com 2,5 metros de altura por 18 metros de comprimento, com mais de 700 quilômetros de cabos e com 750.000 partes (Meirelles, 1994).

Nos Estados Unidos, em 1942, surgiu o primeiro protótipo do calculador eletrônico, denominado de *Atanasoff Berry Computer (ABC),* idealizado por John V. Atanansoff e Clifford Berry, considerado como o primeiro computador eletrônico digital, que utilizava válvulas para circuitos lógicos (Meirelles, 1994; Silva, 2003).

No entanto, o primeiro computador eletrônico digital foi o Z3, que surgiu na cidade de Konrad Zuse, na Alemanha, em 1941, de uso genérico usado na Segunda Guerra Mundial (Sampaio Costa, 2000). Mas foi Alan Turing, em 1943, quem construiu em Bletchley, na Inglaterra, o primeiro computador programável, tendo feito dez Colossus I, computador eletrônico digital com uso de válvulas, para que fosse usado em criptografia e quebra de códigos militares, em particular para decifrar o código de segurança alemão, chamado Enigma, até então considerado indecifrável (Sampaio Costa, 2000).

O Exército Americano, em 1946, criou um computador para fins militares com 17.468 válvulas de 16 tipos diferentes, com peso de trinta toneladas, 10.000 capacitores, consumo de aproximadamente 150.000 *watts* e ocupação de mais de 170 metros quadrados, usado para calcular trajetória balística, denominado de *Electronic Numeric Integrator and Calculator (ENIAC)*, idealizado por J. Presper Eckert e Jonh Mauchly, da Universidade da Pensylvania.

Esse computador custou ao governo americano cerca de meio milhão de dólares, desenvolvido a partir de 1943, baseado no computador ABC, reduzindo-se de 1.000 para 30 segundos os cálculos de trajeto de mísseis, operando em velocidade mil vezes mais rápido que o MARK I (Meirelles, 1994).

No período entre 1945 e 1950, Jonh von Neumann, em conjunto com Arthur Burks e Herman Goldstine, criou a lógica dos circuitos, a definição dos programas e as operações com números binários, revolucionando o funcionamento dos computadores, que, desde então, seguem a arquitetura de Von Neumann (Meirelles, 1994).

O *UNIVAC* foi o primeiro computador criado para ser vendido em escala comercial em 1951 e em 1953. A *IBM Corporation* colocou no mercado o *IBM* 701, que fora substituído pelo *IBM* 650, um recorde de vendas, com pedido inicial de cinquenta unidades, tendo vendido mais de mil computadores no mundo todo.

Em 1957, a *IBM* lançou o *IBM* 305, primeiro computador construído com transístores, e o *NCR* 304. O *PDP1* foi o primeiro minicomputador lançado em 1959 e, em 1960, foi criada a primeira linguagem de programação, de alto nível, a *Common Business Oriented Language (COBOL).*

A *Micro Instrumentation and Telemetry Systems*, em 1972, lançou o primeiro computador de uso pessoal e, em 1973, a *Xérox* produziu um microcomputador completo, incluindo o monitor. De 1975 a 1981, surgiram vários outros tipos de computadores lançados no mercado, todos nos Estados Unidos.

Em 1976, foi desenvolvido por Stephen Wozniak e Steven Jobs o APPLE I, um microcomputador de uso pessoal, comercializando mais de cinquenta mil unidades, o que deu início à indústria da microinformática (Rosa, 2002).

O que se verifica na história do surgimento dos computadores, de acordo com Meirelles (1994) e Rosa (2002), é que houve grande impulso na Segunda Guerra Mundial, no controle do estoque de material bélico e no cálculo da tabela de artilharia para cada lote de munição que fosse fabricado.

Os autores não são concordes em dizer quantas gerações e etapas já se passaram na evolução dos computadores. Alguns se limitam em afirmar que, até hoje, contam-se quatro gerações diferenciadas. A primeira geração, iniciou-se em 1946 até 1958; a segunda geração de 1959 a 1965; a terceira geração de 1965 até 1971; e a quarta de 1975 até a presente data (Rosa, 2002).

Outros autores apontam que a história do computador pode ser classificada em cinco gerações (Meirelles,1994; Silva, 2003).

A primeira geração compreende o período de 1700 a.C. até meados de 1940, com o surgimento do projeto ENIAC, em 1942, um computador construído com base em válvulas, vulneráveis à quebra após o uso. Além do ENIAC, foi criado por Jonh von Neumann o *Electronic Discret Variable Automatic Computer (EDVAC),* o *Electronic Delay Storage Automatic Calculator* (EDSAC) ou *Computer,* e o *Universal Automatic Computer (UNIVAC)*. Este último foi o primeiro computador construído fora das Universidades e Centros de Pesquisa, sendo o Departamento do Censo Americano o primeiro cliente. O UNIVAC I, por sua vez, era menor do que os outros computadores porque ocupava cerca de 20 metros quadrados e pesava cinco toneladas, usado para prever a vitória do presidente americano, Eisenhower, na noite da eleição, em 1952 (Rosa, 2002).

A segunda geração ocorreu no período entre 1959 e 1965, com a substituição das válvulas pelos transistores, mais resistentes, velozes e confiáveis, com tamanho cem vezes menor do que o da válvula, criados em 1948 nos Laboratórios Bell da ATT, por William Shockley, J. Bardeen e W. Brattain. Naquela época, apareceram a indústria do *Software* e as primeiras linguagens de programação que usavam palavras em vez de números ou códigos, como o *Fortran* e o *Cobol*.

A terceira geração compreende o período de 1958 até 1971, quando surgiram os circuitos integrados, que tiveram possibilidade de uso com o auxílio da NASA, viabilizando a comercialização.

A terceira geração teve como marco o IBM 360 com seis modelos básicos, criado por Gene Amdahl, com possibilidade de opções de mais de dois milhões de adição por segundo e cerca de 500 mil operações de multiplicações. Foram vendidos mais de trinta mil sistemas (Meirelles, 1994).

O uso dos circuitos integrados diminuiu a dimensão dos computadores com a utilização dos *chips*, pastilhas bem pequenas, que contêm vários componentes eletrônicos, aparecendo os microcomputadores que calculavam o que fosse preciso em nanossegundos.

A quarta geração iniciou-se em 1970 até a data de 1994. Nessa etapa, há uma supervalorização da miniaturização e da eficácia dos computadores, com os Circuitos Integrados, LSI e VLSIs, tendo como características comuns a Unidade Central de Processamento (CPU), que armazena, copia e modifica informações (Meirelles, 1994).

Os CIs são circuitos integrados, pertencem a esta geração. A Integração em Larga Escala (*Large Scale Integrator* – LSI) integrou milhares de transistores em apenas um *chip.* A *Very Large Scale Integrator* (VLSI) surgiu em 1980, acondicionando centenas de milhares de transistores em um chip, e a ULSI *Ultra Large Scale of Integration (ULSI)* reuniu milhões de transistores em um único chip. Naquela época, surgiram também os supercondutores e as memórias *Read And Memorize* (RAM) e *Read Only Memory (ROM).* O Altair foi o microcomputador inserido nessa nova tecnologia, que em 1975 ficou popular depois de uma publicação na revista Popular *Mechanics*, na Inglaterra (Rosa, 2002).

Quanto à quinta geração, Meirelles (1994, p. 60) aponta que

> A polêmica da classificação em gerações continua com a chamada quinta geração, que para alguns autores começou em 1990 com as máquinas RISC e os circuitos integrados ULSI ou ainda com o uso do processamento paralelo. Entretanto, duas características aparecem como mais prováveis de fazer parte da quinta geração que está por vir. A primeira seria a de possuir uma arquitetura de processamento paralelo, com vários processadores, possivelmente um número muito grande, operando simultaneamente. Uma arquitetura paralela já é técnica e economicamente viável – utilizada por supercomputadores no início da década de 90. A segunda característica estaria associada à primeira e à ruptura, de alguma forma, da estrutura binária de Von Neumann. Acredita-se que a quinta geração irá surgir nesta década, considerando o que já está nos laboratórios e os supercomputadores que de certa forma já tem as duas características descritas acima. E também pelo que principalmente os americanos e japoneses estão investindo e pesquisando no desenvolvimento de uma geração de computadores. Outra característica citada como fazendo parte da quinta geração é a habilidade de realizar tarefas de inteligência artificial.

Em uma visão de mercado, o autor separa as etapas computacionais em três décadas etiquetando-as assim: década de 70 – surgimento do Processamento de Dados (PD) e Centro de Processamento de Dados (CPD); década de 80 – aparecimento do Sistema de Informação (SI), automação e Banco de Dados; e década de 90 – criação da Tecnologia da Informação (TI).

A Terceira Onda ou a Era da Informação é outra denominação para essa época após a invenção de outras mídias, como telefone, rádio, televisão e cinema. Segundo destaque de Alvin Tofler, a *Internet* consolida a Terceira Onda com a inclusão da velocidade e da origem das informações (Peck, 2002; Wolton, 2012).

Dwight Eisenhower, Presidente dos Estados Unidos, em 1959, após quatro meses de o satélite espacial soviético ter sido enviado ao espaço, criou a *Advanced Research Projects Agency (ARPA)*, com o objetivo de pesquisar tecnologias novas para o Exército Americano, para que, em caso de ataque nuclear, houvesse uma forma de se conectar por intermédio de uma rede que, após o bombardeio nuclear, permanecesse em funcionamento. Para desenvolver esse tipo de tecnologia alternativa, a *Rand Corporation*, conselho formado em 1948 sob a fiscalização da ARPA, apresentou, em 1967, o primeiro projeto dessa natureza, criando, em 1969, a rede de comunicações militares, denominada de *ARPANET* (Rosa, 2002; Castells, 2003).

Redes tradicionais baseadas em circuitos telefônicos trocados eram consideradas bastante vulneráveis, pois a simples perda de uma linha ou comutador (*switch*) implicaria interrupção de todos os componentes da rede de quem os estivesse usando.

Para encontrar uma solução para esse problema, o *Departamento de Defesa Americano (DoD)* encomendou uma pesquisa ao *ARPA*. Após algumas discussões, o *ARPA* decidiu que a rede do DoD seria de pacotes comutados (*packet-switched*), consistindo em uma sub-rede e computadores hospedeiros (*hosts*). Surgiram, então, os protocolos e o projeto *Advanced Research Projects Agency Network* (*ARPANET)*, que viria a ser a *Internet.*

A grande inovação do projeto *ARPANET*, primeiro projeto de defesa americano, desde o início, foi o de comunicar através das diversas redes já existentes, qualquer que fosse a tecnologia de transmissão utilizada. Ou seja, ao invés de pregar mudanças nas redes já existentes, construiu um sistema de comunicação que operasse por cima das redes, dando a ilusão de uma única rede global, que seguiria vários caminhos (em caso de destruição de uma linha sempre haveria caminhos alternativos).

A partir de 1983, quando o projeto *ARPANET* adotou o protocolo TCP/IP[1] como padrão, a rede cresceu rapidamente, atingindo 200.000 computadores em 1990. Em janeiro de 1992, a *Internet Society,* uma Comunidade da *Internet,* foi criada para promover o uso da *Internet* e cuidar do seu gerenciamento (Comer, 1995).

Outras invenções importantes apareceram, como a criação do correio eletrônico, por Ray Tomlinson, em 1972. Noruega e Inglaterra se ligaram à rede em 1973, ano em que o Protocolo para Transferência de Arquivos (FTP) foi especificado, oportunizando, a quem estivesse em servidor remoto, a cópia de arquivos e a troca de informações. O que se verifica ao longo da história é que a *Internet* teve uma disseminação maior nos anos 70, ao ser utilizada nos meios acadêmicos e científicos, com o funcionamento da rede demonstrado em 1972, na Conferência Internacional de Comunicações Computacionais, nos Estados Unidos, na cidade de Washington (Rosa, 2002; Castells, 2003).

1 Transporte sem conexão de endereçamento.

Essa rede permitiu o acesso de pesquisadores aos centros de computação para o compartilhamento dos recursos de *hardware*[2] e *software*[3]. Por intermédio de uma tecnologia de interconexão, as redes utilizavam ondas de rádio e de satélites. A *ARPANET,* em 1980, dividiu-se em *ARPANET* e *Military Network* (*MILNET)*, rede militar denominada *DARPA Internet*. No entanto, somente em 1985, a *National Science Foundation (NSF)*, em conjunto com a *ARPANET*, interligou os computadores, formando uma espinha dorsal da rede (*backbones*), conhecida como *Internet* (Castro, 2003).

Tim Berners-Lee foi quem propôs o vínculo das informações em diversas máquinas, influenciado pelo hipertexto com base no sistema *Enquire Within,* no Laboratório Europeu de Física da Partícula em Genebra (Fiorillo, Pegorari Conte, 2016).

O símbolo conhecido como *World Wide Web (WWW)*, criado em Genebra na Suíça, em 1989, propiciou o acesso das pessoas à rede mundial de computadores, com o lançamento do primeiro provedor de acesso comercial, o *World*, em 1990 (Rosa, 2002; Castro, 2003).

O Brasil foi um dos primeiros a se conectar na rede em conjunto com mais dez países – Argentina, Áustria, Bélgica, Chile, Grécia, Índia, Irlanda, Coréia do Sul, Espanha e Suíça (Rosa, 2002).

A Rede Nacional de Pesquisa (RNP), o Comitê Gestor da Internet (CGI.br) e a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) atuaram na oferta dos serviços com a integração entre as instituições de pesquisa, no início da década de 90 (Castro, 2003).

A partir desses pontos, foram criados outros *backbones* regionais, objetivando a integração entre eles e somente em 1994 implantou-se um projeto piloto da Empresa Brasileira de Telecomunicações (Embratel) com o objetivo comercial de permitir o acesso por intermédio de linhas discadas, substituídas, em 1995, por acessos dedicados por Rede Nacional de Comunicação de Dados por Comutação de Pacotes (*RENPAC)*[4] (Atheniense, 2000).

Atheniense (2000) explica a importância da contribuição da *RNP* para nova formação de outros pontos e ampliação do *backbone RNP*, que passou a se chamar *Internet/BR.* Em maio de 1995, o Ministério das Comunicações (MC) e o Ministério da Ciência e Tecnologia (MCT), com o intuito de informar a sociedade brasileira sobre a introdução da *Internet* no País, emitiu Nota Conjunta para prestar esclarecimentos sobre conceitos, Rede Nacional de Pesquisa (RNP), tarifas e preços e outras informações adicionais que diziam respeito à rede mundial de computadores.

No Brasil, o órgão responsável pela regulamentação e fiscalização dos serviços de telecomunicações, incluindo a internet, é a Agência Nacional de Telecomunicações (Anatel). A Anatel é uma agência reguladora vinculada ao Ministério das Comunicações, criada pela Lei nº 9.472, de 16 de julho de 1997 (Lei Geral de Telecomunicações).

Além da Anatel, o Comitê Gestor da Internet no Brasil (CGI.br) desempenha um papel importante na governança da internet no país, coordenando e integrando as iniciativas de todos os setores dessa área.

2 *Hardware* é o equipamento físico que rodam os programas de computador.

3 *Software* é o programa de computador.

4 Acesso em pacotes.

1.1 Conceito e arquitetura da *Internet*

O termo *Internet* tem dois significados: o primeiro, de cunho acadêmico, diz respeito à conexão de duas ou mais redes heterogêneas (*InterNetwork)*, ou seja, ligadas entre si; e o outro, mais popular, se refere a uma rede mundial de computadores específica, largamente usada por Universidades, Agências Governamentais, Companhias e Indivíduos (Commer, 1995; Atheniense, 2000; Castells, 2003).

A *Internet* pode ser definida como

> Um conjunto de tecnologias para acesso, distribuição e disseminação de informações em redes de computadores. A rede é o compartilhamento de informações e serviços. Um trabalho em rede é possível quando pessoas ou grupos possuem informações ou serviços que desejam compartilhar. Pode-se dizer, portanto, que a *Internet* é um conjunto de redes de computadores interligadas pelo mundo inteiro, que têm em comum um conjunto de protocolos e serviços, possuindo a peculiaridade de funcionar pelo sistema de troca de pacotes, ou seja, as mensagens dividem-se em pacotes e cada pacote pode seguir uma rota distinta para chegar ao mesmo ponto (Rosa, 2002, p. 33).

É difícil definir *Internet*. Assim, faz-se necessária uma definição que se destaque com o aprimoramento técnico que a envolve:

> A *Internet* é um sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina a qualquer outra máquina conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem a limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento (Correia, 2000, p. 8).

A *Internet* abandona o princípio de se ter fornecedor e consumidor de comunicação, tecnologia cliente-servidor, e opta por uma solução comunitária em que qualquer um pode se integrar à rede, desde que respeite as regras[5] da comunidade virtual na participação das atividades. Esse "mundo virtual"[6] é "um espaço fruto da interligação de computadores, por exemplo, o ambiente no qual trafegam os dados da *Internet"* (Gibson, *apud* Correia, 2000, p. 9).

Nesse ambiente, percebemos crescimento vertiginoso do alcance da *Internet* resultante da simplicidade de o usuário conectar uma sub-rede qualquer à "comunidade *Internet*".

Em termos específicos, a *Internet* determina que uma sub-rede pode se conectar a outra somente através de um nó que esteja ligado a ambas as redes e que se responsabilize pela troca das mensagens que trafegam de uma rede para outra.

O nó "intermediário" que dá acesso à nova rede é chamado "*Gateway*" (roteador), justamente porque ele serve como passarela entre as máquinas penduradas na sub-rede e os demais nós. No caso global, isso quer dizer que as sub-redes se acoplam ao núcleo (*core*), formando uma rede cada vez maior (Reis, 1997).

5 A *Internet* possui regramentos próprios, como pode ser exemplificado no antigo *Orkut*, em que existem várias espécies de comunidades que exigem uma identidade dos internautas. Para ter acesso ao *Orkut*, a pessoa deve ser convidada a participar e tem uma senha exclusiva de acesso. O *Facebook* substituiu o Orkut e tem a mesma lógica de ingresso dos usuários.

6 Termo construído por Wiiliam Gibson na obra *Neuromancer*, que descreve o mundo dos computadores e da sociedade que os cerca.

Depois de formada, a malha física estabelece-se em rede virtual única, ou seja, qualquer nó na *Internet* pode acessar outro nó da mesma forma, como se estivessem todos conectados em uma só rede. Essa meta é atingida adotando-se um serviço de entrega comum baseado em um esquema de endereços únicos para cada máquina integrante da *Internet*. O principal protocolo de serviço de entrega é o IP *Internet Protocol (IP)* e os endereços atribuídos de maneira única para identificar qualquer máquina ligada à *Internet*, chamados endereços IP.

Nessa arquitetura, se uma máquina de uma sub-rede quiser se comunicar com outra de sub-rede diversa, ela tem de mandar suas mensagens para o roteador, que se encarregará de encaminhá-las para o destino, seja diretamente (caso a outra sub-rede esteja ligada também ao roteador), ou através de um outro roteador ligado a ele. Nesse endereçamento, aplica-se o conceito de entrega por melhor esforço, ou seja, do caminho mais fácil. Esse processo de passagem para diante é chamado de *"fowarding"*, e cada trecho atravessado (roteador) pela mensagem é chamado de "*hop*".

Para compensar o serviço simples e modesto de entrega, a arquitetura *Internet* oferece um protocolo robusto para um serviço de "Transporte" confiável e orientado à conexão, o *Transport Control Protocol (TCP)*. Juntos, os protocolos TCP/IP apresentam o essencial da arquitetura *Internet,* de forma que o modelo funcional dessa rede é conhecido como pilha "*TCP/IP".*

A maioria dos usuários que acessam a *Internet* simplesmente para executar programas de aplicações não entendem e nem precisam entender a tecnologia TCP/IP, a estrutura que há sob a *Internet,* ou sobre os caminhos que os dados viajam até seus destinos.

O esquema de endereçamento IP é perfeito para o roteamento e o planejamento e configuração de sub-redes, apresentando, no entanto, uma dificuldade para os seres humanos que preferem nomes a números. Na *Internet*, a forma amigável encontrada foi a atribuição de nomes às máquinas, levando em conta dois aspectos: primeiro, o esquema de nomes deveria permitir uma atribuição autônoma e sem ambiguidade, ou seja, um administrador de sistema pode dar nomes às máquinas como quiser e sem se preocupar em gerar conflito com outras máquinas; o segundo, relaciona-se com o processamento necessário para resolver os nomes de todos os nós e para todos o nós da *Internet.*

A solução de endereços foi baseada na definição de domínios, os de Autoridade agrupam máquinas sujeitas a uma mesma administração. Dentro de seu domínio, a administração pode nomear as máquinas sem consideração aos nomes usados em outros domínios, criar e nomear subdomínios e delegar autoridade de administrá-los a outras entidades.

Domínio é o nome de uma área reservada em um servidor *Internet* que indica o endereço de um *website*[7]. De maneira recursiva, o espaço do domínio da *Internet* é particionado em domínios que, por sua vez, são particionados em outros domínios. Dentro dessa hierarquia, um nó terá seu nome composto pela agregação dos nomes de domínios, separados por pontos e terminando pelo nome da própria máquina (esquerda para direita). Ex.: *www.ufg.br* (identifica o nó *www* do domínio *ufg* do domínio *br*).

---

7 *Website* é o lugar no ambiente *WEB* da *Internet* que é ocupado com informações como textos, fotos, animações gráficas, sons e vídeo de uma pessoa ou empresa.

Góis Junior (2002) afirma que o *IP* ou *Internet Protocol* tem a função de identificar e localizar uma máquina na rede, tendo sua razão de existir na questão estrutural da rede. Para exemplificar, os *IPs* funcionam como verdadeiros códigos atribuídos aos pontos de conexão da rede e têm, de forma geral, um número composto de nove dígitos.

Ensina o mesmo autor que os IPs funcionam como endereços da *Internet.* No entanto, em razão da dificuldade de localização pelos números (sequência longa e de acesso mais complicado), criaram-se os *domain names*, denominados nomes de domínio.

No nível mais alto, a *Internet* define os domínios de duas formas: por localização geográfica e organizacional. O geográfico é por países, estados ou cidades e utiliza-se de duas letras para identificação (Ex.: *uk*-Inglaterra, *br*-Brasil, *it*-Itália). No organizacional, os nomes comumente encontrados são: *COM* – Organizações Comerciais, *EDU* – Organizações Educacionais, *GOV* – Organizações Governamentais, *MIL* – Organizações Militares, *ORG* – Outras Organizações.

A estrutura da *Internet* pode ser entendida como uma estrutura hierárquica em três níveis. O menor nível consiste em redes locais fornecedoras de serviços para instituições acadêmicas, industriais e comerciais. O segundo nível consiste em redes regionais, as quais usualmente correspondem a uma região geográfica de um país. As redes regionais fornecem serviços que conectam as redes locais ao *backbone* (rede principal) de alta velocidade, que é o primeiro nível. Ex.: 1° nível com o provedor de acesso, 2° nível a Embratel/Fapesp e 3° nível o *NIC* (Núcleo de Informação e Coordenação do ponto *Br*).

A tarefa de resolução de nomes para determinado domínio deve ser executada por um servidor sob responsabilidade desse domínio. A máquina que oferece o serviço de resolução, assim como o mecanismo que o implementa, chama-se "Servidor de Nomes" (*Domain Name Server – DNS*). Um *DNS* mantém uma base de dados sobre os seus domínios que, geralmente, vai além da simples associação entre nome e endereço das máquinas, incluindo também informações sobre os recursos desses domínios, a exemplo dos servidores de *e-mail*. Juntos, os servidores de nomes formam uma árvore, em que cada nó tem um conhecimento parcial das associações relativas a seu domínio. Esses nós devem cooperar para oferecer uma resolução global de nomes, *i.e.*, um DNS deve descobrir qual servidor de nome é responsável por um determinado domínio, conhecido como *DNS* autoritário, para poder consultá-lo no caso de resoluções em seu domínio. A resolução de nomes se faz em duas etapas, sendo a primeira a procura para descobrir o *DNS* autoritário de determinado domínio para, em seguida, consultar este sobre a correspondência desejada.

Para ter acesso à *Internet*, é preciso ter computador, linha telefônica, aparelho de *modem* e *browser* (*software*), e ainda provedor de acesso, o *ISP's (Internet Service Providers).*

Os provedores de acesso podem ser conceituados como "instituições que se conectam na Internet via um ou mais acessos dedicados e disponibilizam acesso a terceiros a partir de suas instalações" (Castro, 2003, p. 69).

Pode-se afirmar que a maneira mais fácil para se ter acesso à *Internet* é via provedor. Nesse sentido,

> Assim, no sistema atual da rede temos, basicamente, milhões de computadores nos lares e empresas, ligados a computadores servidores maiores, em geral instalados em empresas que fornecem acesso, chamadas comumente de provedores de acesso à *Internet.* Os provedores inscrevem as máquinas de menor porte como suas usuárias e tornam disponíveis serviços para essas máquinas, que passam a ter acesso à grande rede por meio dos seus computadores. Por sua vez, os servidores das empresas provedoras são ligadas a grandes estruturas de comunicação chamadas de *backbones* que escoam pelo mundo afora o imenso tráfego de informação proveniente dos provedores de acesso mediante canais de satélite ou cabos submarinos (Góis Júnior, 2002, p. 49).

O provedor de acesso ou provedor de serviço pode ser pago ou gratuito. O provedor de acesso pago é disponibilizado ao usuário ao ser cadastrado os seus dados, junto ao Provedor, pagando-se mensalmente uma fatura do serviço que pode ser por meio de uma conta corresponde à disponibilidade de acesso a *Internet.* Os provedores gratuitos disponibilizam os serviços na própria rede, bastando que o interessado se cadastre para ter acesso aos serviços da *Internet.* Além do provedor, o usuário deve ter disponível uma linha telefônica, e o acesso pode ser discado, por banda larga ou por intermédio de uma rede corporativa, como, por exemplo, *"ADSL"*. Além da linha telefônica, outros meios podem ser utilizados – TV a cabo, satélite ou rádio.

O acesso discado é feito por meio da ligação telefônica via placa *modem* do microcomputador para a central de acesso à *Internet* do seu provedor. O *modem* tem a função de transformar os sinais digitais do computador do usuário em sinais analógicos da rede telefônica e vice-versa no provedor e do provedor para a *Internet*, fazendo a conexão necessária. O internauta paga a empresa Provedora de Acesso à *Internet,* e ainda a concessionária de telefonia pelos impulsos gastos durante o uso da rede.

Já no acesso direto, o usuário acessa o provedor utilizando o computador. Nesse caso, o que liga o usuário ao provedor sem intermediário é uma linha, cabo físico ou frequência de rádio (satélite), pagando uma taxa mensal pelo serviço.

O acesso via banda larga pode ocorrer de duas formas: com a ADSL (*Asymmetric Digital Subscriber Line*) e cabo-*modem*. Enquanto na primeira corre-se menos risco de congestionamento na rede, na segunda, o usuário, na maioria dos casos, é assinante de TV paga, representando um custo adicional. Outra modalidade de acesso pode ser realizada pela tecnologia *wi-fi* (*Wireless Fidelity*), que já pode ser encontrada em bares, restaurantes, hotéis e aeroportos. Para acessar a *Internet*, o usuário deve verificar o lugar da rede disponível, que é feito com o uso de antenas, dispensando o fio tradicional para logar em um provedor para conectar-se.

O acesso via rádio dispensa o uso de linha telefônica e é feito com a transmissão por ondas de rádio em alta frequência, com a instalação de antenas e distribuição de sinal via roteadores. Já o acesso via celular permite ao usuário conectar-se à *Internet* com a inserção de cartões ou *chips* que têm a função de *modems* em *notebooks* e *palmtops* e ainda por conexão, ligando o computador ao celular. A conexão por satélite é recomendada para lugares que não detêm outras tecnologias e tem custo mais elevado.

1.2. Aplicações da *Internet* no mundo contemporâneo

Inicialmente, a rede mundial de computadores tinha aplicação nos estudos científicos, de segurança nacional e nas pesquisas acadêmicas, mas surgiram outras finalidades com a democratização do acesso à *Internet*. O uso da internet no Brasil iniciou-se em 1988, na Universidade de São Paulo, por meio de um projeto desenvolvido por Oscar Sala, objetivando a troca de informações em uma rede de computadores (Fiorillo; Pegorari Conte, 2016)

Se alguém se perguntasse para que serve a *Internet* ou se alguém se questionasse sobre o mundo após conhecer a *Internet* e ter de ficar sem ela, é evidente que a resposta seria de que a tecnologia tem a tendência de evoluir e, portanto, de avançar ainda mais, como, por exemplo, o uso da *Internet* móvel[8].

No mundo contemporâneo, a *Internet* tem aplicações diversificadas. Além das funções primitivas de auxiliar nas pesquisas acadêmicas e nos trabalhos de segurança, outras foram sendo desenvolvidas com a finalidade de facilitar a troca de informações em todo o planeta.

Segundo Atheniense (2000) e Góis Júnior (2002), a *Internet* destaca-se nas seguintes aplicações:

a) *E-mail - Correio Eletrônico*

Tem a habilidade de compor, enviar e receber correio eletrônico (textos, memorandos e pequenos arquivos). Programas de *e-mail* estão disponíveis em praticamente todos os tipos de computadores atualmente, podendo o interessado comunicar-se com transmissões interestaduais e internacionais.

b) *News - Notícias*

Grupos de Notícias ou *news groups*, também chamados de flanelógrafos da rede, são *forums* especializados em que os usuários com interesse comum podem trocar mensagens. Existem grupos de notícias, tanto técnicos quanto não técnicos, que se comunicam sobre interesses comuns em computação, ciência, recreação, política, entre outros.

c) *Remote Login (Telnet) – Lugar Remoto*

Usando o *Telnet*, *Rlogin* ou outros programas, usuários em qualquer lugar na *Internet* podem logar em qualquer outra máquina na qual eles tenham permissão de acesso, sendo criticado pelos técnicos da área por ser de difícil aprendizado, uma vez que a operação necessita de muitos códigos.

d) *File Transfer Protocol (FTP)*

Com o programa Protocolo de Transferência de Arquivos (FTP), torna-se possível copiar arquivos (*download)* de uma máquina para outra na *Internet*. Vasta quantidade de artigos, bancos de dados, músicas em MP3, fotografias e outras informações estão disponíveis via FTP.

e) *World Wide Web (www)*

8 O padrão conhecido como 5G tem a proposta de integração entre redes fixas e móveis. Segundo informações da Teleco, os celulares aproximaram-se em funcionalidade de computadores e *PDAs*, com uma clara tendência dos terminais móveis computarem e dos computadores comunicarem cada vez mais.

Correa (2000) afirma que, em 1989, Tim Bernes-Lee proporcionou uma sugestão de trabalho de troca de informações entre estudiosos de lugares diversos, que faziam parte da *High Energy Physics Community*, mas tornou-se a mais nova aplicação, trazendo também milhões de usuários não acadêmicos para a rede.

O *www* possibilita o uso de todas as outras facilidades. Juntamente com um programa de navegação *(Browser)*, é possível para um *site* (máquina na rede rodando *www*) configurar um número de páginas de informação contendo textos, figuras, sons e vídeos, com ligações encapsuladas para outras páginas. Esse recurso viabilizou navegação e pesquisa na *Internet* com o uso de hipertextos.

Wolton (2012) informa que a *Internet* veio para fazer parte das comunicações sociais, somando-se ao rádio e à televisão, com importância em vários segmentos sociais. Esse avanço tecnológico trouxe várias consequências no mundo virtual que, de forma singular, alcança o mundo real com as facilidades atingidas que antes eram consideradas impensáveis.

Por intermédio da rede mundial de computadores, as pessoas podem comercializar os mais diferentes e exóticos produtos, adquirir objetos e serviços no pregão eletrônico e participar de licitações.

O campo de prestação de serviços cresceu vertiginosamente, uma vez que todos os profissionais liberais podem anunciar seus trabalhos na *Internet,* com contrato celebrado na forma virtual e possibilidade de se realizar trabalho *on-line*, flexibilizando o local de sua realização, sem contato físico com o empregador.

Para o profissional do Direito, a *Internet* é de grande valia, uma vez que é fonte de pesquisa doutrinária, legislativa e jurisprudencial, com acesso à pesquisa em tempo real e oportuniza, ainda, a quem tiver interesse a publicação de artigos científicos.

Para efetuar serviços bancários, a *Internet* tem servido como uma facilitadora para o usuário, que não necessita se deslocar até uma agência para pagar contas, retirar extratos, saldos e fazer outras transações. O uso de internet *banking* no Brasil tem crescido significativamente nos últimos anos. Segundo a Pesquisa FEBRABAN de Tecnologia Bancária de 2024, realizada pela Federação Brasileira de Bancos (Febrabam, 2025), o percentual de clientes que utilizam canais digitais (internet banking e *mobile banking*) tem aumentado constantemente.

De acordo com essa pesquisa, aproximadamente 82% dos correntistas no Brasil utilizam internet *banking* ou *mobile banking* como principal meio de acesso aos serviços bancários. A pesquisa indica que o *mobile banking*, em particular, tem sido o canal mais utilizado, utilizando-se ainda aplicativos específicos que podem ser acessados em aparelhos celulares e a pesquisa apontou que de 208,2 bilhões de transações bancárias feitas pelos correntistas, 75% delas ocorreram por um aparelho celular (Febrabam, 2025, on line).

Todavia, a *Internet* tem sido usurpada por pessoas que têm acesso permitido ou não, para fins lesivos previstos e não previstos em lei. As instituições bancárias, por exemplo, têm sofrido grandes prejuízos pelas fraudes praticadas em contas bancárias de seus clientes, o que implica grandes investimentos na segurança. De acordo com o Relatório FEBRABAN de Segurança Cibernética de 2022, os

ataques cibernéticos e as tentativas de fraudes contra bancos e seus clientes têm aumentado. Em 2021, os bancos investiram cerca de R$ 2,5 bilhões em segurança da informação, um aumento de 8% em relação ao ano anterior. Esse investimento inclui medidas para prevenir fraudes e fortalecer a segurança dos sistemas bancários.

1.3. Administração da *Internet*

O controle mundial da *Internet* é exercido pela *Internet Corporation for Assigned Names and Numbers* (ICANN) ou, em português, "Corporação da Internet para atribuição de Nomes e Números", vinculada ao Departamento de Comércio dos Estados Unidos. O ICANN é uma associação norte-americana sem fins lucrativos, que detém a chave tecnológica em que são distribuídos os nomes de domínio, os "endereços" na *Internet* (regido por um conselho de quinze representantes de todos os continentes, entre eles o Brasil), possibilitando que um *e-mail* chegue ao seu destinatário.

Os Estados Unidos têm sido o administrador mundial da rede desde que a *Internet* foi criada nos anos 60. O poder de força americano é grande, uma vez que pode tirar do ar o domínio de um país *TLD TOP LEVEL DAMAIN* (TLD), como o *Br* do Brasil. Todavia, vários países têm levantado a hipótese de repartição de poderes da *Internet*, como Brasil, China, Índia e União Europeia.

Contudo, corporações como as empresas do *Google*, *Amazon*, Meta (*Facebook*) e *Microsoft* possuem grande influência na infraestrutura da *Internet*, controlando servidores, cabos submarinos e outros recursos essenciais.

A administração mundial da rede foi tema da Cúpula Mundial da Sociedade da Informação em Tunis, na Tunísia, no mês de novembro de 2005, e em outros eventos promovidos pela *Internet Corporation for Assigned Names and Nu*mbers (ICANN), responsável pela gestão do sistema de nomes de domínio (DNS) e endereços IP, enquanto a *Internet Engineering Task Force* (IETF) define os padrões técnicos da internet.

Outra organização chamada *IAB Internet Architecture Board (IAB)* é responsável pelo desenvolvimento e pelas publicações dos padrões dos protocolos que foram ou irão ser adotados pela *Internet*. O *IAB* é um comitê para projeto, engenharia e gerenciamento da *Internet* (Corrêa, 2000).

No Brasil, o grande problema enfrentado pela *Internet* diz respeito à infraestrutura das telecomunicações com serviços caros e de má qualidade, o que inibe um investimento maior nessa área. O espaço .br é controlado pelo Comitê Gestor de *Internet*, CGI.br, que define diretrizes estratégicas e políticas para desenvolvimento e uso da internet no Brasil e coordena as atividades do NIC.br para promover iniciativas e garantir segurança, estabilidade e desenvolvimento da infraestrutura da internet no País.

2. VULNERABILIDADE E SEGURANÇA NA *INTERNET*

Com o surgimento da *Internet*, a aparente democratização ao acesso de informações e a multiplicidade de aplicações implicou práticas de condutas lesivas, sejam elas tipificadas em lei penal ou não, o que demonstra vulnerabilidade e falta de segurança na rede.

Assim, estudiosos do tema que engloba Direito, Informática, Comunicações e Pedagogia têm se preocupado com a fragilidade da rede Mundial de Computadores, isso porque,

> Da mesma forma que uma pessoa dirigindo um veículo pode sofrer um acidente ou cometer algum ato ilícito, quando, por exemplo, atropela ou albaroa seu carro por não ter obedecido à sinalização, outra navegando pela Internet é perfeitamente vulnerável à ação de *hackers,* vírus de computadores e fraudadores, podendo, até, cometer atos ilícitos, quando desrespeita os limites estabelecidos pelos sistemas de segurança de determinada empresa conectada à Rede, ou remete mensagens eletrônicas ameaçando outrem (Corrêa, 2000, p.10).

A utilização da *Internet* pode ocorrer de várias maneiras, pois o usuário pode ter acesso por meio de provedores pagos ou gratuitos. Os provedores pagos, ou seja, em que o usuário paga uma taxa mensal, devem disponibilizar informações por escrito ou na via eletrônica para que o serviço prestado não tenha descaracterizado sua utilização. Essa preocupação tem razão de ser, uma vez que os doutrinadores têm entendido que os provedores têm responsabilidade perante o usuário (Góis Júnior, 2002; Drummond, 2003).

Ao abrir uma conta em um provedor, serão fornecidos senha e *login* da conta na *Internet*, que não poderá ser divulgada, a exemplo de dados de uma conta bancária. Se o usuário *clicar* no campo de lembrar senha, já estará vulnerabilizando seu acesso a pessoas estranhas.

As fraudes, segundo informa o CERT.br, representam 45% de todos os incidentes de segurança, ficando em segundo lugar os *Worms* e *Scans*[9]. Além das técnicas acima explicitadas, outras condutas poderão surgir a qualquer momento e podem levar ao descompasso entre a evolução da tecnologia e do direito.

Sobre a fragilidade da *Internet,* autores como Wolton (2012) e Ribeiro (2019) concordam que o anonimato é uma das principais causas que facilitam o ataque. Os provedores gratuitos dificultam a defesa das vítimas. O acesso anônimo, ou conexão anônima, como ensina Góis Júnior (2002), impossibilita a identificação do usuário, o que pode levar à impunidade.

Os agentes podem escolher o ambiente de um *cybercafé*[10], ou de uma *lan house*[11], com a certeza de que estarão seguros para cometer o ilícito. Nessas empresas, em geral, não há identificação de quem tem o acesso à *Internet,* bastando que se faça o pagamento do serviço prestado, cobrado por hora de

---

9 *Scans* são programas que varrem portas de comunicação de *PCS* em busca de uma brecha e se diferem dos *scams*, que são *e-mails* que capturam dados pessoais e financeiros.

10 Os *cibercafés* são bares, restaurantes e outros lugares abertos ao público que fornecem serviços de acesso à Internet.

11 *Lans Houses* são empresas que prestam pequenos serviços informáticos, tais como digitação, baixa de arquivos e serviços de *Internet*, de que os internautas fazem uso nas cidades brasileiras.

acesso. Viana (2003) assevera que a falha apontada por autores é o uso de *laptops*[12] conectados por *wi fi* gratuita para a prática de crimes digitais que vulnera a *Internet* e dificulta a ação policial na identificação da chamada, porque o criminoso faz uso de senhas falsas.

Fatores que podem levar à vulnerabilidade da rede são o acesso precário à infraestrutura, como falta de cobertura de internet banda larga, conexões lentas e instáveis, custos elevados para acesso à internet e equipamentos e má qualidade da infraestrutura de telecomunicações.

A ausência de habilidade digital e o baixo nível de conhecimento da população para utilizar a *Internet* de forma eficaz e segura dificultam o acesso à informação, aos serviços *online* e às oportunidades de inclusão social e econômica.

A Segurança cibernética torna-se precária pelo uso de infraestrutura de *Internet* vulnerável a ataques cibernéticos, falta de medidas de segurança adequadas por parte de governos e empresas e baixo nível de conhecimento da população sobre segurança *online*.

Outro fator importante que deve ser mencionado é a falta de leis e políticas claras que regulem o uso da internet, protejam a privacidade dos dados e combatam crimes *online,* o que cria um ambiente propício para abusos e violações.

2.1. Os ilícitos penais praticados na rede mundial de computadores

Após o advento da *Internet* e a abertura ao uso público, várias foram as condutas praticadas para lesar as pessoas, com ofensa direta a bens jurídicos tutelados. Além de graves ofensas a direitos já resguardados, outras questões surgem quando se verificam, na prática, condutas ofensivas que sequer estão regulamentadas.

Inicialmente, será feita uma breve exposição conceitual do que seja ilícito, ilícito penal e crime, para, posteriormente, ingressar-se na exposição dos ilícitos penais praticados na rede mundial de computadores.

A palavra ilícito advém de *illicitus,* de *il*, em vez de *in*, e *ilicitus*, que quer dizer o que é proibido, vedado por lei, em sentido próprio ou vedado por lei. Ilícito pode ser assim definido: "Todo fato ou ato que importe numa violação ao direito ou em dano causado a outrem, provenha do dolo ou se funde na culpa" (Silva, 1987, p. 407).

Ainda no dizer de Silva (1987, p. 408), o ilícito é o gênero, podendo ser dividido em ilícito civil e ilícito penal. O ilícito civil consiste em "toda ação ou omissão, de que resulte ou se gere prejuízo a direitos alheios ou ofensa a legítimos interesses de outrem, a qual se pratique em contravenção ao que se preceitua na lei ou contrariamente aos princípios gerais do *neminem laedere*". Já o ilícito penal é

> Ato vedado em lei ou, a omissão de fato não permitido, constitui o delito propriamente dito, sujeitando a pessoa a duas sanções diferentes: a penal, consistente na repressão e consequente punição da ilicitude, e a civil, decorrente de indenização a que se sujeita, para reintegração da ofensa material causada ao patrimônio da vítima (Silva, 1987, p. 408).

12 *Laptops* são um tipo de *notebook* mais simplificado. Não confundir com *Palmtop*, espécie de computador portátil.

Para melhor entender sobre o delito, primeiramente se fará a conceituação clássica de crime para, em seguida, serem definidos os crimes digitais. Para Gioseppe Bettiol (apud Teles, 2006, p. 153), o crime pode ser conceituado, materialmente, como "todo fato humano lesivo de um interesse capaz de comprometer as condições de existência, de conservação e de desenvolvimento da sociedade".

Francesco Carrara (1841, p. 50-51), em uma orientação clássica do delito, o entende como ente jurídico, pois "a ideia de delito não é senão uma ideia de relação, a saber, a relação de contradição entre o fato humano e a lei. Somente nisso consiste o ente jurídico, ao qual se dá o nome de delito". Prado (2011) explica que o delito é compreendido como ente indivisível, ou seja, como uma contrariedade de uma norma indivisível a todo o ordenamento jurídico.

Nesse tópico, não se tratará da teoria do crime. Contudo, a ideia é justificar o que configura crime ou, para alguns autores como Prado (2011), delito como a desobediência a uma norma existente que prevê penalidade em caso de descumprimento.

A Organização de Cooperação e Desenvolvimento Econômico (OCDE) propôs, em 1986, uma definição ampla, conceituando crime informático como "qualquer conduta ilegal não ética, ou não autorizada que envolva processamento automático de dados e/ou transmissão de dados".

A expressão 'crimes informáticos' não é uniforme na doutrina e possui variações de acordo com o entendimento dos autores. Também é conhecida como crimes de computadores, *cybercrimes,* cibercrimes, *computer crimes, computing* crimes, crimes tecnológicos, delitos informáticos, crimes digitais, e crimes eletrônicos (Reis, 1987; Rosa, 2002; Silva, 2003; Crespo, 2011; Kolbe Júnior, 2020).

O crime de informática pode ser utilizado em uma acepção mais ampla, abrangendo os crimes cometidos por intermédio da *Internet,* ou seja, os crimes praticados na *Internet* são espécies dos crimes informáticos (Castro, 2003). Nesse entendimento, pode-se conceituar o crime de informática como sendo

> Aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através do computador. Inclui-se neste conceito os delitos praticados através da *Internet,* pois pressuposto para acessar a rede é a utilização de um computador (Castro, 2003, p. 9).

Podem ser denominados de *computer* crime, abuso de computador, crime de computação, criminalidade mediante computadores, delito informático, fraude informática, delinquência econômica e *computerkriminalista*. Entrementes, Reis (1996) e Crespo (2011) criticam todas essas acepções, concluindo que vinculam, de algum modo, a conduta aos computadores, preferindo a denominação de *computer* crime, porque a conduta pode "se dar na unidade de entrada, de saída, na central de processamento, em um dispositivo de armazenamento ou de transmissão de informações" (Reis, 1996, p. 24).

Ainda seguindo o pensamento de Reis (1996), afirma-se que podem ser sintetizados como violação dos direitos autorais sobre *softwares*, furto de dados e dano causado pelos famosos *vírus* de computador.

Na denominação de crimes digitais,

> Poderíamos dizer que os "crimes" digitais seriam todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico (Corrêa, 2000, p. 43).

Vladimir Aras (2001, *online*), em artigo na *Internet*, ensina que,

> Dentre essas designações, as mais comumente utilizadas têm sido as de crimes informáticos ou crimes de informática, sendo que as expressões "crimes telemáticos" ou "*cibercrimes*" são mais apropriadas para identificar infrações que atinjam redes de computadores ou a própria *Internet* ou que sejam praticados por essas vias. Estes são crimes à distância *strictu sensu*.

Quanto à terminologia "crimes virtuais", Pinheiro César (2001) e Fiorillo e Pegoraro Conte (2016) definem o conceito amplo de criminalidade informática abrangendo situações que envolvem o uso do computador para praticar crimes ou crimes contra o próprio computador ou as informações armazenadas como puros, mistos e comuns. Os virtuais puros são os que tenham por objetivo o sistema de computador, seja causando danos físicos ou técnicos dos equipamentos ou seus componentes. Os virtuais mistos são aqueles em que a *Internet* é um requisito primordial para que a conduta seja realizada, embora o bem jurídico tutelado seja diverso ao informático. Os virtuais comuns são aqueles em que a *Internet* é apenas um meio para se praticar condutas tipificadas na lei.

Crespo (2011, p. 21) assevera que,

> [...] embora haja inúmeras divergências doutrinárias, a expressão que nos soa mais adequada é "crimes digitais", seja pelo que se pretende regular – a informática – seja porque, ainda que haja ilícitos praticados por meio da telemática (mais modernos), a informática é pressuposto daquela, de modo que a expressão não é equivocada, sendo a adotada neste trabalho.

Apenas para exemplificar a grandeza do universo dos fatos tipificados ou não em lei, podem ser citados: ofensas contra a honra, incentivo ao uso de drogas, ameaças e extorsão, acesso não autorizado a arquivos confidenciais, destruição e falsificação de documentos eletrônicos, crimes eleitorais, propaganda não autorizada, concorrência desleal, violação de direito autoral, pedofilia, fraudes em instituições financeiras, furto de tempo, racismo, estelionato em todas as modalidades, lavagem de dinheiro, crimes do colarinho branco, *salami slicing*[13], contrabando, terrorismo, vandalismo, sabotagem, vírus de computador, pirataria, tráfico internacional de armas, jogos ilegais, entre outros.

É imprescindível explicar os ilícitos penais cometidos na *Internet*, classificando-os em próprios e impróprios.

13 É a conduta que permite que pessoas que transfiram, periodicamente, pequenas quantias de dinheiro de muitas contas bancárias para sua própria conta ou em conta de terceiros, conhecidos pela polícia de laranjas porque emprestam suas contas para receber créditos fraudulentos.

2.1.1. Crimes próprios

Os crimes informáticos podem ser chamados de crimes digitais ou virtuais e são classificados em crimes próprios e impróprios. Os crimes próprios são aqueles em que o autor do fato só pode praticá-los utilizando-se da informática, e só podem ser cometidos no ambiente digital. A tecnologia não é apenas um meio para o crime, mas sim o objeto ou a essência da conduta criminosa. Sem a internet ou um sistema informático, esses crimes simplesmente não existiriam, como os exemplos a seguir.

a) Pirataria de *software*

O *software* no Brasil encontra-se regulamentado no art. 12 da Lei nº 9609, de 19 de fevereiro de 1998, ao dispor sobre a reprodução não autorizada de um programa de computador. O agente responde na conduta de reproduzir, difundir ou comunicar ao público, sem autorização, um programa de computador, estando ele registrado ou não no Instituto Nacional de Propriedade Industrial (INPI), sediado em Brasília.

O crime é de ação múltipla, com a previsão, no parágrafo segundo do mesmo artigo, de outras formas de se praticar o crime, quais sejam: venda, exposição à venda, introdução no país, aquisição e ocultação ou depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral[14].

A *Internet* pode ser utilizada pelos piratas da rede na modalidade de divulgar e distribuir, sem pagamento ao autor do programa, das cópias reproduzidas na rede, tornando, de forma indevida, acessível a qualquer pessoa ao fazer *download*[15] no computador (Castro, 2003).

b) Vandalismo na *Internet*

A *Internet* tem sido objeto para a prática de vândalos que colocam, sem autorização, textos ou figuras em *sites* ou *blogs* de terceiros. É a chamada pichação virtual ou *defacement*. Segundo Jesus e Milagre (2016), em algumas situações pode configurar crime de dano.

c) Envio e provocação de dano na rede por *vírus*

Essa conduta é de difícil classificação em crime próprio ou impróprio, porque o vírus só pode ser enviado por intermédio de um arquivo para o destinatário, logo, um crime que só se pratica via *Internet.* Por outro lado, é uma conduta já tipificada, seja como crime de dano, prevista no art. 163 do Código Penal, se tiver causado prejuízo para as vítimas, seja como crime de perigo, art. 259 do Código Penal, na hipótese em que o vírus for disparado, mas não danificar e não se difundir pela rede, sendo impedida a infecção de vários arquivos nos computadores que estejam interligados (Castro, 2003; Góis Júnior, 2002).

Vírus pode ser definido como "um programa estranho ao sistema do computador capaz de copiar e instalar a si próprio, resultando na realização de tarefas não solicitadas e destruindo arquivos e seus correspondentes dados" (Castro, 2003, p. 27). É, na opinião de Rosa (2002), o segmento de programa de computação capaz de mudar a estrutura do software do sistema e destruir, alterar dados ou programas ou outras ações nocivas, com ou sem o conhecimento do operador.

14 Nos termos do art. 12, § 2º. da Lei n. 9.609/1998.

15 *Download* significa baixar um arquivo da *Internet*.

Paralelamente aos vírus, existem outros tipos de arquivos, os *worms* e os *trojans*. Para Castro (2003), *Worms* (vermes) são programas ou conjunto de programas que têm a função de replicação e reenvio para execução de ataque. Pode-se dizer também *que* "*worm* é um programa de proteção de cópias que destrói os dados armazenados quando é detectado qualquer programa não autorizado que procura copiar os arquivos" (Camarão, 1994, p. 687).

A *Internet* foi cenário de vários tipos de vírus, tais como: *Iloveyou* (2000), *Code Red* (2001), *Welchia/Nachi* (2003), *Mydoom* (2004), *Emotet* (2014), entre outros, e podem ser classificados em: os que não causam perturbação ao sistema informático; o humorístico; o alterador que modifica dados em arquivos, planilhas, bancos de dados; o catastrófico, que apaga dados ou arquivos, com a destruição desordenada de informações do disco rígido e de dispositivos conectados ao sistema; o genérico, que fica escondido no meio, começo e fim dos programas de informática e, só quando tem a função ativada, modifica e destrói arquivos (Reis, 1996; De Lima, 2020).

d) Violação de *e-mail*

O *e-mail* ou correio eletrônico, como é chamado, é uma forma de se corresponder na *Internet*, com o envio de mensagens por escrito ao destinatário. Tem a função de transmitir documentos que podem ser anexados à mensagem enviada e possibilita o envio de imagens, planilhas, arquivos de som e vídeo, sendo uma tendência nova em comunicação (Atheniense, 2000).

A conduta irregular ocorre com a violação dessa correspondência, com a leitura de mensagens armazenadas na memória do computador. São as mensagens abertas que não são lacradas por envelope, como se faz usualmente na correspondência comum. Contudo, o conteúdo das mensagens, na maioria das vezes, é de cunho confidencial, particular, devendo ter a proteção da privacidade, prevista em lei. Os autores discordavam, nesse aspecto, em qual medida tomar, em face da inexistência de legislação específica, para adequar a conduta supracitada no art. 151 do Código Penal Brasileiro, qual seja a violação de correspondência, ou no art. 10 da Lei nº 9.296/1996, que regula a interceptação do fluxo de comunicações em sistema de informática e telemática (Castro, 2003; Góis Júnior, 2002; Drummond, 2003).

Todavia, com a Lei nº 12.737/2012, mais conhecida como Lei Carolina Dieckmann, essa possibilidade encontra-se tipificada no art. 154-A e seus parágrafos do Código Penal brasileiro, ao prever pena de reclusão de até dois anos para o invasor de dispositivo informático conectado ou não à *Internet* que tiver acesso às comunicações eletrônicas privadas.

e) Envio de *spans*

Atividade muito comum na *Internet*, ocorre com o envio de mensagens não solicitadas de conteúdo comercial ou de *marketing*, com a finalidade de vender produtos ou serviços (Jesus; Milagre, 2016). Nesse sentido,

> O *span* é uma comunicação. Uma comunicação que não fora solicitada pelo usuário de uma determinada conta de correio eletrônico. Ou seja, ainda que não tenha feito qualquer tipo de pedido ou solicitação, uma mensagem qualquer irá ser enviada ao correio eletrônico de um usuário na *Internet* e este terá a possibilidade ou não de tomar conhecimento de seu teor (Drummond, 2003, p. 108).

Os doutrinadores que estudam o *spam* entendem que se trata de uma conduta nova, porque só pode ser enviada com a utilização da *Internet*. Outros entendem que é mais uma modalidade de crime de dano, porque se todos puderem enviar *spams* a todos os usuários da rede, haverá prejuízos de grande monta para o recebimento das mensagens não autorizadas, no congestionamento do tráfego na *Internet* e no gasto da memória do computador, acarretando a incapacidade técnica de funcionamento da máquina utilizada pelo internauta e perda de tempo na leitura (Drummond, 2003; Vianna, 2005).

2.1.2. Crimes impróprios

Os crimes impróprios, ao contrário dos próprios, são aqueles que podem ser praticados por qualquer meio, inclusive com uso do computador, utilizando-se o agente da *Internet.* A seguir, serão abordadas algumas condutas que podem ser praticadas na rede e que são tipificadas legalmente.

a) Crimes contra o Patrimônio

O crime de estelionato previsto no art. 171 do Código Penal pode ser praticado na *Internet.* Ocorre o crime quando o sujeito ativo aproveita de ingenuidade ou desconhecimento da vítima para aferir qualquer vantagem patrimonial. Mirabete (2013, p. 303) ensina que "existe o crime, portanto, quando o agente emprega qualquer meio fraudulento, induzindo alguém em erro ou mantendo-o nessa situação e conseguindo, assim, uma vantagem indevida para si ou para outrem, com lesão patrimonial alheia".

Essa modalidade de ilícito pode ser praticada na *Internet* quando o agente compra, vende, investe e engana outras pessoas ao descrever produtos com defeito, ou inexistentes, muito comuns na venda de falsos aparelhos celulares. Também se pode fazer o uso de métodos na invasão dos sistemas, como o Cavalo de Troia (*Trojan Horse*), sabotando dados do usuário na *Internet*. O golpe é comumente utilizado pelos *hackers* para capturar senhas bancárias, números de contas bancárias, números de documentos, como identidade e CPF, e dados de cartões bancários e de créditos.

O contato direto ou indireto com a vítima se faz por intermédio das *homepages*, *sites*, conversas *online* e eletrônicas. O estelionato virtual tem gerado prejuízos às instituições públicas e particulares e ainda a pessoas físicas que possuem relações comerciais ou não com essas instituições. Além do estelionato, outras condutas estão subsumidas no tipo penal como crime de dano, previsto no art. 163 do Código Penal, por exemplo, a inserção não autorizada de *spans.*

b) Crimes contra a dignidade sexual

Os crimes contra a dignidade sexual previstos no Código Penal, capítulo VI, do Ultraje Público ao Pudor, nas figuras dos arts. 213 e 234, abrangem diversas figuras típicas, inclusive aquelas que podem ser praticadas na *Internet,* em ambiente exposto ao público, com o uso de imagens acopladas ao computador.

O art. 218-C detalha o crime de divulgação de cena de estupro ou de cena de estupro de vulnerável em diversas modalidades, dentre elas a de divulgar as imagens por qualquer meio que pode ser incluído à *Internet* com penas de reclusão de 1 a 5 anos. No Estatuto da Criança e do Adolescente, a figura

do art. 241-A, §1º, possui redação semelhante e traz com clareza a intenção da legislação em proteger essas pessoas mais vulneráveis de criminosos digitais:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
>
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
>
> § 1 ° Nas mesmas penas incorre quem:
>
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
>
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
>
> § 2 ° As condutas tipificadas nos incisos I e II do § 1 ° deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo. (Brasil, 1990).

Para Nucci (2020, p. 1203),

> O tipo penal foi criado com destino certo: tutelar a exposição, pela internet, de foto/vídeo de: a) estupro nas duas formas: típica (art. 213, CP) e contra vulnerável (art. 217-A, CP) ou a sua apologia (defesa, elogio, enaltecimento) ou induzimento (dar a ideia; incentivo); b) sexo, nudez ou pornografia (forma de explorar o sexo de maneira chula ou grosseira). Esses dois objetivos advieram dos vários casos concretos, acompanhados pela sociedade brasileira, nos últimos tempos. Houve quem estuprasse uma moça, inconsciente ou semi-inconsciente, colocando o vídeo dessa conduta na internet para conhecimento público. Houve, ainda, quem divulgasse foto de namorada nua ou de relação sexual mantida entre namorados, igualmente, para ciência pública em redes sociais.

Outra conduta seria a de praticar ato obsceno na rede, que é verificada com a difusão de páginas de cenas de sexo explícito, levando ao conhecimento público de *site* com conteúdo dessa natureza. Para alguns usuários, funciona como um programa de acesso livre, um *Big Brother*[16], por exemplo, quando as imagens são divulgadas em tempo real.

O crime de escrito ou objeto obsceno é materializado com aquisição, guarda, para fins de comércio, de distribuição ou de exposição pública de escrito, desenho, pintura, estampa ou qualquer outro objeto obsceno. Vender produtos eróticos na *Internet* pode ser tipificado como conduta ilícita, assim como, também, é a prática de qualquer dessas condutas em estabelecimentos comerciais.

No entanto, era uma prática tolerada pelo poder público, como, por exemplo, em uma locadora de vídeo, o armazenamento de material (*DVDS*) pornográfico em local restrito às pessoas maiores de dezoito anos (Castro, 2003).

16 *Big Brother* é um programa de televisão em que pessoas aceitam morar em uma casa fornecida pela rede de televisão por um determinado período. Os participantes autorizam as filmagens da casa em tempo real, tendo o telespectador a oportunidade de ter acesso a tudo que ocorre, tanto na TV quanto na *Internet*.

Percebe-se a preocupação do legislador ao dispor, expressamente, que a *Internet* é um meio de se praticar o crime de pornografia infantil. Uma das condutas mais combatida pelos doutrinadores é a pedofilia praticada na *Internet,* apesar de a pedofilia ser o sentimento que os agentes têm em relação às crianças e aos adolescentes (Góis Júnior, 2002).

c) Crimes contra a Liberdade Individual

O crime de intimidação sistemática, previsto no art. 146-A, prevê o formato de intimidar a vítima, seja individual ou em grupo, mediante violência física ou psicológica, com a prática de atos de humilhação, discriminação ou ações verbais, morais, sexuais, sociais, materiais ou virtuais, que podem ser praticadas na internet, seja em rede social, de aplicativos, de jogos *online* ou qualquer outro meio, ou transmitida em tempo real.

O crime de ameaça disposto no art. 147 do Código Penal pode ser praticado na rede, uma vez que é possível o envio de conteúdo ameaçador de correspondência eletrônica, para que a pessoa se sinta constrangida e intimidada. Masini Neto (2025) explica sobre novas regras mais gravosas ao entrar em vigor a Lei nº 14.132/2021, que incluiu o tipo de perseguição obsessiva que pode ocorrer na internet (*cyberstalking).* Nessa hipótese, o perseguidor envia e-mails, mensagens nas redes sociais da vítima para manter contato forçado e reiterado, além de, em alguns casos, ameaçar de morte seus parentes.

d) Crimes contra a Honra

Uma das modalidades mais comuns na *Internet* é a prática de crimes de calúnia, difamação e injúria, arts.138, 139 e 140 do Código Penal. Tanto a calúnia quanto a difamação tutelam a honra objetiva da vítima, consumando-se o crime com o conhecimento de terceiros do conteúdo de calúnia ou difamação inseridas na *Internet.* Tais condutas podem ser cometidas na rede, como, por exemplo, em *homepages,* salas de bate-papo e conversas *online*, em que várias pessoas estão conectadas ao mesmo tempo.

A injúria afeta a honra subjetiva e se consuma quando a vítima toma conhecimento de uma característica particular que lhe é imputada, um conceito que lhe é endereçado, por exemplo, afirmar que a vítima é malandra, podendo ocorrer em salas de conversas *online*, *homepages*, *e-mails*, entre outros (Castro, 2003). É o caso do *cyberbullying,* versão informatizada do *bullying,* este último é o termo denominado para agressões presenciais físicas ou psicológicas feitas entre crianças e adolescentes nas escolas, por exemplo, as brigas no horário de intervalo das aulas.

O *cyberbullying,* por sua vez, ocorria em ambiente virtual com o antigo *MSN,* mensagens via celular e *Orkut*. Atualmente, via *Facebook,* Telegram, *WhatsApp*, entre outras plataformas digitais, em que há agrupamentos de pessoas praticando ofensas entre si, tudo via *on-line* e em tempo real. Ribeiro (2019) cita como exemplos de *cyberbullying*: mensagens inflamadas nas redes sociais, assédio, perseguição, videolinchamento, exposição, difamação, dentre outras.

f) Outros crimes

Ainda é possível na *Internet* a prática de jogos de apostas na rede (contravenção penal, art. 50 do Decreto-Lei nº 3.688/1940); a pirataria cibernética (uso de *MP3*) para piratear a música, causando prejuízos de ordem material e moral com violação de direito autoral; o terrorismo, com a recente Lei nº 13.260/2016; a prática de racismo; crime de dano, previsto no art. 163 do Código Penal; crime de divulgação de segredo, disposto no art. 153, do Código Penal, entre outros.

Nesse ponto, Masini Neto (2025) informa que é importante lembrar que alguns tipos penais foram modificados pela Lei nº 14.155, de 27 de maio de 2021, marco importante na legislação brasileira sobre crimes cibernéticos. Ela alterou o Código Penal (Decreto-Lei nº 2.848/1940) e o Código de Processo Penal (Decreto-Lei nº 3.689/1941) para tornar mais graves as penas de crimes já existentes e para inserir novas modalidades e qualificadoras relacionadas ao uso da tecnologia. As principais modificações e tipos penais afetados podem ser observados a seguir.

a) Invasão de dispositivo informático (art. 154-A do Código Penal): a pena para o crime de invasão de dispositivo informático, que antes era de detenção, passou a ser de reclusão, aumentando o rigor da punição, e inseridas qualificadoras que aumentam a pena em casos de: obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas e controle remoto não autorizado do dispositivo invadido (Masini Neto, 2025).

b) Furto qualificado pela fraude eletrônica (art. 155, § 4º-B e § 4º-C, do Código Penal): foi criada nova qualificadora para o furto, específica para os casos em que a fraude é cometida por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem violação de mecanismo de segurança ou utilização de programa malicioso. Foram incluídas causas de aumento de pena para esse tipo de furto se ele for praticado mediante a utilização de servidor mantido fora do território nacional e contra idoso ou vulnerável (Masini Neto, 2025).

c) Estelionato mediante fraude eletrônica (art. 171, § 2º-A e § 2º-B, do Código Penal): foi inserida a figura do estelionato cometido mediante fraude eletrônica, quando a fraude é praticada com a utilização de informações fornecidas pela vítima ou por terceiro, induzido a erro, por meio de redes sociais, contatos telefônicos, envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. Foram estabelecidas causas de aumento de pena se o crime for praticado: mediante a utilização de servidor mantido fora do território nacional e contra idoso ou vulnerável (Masini Neto, 2025).

d) Estelionato contra idoso ou vulnerável (art. 171, §4º, do Código Penal): a lei ampliou a proteção a idosos e vulneráveis. Antes, a pena do estelionato era dobrada se cometido contra idoso. A Lei nº 14.155/2021 estabeleceu um aumento de pena de 1/3 (um terço) ao dobro se o crime for cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso (Wendt; Jorge, 2021).

Em resumo, a Lei nº 14.155/2021 teve como principal objetivo endurecer o combate aos crimes cibernéticos no Brasil, especialmente aqueles de fraude e furto praticados no ambiente digital, e aprimorar a capacidade de investigação e processamento desses delitos.

2.1.3. As técnicas de ataques mais utilizadas na *Internet*

Para a prática das condutas lesivas e dos ilícitos na *Internet*, são utilizadas diversas técnicas. Vários exemplos são citados no site do CERT.Br, que é um CSIRT (grupo de segurança e respostas a incidentes) Nacional de Último Recurso, mantido pelo NIC.br, e presta serviços na área de Gestão de Incidentes de Segurança da Informação para qualquer rede que utilize recursos administrados pelo NIC.br. Vejamos alguns.

a) Cavalo de Troia – *Trojans Horses*

Camarão (1994) afirma que é uma técnica utilizada pelos agentes digitais utilizando-se de um sistema de processamento de dados desconhecido, direcionado para os administradores desse sistema e para seus usuários.

Vianna (2005) complementa que o programa denominado Cavalo de Troia chega anexado a um *e-mail* ou a um *link,* simulando ter propósito útil ou de forma que o internauta não saiba que está tendo seu computador invadido por um programa intruso, não solicitado. Os *trojans* monitoram a digitação do *login*[17] e da senha que a vítima informa ao adentrar em um sistema informático, armazenando-a e gravando-a em um arquivo oculto (Jesus; Milagre, 2016).

Uma das formas de invasão ocorre com o acesso de jogos baixados na *web,* em que quem envia o arquivo do jogo envia também o programa de Cavalo de Troia embutido no arquivo do jogo. Este, ao ser aberto, pode causar danos irreparáveis ao usuário, como furto de dados e danos em outros arquivos.

b) Engenharia Social

Técnica que se utiliza para ganhar a confiança da vítima, fazendo-se passar por outra pessoa, que a vítima tenha amizade ou seja subordinada em seu trabalho, para obter dados privativos de caráter confidencial. Pode ser denominada como um "conjunto de ações com a finalidade de captar dados do usuário, e com o uso deles, acessar via Internet e cometer crimes" (Góis Júnior, 2001).

O autor explica que o agente telefona para a central de cartão de crédito e informa que perdeu a senha, se passando pelo cliente. O operador, ao supor que se trata realmente de um cliente, solicita dados dos quais o *cracker* já disponibiliza informando a senha. A engenharia social pode ser normal ou inversa. A inversa ocorre quando o atacante cria uma situação-problema que induz a vítima a buscar ajuda e é levada a entrar em contato com o *cracker* (Mitnick, 2003). Geralmente, o engenheiro social utiliza-se do mecanismo do *e-mail drops*[18] ou de envio de texto no (MSN) no celular da vítima com mensagens informativas de que a pessoa foi premiada com pontos de milhagens no cartão de crédito. Ao ler a mensagem, a vítima acessa um *link* que dá acesso a informações sigilosas da conta bancária, que são capturadas pelo agressor.

---

17 *Logins* são formas de acesso em um sistema. Um sistema utilizado por vários usuários necessita que cada um deles se identifique usando uma senha, possibilitando-lhes o acesso aos arquivos e demais recursos.

18 Caixa postal alugada com nome fictício para receber documentos ou pacotes em que a vítima for convencida a enviar (Mitnick, 2003).

c) Sniffing – Furto de Senhas

É um programa que analisa o tráfego na *Internet* com a função de gerenciar redes (Plantullo, 2003). Alguns o denominam de outra forma, como sendo roubo de senhas, mas Góis Júnior (2002) critica esse posicionamento, uma vez que não há uso de força ou coação.

São também conhecidos como ferramentas *cracker* usados pelos agentes, porque permitem a descoberta da senha quando são rastreadas pelos computadores com pesquisa à cadeia numérica ou pacotes de dados, podendo ser armazenadas para uso em momento oportuno.

d) *Mails Bombs*. *E-mails* com bombas

Método adotado para inundar um computador de mensagens eletrônicas, abarrotando a caixa postal do usuário, o que acarreta sobrecarga, que provocam negação no serviço de correio eletrônico (Plantullo, 2003; Jesus, Milagre, 2016).

e) Alteração de conteúdo

Para Plantullo (2003), é uma das formas mais comuns que os *crackers* fazem para modificar o teor dos documentos na *Internet*, como as páginas *WEB*, e consiste na técnica de se fazer passar por outro computador da rede para conseguir acesso a um sistema.

Geralmente, o usuário não tem a percepção de que a página acessada é falsificada, tamanha é a similaridade com a página original. Com a técnica denominada de *IP spoofing*, os *crackers* direcionam todos os acessos a um determinado *site*, cópia da página original, fazendo a interação com a vítima como se fosse a página verdadeira. Com o *IP spoofing*, o agente é capaz de capturar o número do cartão de crédito de várias vítimas que, levadas a erro, pensavam estar inserindo informações em um site verdadeiro, ao fazerem compras *on-line*[19].

f) *Denial of Service* – Negação de serviço – Sabotagem eletrônica

Plantullo (2003) afirma que o usuário tem os *sites* paralisados com o acesso indevido e contínuo pelo agente, o que torna o fluxo do servidor incompatível com o número de acesso, utilizando-se o atacante apenas de um computador.

Além do *Denial of Service*, outra técnica conhecida é o *Distibuted Denial of Service*, que se diferencia do primeiro por se constituir como um conjunto de computadores utilizado para tirar de operação um ou mais serviços ou computadores conectados à rede (CERT.BR, 2025).

O objetivo é deixar o computador do usuário lento, uma vez que é gerada grande sobrecarga no processamento de dados, grande tráfego de dados para uma rede, com a ocupação de toda banda disponível, e impossibilitar o acesso dos usuários às caixas de correio no servidor de *e-mail* ou ao servidor *Web*.

g) Quebra de Senhas (*brute force*)

Método de se descobrir uma senha do sistema do usuário, testando várias vezes as palavras do dicionário, até encontrar a senha correta. Nesse caso, o atacante pode se valer de dois métodos: ataque de dicionário e da força bruta (Masini Neto, 2025).

19 Expressão utilizada para designar que se encontra ligada à rede *(net)* ou a outro computador.

O ataque de dicionário é feito tomando-se como ponto de partida nomes mais comuns mais "@", garimpando os termos mais comuns. Todavia, tanto as senhas quanto endereços de *e-mail* entre outros dados podem ser encontrados na internet: https://brasil.io/dataset/documentos-brasil/documents/.

O ataque à força bruta consiste em se fazer, na base da tentativa e do erro, por diversas vezes, as combinações de caracteres alfabéticos, numéricos e especiais[20]. Por essa razão, há *sites* especializados, como o https://joindeleteme.com/blog/opt-out-guides/, sugerindo dicas para a exclusão de dados na *Internet* (Jesus; Milagre, 2016).

h) *Vírus* e *Worms*

Os *vírus* se parecem com os *Worms*, que são programas ou conjunto de programas que têm como função a replicação e o reenvio à vítima para execução e ataque, enquanto os *worms* se caracterizam por consumir todos os recursos da máquina, tais como memória, *CPU* (Unidade Central de Processamento) e disco, inviabilizando seu uso produtivo. Daí o sentido do seu nome, vermes ou parasitas (Jesus; Milagre, 2016).

Os *vírus* são programas que infectam os arquivos de um computador, deixando-o vulnerável, e são propagáveis por meio de envio de arquivos, troca de *CDs*. Assim, pode-se dizer que

> Especialistas confirmam a possibilidade de ´sequestro ´de computadores por meio de *vírus* que permitem a um *hacker* controlar remotamente o computador ´sequestrado´, sem deixar sinais dessa operação. O *vírus* pode se instalar no computador quando o usuário, sem saber, faz o *dowload* de um programa infectado, através de um *website* de aparência amistosa (mas preparado intencionalmente pelo *hacker*) (Greco Filho, 2005, p. 55).

Um computador é infectado de várias maneiras, e isso acontece quando um programa dessa natureza é executado, por exemplo, com: abertura de arquivos anexados aos *e-mails* e arquivos e de editores de texto ou planilhas eletrônicas[21]; abertura de arquivos armazenados em outros computadores quando compartilhados nas redes; instalação de programas de procedência desconhecida, obtidos na *Internet*; e ainda com inserção de mídias (antigamente eram os disquetes e *pen drives*) removíveis que estejam infectadas no computador (CERT.BR, 2025, p.4).

i) *Phishing* – Envio de mensagens eletrônicas falsas

Phishing advém de "*fishing*", analogia criada pelos fraudadores para designar como sendo as "iscas" (*e-mails*). São usados para a coleta, "pesca", de senhas e dados financeiros de usuários da *Internet*.

Ocorre com o envio de mensagens eletrônicas falsas ao usuário, solicitando acesso a um *link*[22] que, por sua vez, dá acesso a um *site* falso que solicita dados pessoais da vítima, por exemplo, dados da conta bancária. Muitas vezes, o criminoso envia mensagens no aplicativo do MSN informando que a vítima possui milhares de pontos de companhia aérea a receber, mas que, para isso, deverá clicar em um *link* que, com certeza, recolherá dados da vítima, podendo ser lesada em sua conta bancária.

---

20 São exemplos de caracteres especiais: *@;%;&;$*.

21 Como exemplos: *Word* e *Excel*.

22 *Link* significa uma ligação, interconexão, enlace. Ou seja, parte de um subprograma que interage com o programa principal.

Exemplo real enviado por um atacante virtual de mensagem que a autora desta obra recomenda que em hipótese alguma seja acessada: "BB: Liberado! 197.742 mil pontos que acabam em 24h. Podendo trocar em saldo, descontos na fatura ou *cashbck*: link". Nesse caso, o criminoso usa de engenharia social para entrar em contato com a vítima e acessar dados bancários, que pode ser feita com o uso indiscriminado da Inteligência Artificial (IA).

Em comunicação a seus clientes, o SERASA, serviço centralizado de informações relacionadas aos dados dos consumidores, informa que não envia mensagens para notificação ou verificação de pendências financeiras cadastradas em seus bancos de dados. A página recomenda aos usuários que eventuais *e-mails* recebidos com esse tipo de mensagem sejam imediatamente excluídos, sem a abertura de arquivos anexados, e que o *link* oferecido não seja acessado, por se tratar de *scan* (*spam* fraudulento).

A tabela a seguir contém vários tipos de técnicas utilizadas e os textos das mensagens enviadas ao usuário. Entre as modalidades de fraudes, as mais utilizadas com frequência pelos estelionatários da rede são aquelas que buscam obter dados da vítima, tais como: senha do cartão de crédito e de contas bancárias, número da conta bancária e do CPF.

Tabela 1. Exemplos de temas de mensagens de *phishing*

Tema	Texto da mensagem
Cartões virtuais	UOL, *Voxcards*, Humor Tadela, O Carteiro, *Emotioncard*, Criança Esperança, AACD/Teleton.
SERASA e SPC	Débitos, restrições ou pendências financeiras.
Serviços de governo eletrônico	CPF/CNPJ pendente ou cancelado, Imposto de Renda (nova versão ou correção para o programa de declaração, consulta da restituição, dados incorretos ou incompletos na declaração), eleições (título eleitoral cancelado, simulação da urna eletrônica).
Álbuns de fotos	Pessoa supostamente conhecida, celebridades, relacionado a algum fato noticiado (em jornais, revistas, televisão), traição, nudez ou pornografia, serviço de acompanhantes.
Serviço de telefonia	Pendências de débito, aviso de bloqueio de serviços, detalhamento de fatura, créditos gratuitos para o celular.
Antivírus	A melhor opção do mercado, nova versão, atualização de vacinas, novas funcionalidades, eliminação de vírus do seu computador.
Notícias/boatos	Fatos amplamente noticiados (ataques terroristas, *tsunami*, terremotos), boatos envolvendo pessoas conhecidas (morte, acidentes ou outras situações chocantes).
Reality shows	*Big Brother* – fotos ou vídeos envolvendo cenas de nudez ou eróticas.
Programas ou arquivos diversos	Novas versões de *softwares*, correções para o sistema operacional Windows, músicas, vídeos, jogos, acesso gratuito a canais de TV a cabo no computador, cadastro ou atualização de currículos, recorra das multas de trânsito.
Pedidos	Orçamento, cotação de preços, lista de produtos.
Discadores	Para conexão *Internet* gratuita, para acessar imagens ou vídeos restritos.
Sites de comércio eletrônico	Atualização de cadastro, devolução de produtos, cobrança de débitos, confirmação de compra.
Convites	Convites para participação em *sites* de relacionamento (como o *Facebook, Instagran, Tinder*) e outros serviços gratuitos.
Dinheiro fácil	Descubra como ganhar dinheiro na *Internet*. Jogos on-line.
Promoções	Diversos.
Prêmios	Loterias, instituições financeiras, pontos em companhias aéreas ou programas como LIVELO.
Propaganda	Produtos, cursos, treinamentos, concursos.
FEBRABAN	Cartilha de segurança, avisos de fraude.
IBGE	Censo.
CORREIOS	A existência de mercadoria ou objeto apreendido pela Receita Federal na agência dos correios que precisa ser paga uma taxa imediata para liberação.

Fonte: elaborado pela Autora com base na obra de Wendt e Jorge (2021).

Todavia, além das técnicas já tratadas, outras existem, tais como: *hoaxes* na rede, que são boatos, notícias falsas espalhadas com o condão de propalar fatos inverídicos e que, geralmente, apontam como remetente uma instituição governamental, noticiando, por exemplo, que uma pessoa importante está acometida de uma doença e está preste a morrer. Ocupam muito espaço na caixa postal do usuário e podem conter nos e-mails diversas espécies de *vírus* (*malware)* (Jesus; Milagre, 2016).

Spywares são grandes categorias de softwares que têm o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Tem nas mãos dos atacantes uma poderosa ferramenta com o monitoramento dos hábitos do usuário durante a navegação na rede e podem direcionar as propagandas de produtos e de serviços (por exemplo, na venda do remédio Viagra), que pode capturar senhas bancárias e de cartões de crédito para uso malicioso (CERT.BR, 2025, p. 9-10).

Backdoors são programas que permitem ao atacante retornar ao computador invadido sem a utilização da técnica inicial, tal qual um *e-mail,* com a disponibilização de um novo serviço ou com a substituição do serviço com a versão alterada. Podem ser feitos com o uso do Cavalo de Troia, com a instalação de pacotes de *software* mal configurados ou utilizados sem o consentimento do usuário, tais como: o *BackOrifice* e *NetBus*, da plataforma *Windows* (CERT.BR, 2025, p. 11).

Keyloggers consiste em "técnica para monitorar tudo o que é digitado pela vítima" (Jesus, Milagre, 2016, p. 36) e são conhecidos também como códigos maliciosos, *malwares*. Os *malwares* são o gênero em que programas (espécies) são desenvolvidos de forma específica para executar ações lesivas no computador do usuário.

2.2. Segurança e criptografia

Em face das diversas espécies de técnicas usadas pelos usuários que fraudam a *Internet* e que a cada dia são modernizadas e renovadas com o uso da própria tecnologia, tem sentido a preocupação dos doutrinadores em sugerirem uma política de segurança na rede (Reis, 1996; Góis Júnior, 2001; Plantullo, 2003).

Jesus (2016, p. 166) define segurança na rede como "proteções ou medidas que objetivam livrar a informação de situações que possam causar danos". Ou seja, os itens de segurança podem ser exemplificados como senhas, cofres, portas e fechaduras administrativas, entre outras. Frente a essa preocupação, considera-se um sistema computacional seguro quando estão presentes três requisitos essenciais: confidencialidade, integridade e disponibilidade. Nesse sentido,

> A confidencialidade diz que a informação só está disponível para aqueles devidamente autorizados; a integridade diz que a informação não é destruída ou corrompida e o sistema tem um desempenho correto, e a disponibilidade diz que os serviços/recursos do sistema estão disponíveis sempre que forem necessários (CERT.BR, 2025).

A cartilha de segurança da *Internet*, disponível no site https://internetsegura.br/pdf/guia-internet-segura.pdf, informa que ocorre a violação da confidencialidade quando alguém obtém acesso não autorizado ao computador e lê as informações da declaração do Imposto de Renda da vítima; viola a

integridade com o acesso ao computador alterando os dados lá contidos, como a alteração dos dados do Imposto de Renda antes de serem enviados à Receita Federal e, ainda, com o recebimento de uma enorme sobrecarga de dados com a negação de serviços em que a pessoa fica impossibilitada de enviar (via *Internet*) a declaração do Imposto de Renda em tempo hábil à Receita Federal.

Como são variadas as modalidades de condutas maliciosas que podem acarretar prejuízos de grande monta para os usuários, o Comitê Gestor da *Internet* no Brasil (CGI) elaborou uma Cartilha de Segurança com recomendações de segurança que podem minimizar que usuários sejam presas fáceis dos atacantes digitais. O CGI aconselha ainda ao usuário da *Internet* que, caso desconfie de alguma irregularidade, notifique o incidente ao Comitê[23].

Além disso, a autenticidade das informações é um meio que garante a segurança na rede quando o emissor assina a própria mensagem. Ou seja, é a confirmação da identidade do usuário, de um dispositivo ou de outra entidade, permitindo o controle de acesso aos recursos de sistema computadorizado, segundo a ISO-IEC 27002.

A prevenção, portanto, consiste em ter alguns cuidados como medidas de segurança na utilização da *Internet*, algumas delas sugeridas na Cartilha, os quais são:

a) uso de senhas:

- utilização de uma boa senha[24] com, no mínimo, oito caracteres mesclados com letras, números e símbolos, que sejam fáceis de lembrar. Usualmente, com letras maiúsculas e minúsculas alternadas, o que dificulta sua tradução, por exemplo "*Ci2tapop*" ou "*cI2TApOP*";
- inserção de uma frase na senha, por exemplo: "batatinha quando nasce esparrama pelo chão" pode gerar a seguinte senha: "*!BqnsepC*"[25];
- mudança da senha periodicamente, a cada três ou quatro meses;
- certificação de que a senha não esteja sendo observada por alguém no momento de uso e o não fornecimento da senha para terceiros, sob nenhuma hipótese;
- utilização de computadores de terceiros para efetuar transações que necessitem da senha, como: *LAN houses*, *cybercafés, stands* de eventos, de amigos etc.;
- uso de serviços criptografados;
- elaboração de uma boa senha para o usuário de um computador que sirva como servidor em uma rede doméstica ou de serviço;
- armazenamento de senha salva em lugar seguro.

23 O *site* a que nos referimos é o seguinte: https://www.cert.br/docs/faq1.html. Acesso em: 20 abr. 2025.

24 Várias instituições bancárias implementaram a senha randômica, aquela composta de números, letras e símbolos. Para ter acesso ao extrato bancário em caixas eletrônicos, o cliente digita a senha numérica e, em seguida, a senha alfabética, que muda de lugar em cada operação bancária realizada.

25 Recomenda-se ao leitor que não use essa senha exemplificada aqui.

b) Privacidade no acesso das páginas da *Web* e no recebimento de *e-mails:*

- desabilitação do recebimento de *cookies*[26] ou utilização apenas mediante prévia e expressa autorização do usuário;
- aquisição de *softwares anti-spywares* que permitam controlar recebimento e envio de informações entre *browser*[27] e *sites* visitados;
- acesso a páginas da *web* que permitam o anonimato *(anonymizers)* do usuário;
- não fornecimento dos dados pessoais (senha, nome completo, endereço residencial e de números de documentos) para terceiros, salvo se tiver a certeza da idoneidade da instituição mantenedora do *site*;
- hábitos diários, tais como: a hora que sai de casa, informações sobre os familiares e amigos, sobre os *softwares* que utiliza, horários de tráfego pessoal, bancos em que mantém contas bancárias e dados sobre o computado não devem ser inseridos no computador;
- nas compras virtuais ter cautela em adquirir coisas que o preço não condizer com o valor de mercado;
- desconfiar de mensagens que tenham as palavras "URGENTE" e "CONFIDENCIAL", que servem para chamar a atenção do usuário;
- ter atenção no recebimento de *e-mails* que contenham arquivos anexados com extensões *".exe", ".zip" e ".scr"* e outros *".com", ".rar"* e *".dll"* e não executar a instalação de tais arquivos/programas;
- checar junto às instituições (vide tabela no item anterior) se é costume solicitar informações via *internet* antes de fornecer quaisquer tipos de dados.

c) Páginas de comércio eletrônico ou de *Internet Banking*:

- fazer transações com instituições confiáveis;
- certificar se o Banco ou instituição a ser acessada pelo usuário/cliente tenha conexão segura com o uso de *browser* e de criptografia no *site*;
- conferir se o *browser* a ser acessado corresponde ao *site* que se pretende acessar;
- manter a *webcam*[28] desligada ao acessar um *site* de comércio eletrônico ou *Internet Banking*;
- conferir extratos bancários e contas de cartões de créditos mensalmente; ter atenção com ataques de engenharia social.

---

26 *Cookies* são programas usados para rastrear e manter as preferências do usuário da *Internet*. O Comitê Gestor da *Internet* assevera que não é incomum que ao se acessar pela primeira vez em um *site* de música, por exemplo, verificar que as ofertas *de CDs* são compatíveis com o gosto musical do internauta sem que ele tenha feito previamente tal opção.

27 *Browser* é um *software* que permite ao internauta passear de uma página para outra na *WEB*, equivalendo-se ao navegador.

28 *Webcan* é um pequeno aparelho (filmadora) que, ligado ao computador, permite que as pessoas se vejam em uma conversa *on-line*.

d) Instalação de ferramentas potentes contra vírus

- instalar no computador programas *antivírus,* que podem ser adquiridos mediante pagamento ou gratuitamente, como o Avast Free Antivírus, AVG antivírus Free, Bitdfender antivírus, Avira Free Security, dentre outros;
- configurar o *antivírus* para detectar os arquivos obtidos pela *Internet*, instalados nos discos rígidos *(HDs)* e em dispositivos móveis como pen drives;
- desabilitar no programa leitor de *e-mails* a autoexecução de arquivos anexados às mensagens;
- ao elaborar documentos, utilizar formatos menos suscetíveis à propagação de *vírus* tais como: *RTF* e *PDF*.

e) Cavalos de Troia, *backdoors, keyloggers e spywares*:

- seguir as recomendações do item "*d*" que dizem respeito aos vírus;
- manter o sistema operacional e *softwares* atualizados;
- instalar um *firewall*[29] pessoal para evitar que uma vulnerabilidade existente seja explorada;
- utilizar ferramenta *anti-spywares;*
- verificar se o provedor de *Internet* utiliza programas de filtragem na rede (*software* de filtragem de *e-mails*);

Destaca-se que as medidas acima elencadas não exaurem outras que instituições comerciais, como os bancos, noticiam aos seus clientes e que devem ser adotadas no cotidiano virtual.

Uma das medidas de segurança mais importantes destaca o uso de criptografia. Reis (1997), ao citar Gustavo Kruel, afirma que a criptografia é uma solução, já que as informações que trafegam na rede perpassam por vários pontos dentro da *Internet*, o que facilita a interceptação pelos predadores virtuais. Nesses termos, ensina que

> A segurança então da transmissão de dados através da *Internet* pode ser qualificada em três pontos principais: *autenticação*, que garante que a informação tenha origem onde diz que tem, a *integridade dos dados*, que garante que o conteúdo da informação não tenha sido alterado no caminho, e a *segurança dos dados*, que garante que só o destinatário vai ler o conteúdo da informação. Os métodos de criptografia têm, como toda certeza, a capacidade de suprir este monte de garantias (Kruel *apud* Reis, 1997, p. 54).

Criptografia advém de *cripto* e de *grafo*, que significa "a arte de escrever em cifras ou em códigos. Ou o conjunto de técnicas que permitem criptografar escritas" (Holanda, 1986, p. 499).

29 *Firewalls* são sistemas de proteção em que o computador não se comunica diretamente com outros computadores externos, e sim, com um servidor denominado de *PROXI* que restringe o acesso fazendo uma triagem das conexões estabelecidas.

Conclui Gustavo Corrêa (2000, p. 78) que

> Os principais programas de criptografia funcionam por meio do princípio pelo qual documentos legíveis sejam transformados em um agrupamento de caracteres sem sentido, o mesmo utilizado pelo imperador romano Júlio César, só que de maneira bem mais completa. Tais programas trabalham com dois sistemas de codificação.

Para verificar se uma conexão é segura, podem ser visualizados pelo menos dois itens na janela do *browser*, que significa que as informações transmitidas estão sendo criptografadas entre o *browser* e o *site* (CERT.BR, 2025).

Assim, o *https* é o primeiro item que pode ser visualizado no local em que o endereço do *site* é digitado. O "s" inserido antes dos dois pontos significa que o endereço tem uma conexão segura e, logo, as mensagens serão criptografadas antes do envio (CERT.BR, 2025).

Para garantia da segurança das informações, o HTTPS utiliza uma combinação de criptografia simétrica e criptografia de chave pública, ou assimétrica. Portanto, apesar da criptografia ser um meio de se ter mais segurança na *Internet*, não é o único, como também não está isento de ser fraudado na rede.

3. OS SUJEITOS ENVOLVIDOS NA PAREDE DIGITAL

São intermináveis os benefícios trazidos pelo advento da tecnologia, em especial, da *Internet.* Com a superestrada da informação, a *Internet*, alcançou-se uma intersimultaneidade de informações em todo o planeta em tempo real, algo que jamais foi visto na história.

Perfilar esse novo sujeito andarilho da rede é papel da criminologia, porque a criminologia estuda, ou tem como objeto, a análise das condutas antissociais ou culturalmente desviadas (Alves, 1986).

O objeto da criminologia é a relação existente entre delito, delinquente, vítima e controle social. Assim, existe uma relação entre o criminoso e a vítima muito próxima, mesmo estando em lugares diversos, como se demonstrará adiante (Shecaira, 2004).

A *Internet* tem uma facilidade de romper barreiras e difundir informações em tempo real a várias pessoas simultaneamente e em vários lugares do planeta. A análise que se pretende fazer, neste tópico, é direcionada ao comportamento dos sujeitos que estão envolvidos no crime, ou seja, o criminoso e a vítima.

Quanto à vítima, ela tem um papel importante nesse contexto, uma vez que o criminoso pode depender dela para agir. Ao ser examinado o comportamento de ambos os sujeitos na *Internet*, tratou-se da segurança na rede e de algumas medidas que podem ser adotadas para minimizar os danos, principalmente em relação aos clientes de bancos que sejam usuários de movimentações bancárias na *Internet*, ao consultar suas contas com uso de senhas e outras transações que põem em risco o internauta.

Sobre esse tema, serão abordados nos próximos tópicos: ações e comportamento dos sujeitos envolvidos nos crimes praticados na *Internet.*

3.1. Os atacantes digitais

Os atacantes virtuais que atuam na *Internet* têm o propósito de ostentar a inteligência, demonstrar habilidade para conduzir e/ou desviar informações movidos pela competição na rede como prova de força na atuação digital, configurando como um novo meio de autoafirmação juvenil (Amorim, 2004).

Outro fato que merece ser considerado é a impunidade pela qual são compelidos ao movimentarem dados de terceiros, muitas vezes por puro divertimento. O meio digital é considerado um submundo marginal em que a ilegalidade impera, trazendo uma sensação de que o criminoso não está sendo vigiado, ao ter instalado em sua residência o instrumento (computador e periféricos) utilizado para a prática do delito (Peck, 2002; Ribeiro, 2019).

Ao invés de correr riscos, andar armado, por exemplo, para praticar quaisquer condutas ilícitas, é mais cômodo ficar isolado em um ambiente que muitos imaginam que está fora do alcance de investigação policial.

Interessante explicação desse novo mundo a ser descoberto:

> Os piratas já não têm um tampão no olho nem um gancho no lugar da mão. Tampouco existem os barcos e os tesouros escondidos no fundo do mar. Chegando ao ano 2000, os piratas se apresentam com um cérebro desenvolvido, curioso e com pouquíssimas armas: um computador e uma linha telefônica. *Hackers*. (...) Proveniente de *'hack'*, som produzido pelos técnicos das empresas telefônicas ao golpear os aparelhos para que funcionem. Hoje é uma palavra temida por empresários, legisladores e autoridade que desejam controlar aqueles que se divertem decifrando chaves para entrar em lugares proibidos e ter acesso a informação não autorizada (Merlat *apud* Mustaro, 2003, p. 22).

Entretanto, os autores discutem sobre o controle da internet. Silveira (2010) explica que o controle tem lado positivo e negativo, levando-se em conta que um dos princípios que regem a internet é o da liberdade na rede. Por outro lado, o autor pondera sobre a importância de se ter clareza dos instrumentos de controle, a exemplo das regras que os internautas se subordinam por meio dos protocolos TCP/IP e *Domain Name System* (DNS), o que, em muitos casos, não são suficientes para impedir ações nefastas na rede.

No ambiente virtual, surgem outras condutas, de pessoas antes desconhecidas, como os *Hackers* e *Crakers.* A denominação *hacker* surgiu em Massachusetts, nos Estados Unidos, para designar os alunos de computação que pesquisavam em laboratório, passando noites em claro. Os quais são classificados em duas espécies de *hacker,* sendo o *hacker* ético e o não ético, mais conhecido como *cracker* (Silva, 2003).

Hackers éticos são aqueles que "invadem sistemas, corrigem falhas de segurança e instalam uma porta única e controlada, com o propósito de garantir a exclusividade no acesso" (Paesani, 2001, p. 45). Ou seja, são pessoas que detêm conhecimento de programas e sistemas de computadores, diferenciando-se do usuário comum, que utiliza a *Internet* com fins específicos e conhecimento reduzido, muitas vezes, ao mínimo necessário.

Assim, pode-se conceituar *hacker* como

> [...] pessoa interessada em testar e recondicionar qualquer tipo de sistema operacional. Muitos deles são programadores e possuem alto grau de conhecimento em sistemas operacionais em linguagem de programação. Eles descobrem falhas nos sistemas, bem como as razões que foram detectadas. *Hackers* procuram por conhecimento, compartilham gratuitamente o que descobrem e não tem por objeto a destruição dos sistemas ou arquivos (Gomes, 2000, p. 27).

Ao contrário dos *hackers,* o *cracker* é "o invasor destrutivo que tenta invadir furtinosamente, portões de entrada dos servidores *Internet,* que são a melhor forma de disseminar informações" (Paesani, 2001, p. 45). A denominação *hacker,* segundo este autor, não deve ser usada para identificar indivíduos que danificam sistemas ou que utilizam seus conhecimentos de forma danosa. Esses são os *crackers*, que, apesar de possuírem as mesmas habilidades dos *hackers*, podem ser diferenciados pela intenção e pela ação: danificar sistemas, roubar, alterar e apagar dados.

São as condutas praticadas pelos *crackers* que interessam neste estudo, tendo em vista que são pessoas que trabalham em programas de computador capazes de invadir *sites* de empresas, estabelecimentos comerciais e instituições governamentais possuidoras de valiosas informações.

Cracker pode ser definido como

> [...] indivíduo que se vale de seu conhecimento para comprometer a segurança na rede. Muitos deles possuem alto grau de conhecimento de linguagem de programação e sistemas operacionais. Suas atividades incluem acesso não autorizado, danificação de todo e qualquer sistema de espionagem, etc. Geralmente, tais atividades são tidas como ilegais e estão sujeitos às sanções previstas em lei (Plantullo, 2003, p. 80).

No Brasil, os *hackers* foram percebidos em 1988, quando as vias de controle estatais tomaram conhecimento de ataques a sistemas bancários e órgãos públicos. Em 1988, os computadores da Universidade de São Paulo (USP), da Universidade de Campinas (UNICAMP) e da Empresa Brasileira de Pesquisa Agropecuária (EMBRAPA) foram invadidos, provocando pane nos equipamentos (Silva, 2003).

O criminoso da *Internet* pode ser classificado em várias espécies, como: os *hackers*, os *crackers*, os *phreackers,* os *warez* e os *cyberpunks*. Vejamos cada um deles.

Os *phreackers* são os piratas do *software,* que fazem ligações internacionais sem pagamento, causando enormes prejuízos a empresas de telecomunicações. Têm a capacidade de burlar tarifas telefônicas, reprogramar centrais telefônicas, instalar escutas, clonar celulares, entre outros (Góis Júnior, 2002).

Os *warez* são pessoas que pertencem aos grupos que atuam em segredo e que se comunicam com códigos e sinais de reconhecimento. A atuação ilícita do *warez* consiste em copiar *softwares* caros e distribuí-los gratuitamente (Góis Júnior, 2002; Plantullo, 2003).

Os *cyberpunks* são os mais perigosos e menos acessíveis, porque são capacitados para quebrar senhas complicadas, interceptar mensagens e são especialistas em criptografia. Na verdade, são subespécies dos *crackers*, com uma atuação bem definida (Aras, 2001).

Os *lammers* ou *script kidders* são pessoas que tentam se tornar *hackers.* São internautas iniciantes que detêm pouco conhecimento na rede (Rosa, 2002; Jesus; Milagre, 2016). Diferentemente dos *newbies*, que são humildes, novatos no ramo e taxados de ingênuos, porque fazem perguntas na rede que não deveriam.

Os *wannabes* são principiantes que aprenderam a usar programas prontos dos *hackers*, e os *arackers* são denominados de *hackers* falsos porque pensam que detêm o conhecimento das técnicas utilizadas por eles. No entanto, o que fazem é acessar revistas pornográficas virtuais durante as madrugadas (Rosa, 2002; Plantullo, 2003).

Além desses, a doutrina ainda classifica outras categorias, como os gurus e larvas. Os gurus ou *wizards* são aqueles que "possuem habilidades técnicas em todos os segmentos" (Plantullo, 2003, p. 79); e os larvas são pessoas que estão entre a categoria dos *wannabes e hackers* e atacam sistemas de segurança média; e os *carders* são pessoas especializadas em fraudar cartões na internet (Jesus; Milagre, 2016).

De todo modo, os atacantes digitais costumam praticar ilícitos porque aproveitam vulnerabilidades, inexperiência e desconhecimento dos usuários. A fragilidade de quem está do outro lado da tela do

computador ou em outro meio como o aparelho celular, usando a internet sem as devidas precauções, facilita a ação criminosa.

3.2. A vítima virtual

Após traçar o perfil do atacante da *Internet*, passa-se a considerar a vítima virtual. Vários são os autores que fazem um estudo da vítima, de forma a classificá-la em diversas modalidades, entre elas, citam-se as classificações de Von Hering, de Mendelsohn, de Fattah, de Guglielmo Gulotta, de Elias Neuman, que considera original a feita por Ellenberger (Oliveira, 1999).

As vítimas dos crimes cometidos na *Internet* que facilitam a prática do delito em geral são analfabetas digitais. Explicando melhor, o usuário, aqui chamado de vítima, ao preencher campos ou mapas digitais na *Internet* e inserir dados pessoais, dá margem às ações dos predadores digitais.

Os chamados *chats*[30], *flogs*[31], grupos de discussão e redes sociais, como o *WhatsApp*, de envio e recebimento de mensagens eletrônicas e outras estruturas da *web* são um poderoso espaço de conhecimento de inúmeras pessoas à distância. Nesse ambiente, as pessoas se conhecem, e a comunicação entre elas, na maioria das vezes, é descompromissada e aleatória.

Ao que tudo indica, a ausência física e o desconhecimento do outro levam as vítimas a se tornarem presas fáceis ante a naturalidade com que relatam dados pessoais. Sem contar que é farta a inserção de imagens de vítimas originadas de fotografias ou filmagens (Ribeiro, 2019).

Isso pode ser explicado pelo motivo de que

> Tal fato ocorre por consequência do escudo protetor erigido pela tela do computador. Isto é dizer que a sensação de invisibilidade decorrente do referido escudo protetor projeta-se por sobre as reais sensações de determinados usuários, e estes têm a sensação de não poderem ser observados por outros usuários ou atores da *Internet*. Realmente não podem ser visivelmente encontrados, mas podem ser rastreados (Drummond, 2003, p. 23).

A proliferação de dados e imagens como fotografias de conteúdo pornográfico na *Internet* causa um resultado devastador na vida da vítima. O resultado é consequência da velocidade de comunicação e proliferação quase que instantânea da informação virtual (Drummond, 2003).

Essa espécie de vítima é encontrada na classificação feita por Hans Von Henting (*apud* Oliveira, 1999) como espécie de vítima isolada, que não se integra na comunidade, e por isso se expõe ao perigo. Jean Pinatel (*apud* Oliveira, 1999), autor francês, intitula como a vítima facilitadora aquela que desperta no criminoso a oportunidade de agir, exemplificando com condutas dos crimes de extorsão e estelionato.

Por outro lado, as vítimas virtuais, analfabetas digitais, não têm o mínimo conhecimento do risco que correm ao navegarem na rede. A aldeia global, como é chamada pela mídia, constitui-se de milhões de pessoas de toda natureza, conectadas em tempo real. É o que explica Ribeiro (2019, p. 79), ao afirmar que

30 *Chats* são salas de bate papo na *Internet*.

31 *Flogs* são páginas pessoais construídas com inserção de imagens.

> A atuação e a comunicação dos jovens nas redes sociais e a relação com os riscos e os danos que a Internet pode trazer é importante se destacado porque apesar de, muitas vezes, os jovens entenderem que são autossuficientes em redes sociais essa premissa pode ser falsa. Dessa forma, o perigo deles serem capturados por pessoas que gastam o tempo vasculhando as redes sociais é o indício que os agressores conseguem identificar quem tem o perfil vulnerável e suscetível para cair em armadilhas virtuais. Após o usuário da web ter se exposto em redes sociais sem tomar as precauções necessárias, há a probabilidade de ter os dados e/ou imagens copiadas, replicadas e compartilhadas a um número indefinido de pessoas.

Sem mencionar que, além dos riscos, é ainda mais hipossuficiente quem se encontra na condição de analfabeto digital. Veja-se:

> Com a *Internet*, especialmente com *World Wide Web*, a sociedade cibernética, caracterizada pela difusão da informação por sistemas de telemática, passa a ser composta por uma elite, a daqueles plugados na rede, os *on-line*, que têm acesso ao conhecimento em qualquer parte e podem interagir com o mundo em tempo real. Navegam as ondas virtuais do mundo novo, etéreo, mas concreto, que surgiu com a Internet. Do outro lado, ou fora dessa sociedade, como marginalizados do mundo *hitech*, estão os desplugados, ou povo *off-line*, grupo muito mais numeroso que não tem computadores, não tem linhas telefônicas e às vezes nem mesmo é alfabetizado. Muitos brasileiros são analfabetos em português e serão também analfabetos tecnólogos no século XXI. Não navegam. Não interagem. São náufragos do futuro (Aras, 2001, p. 1122).

Como já foi explicitado, no espaço digital, há criminosos de alta periculosidade. No entanto, como não são perceptíveis, fica muito mais fácil pinçar uma vítima considerada analfabeta digital. Embora o Brasil seja uma "nação digital", com mais de 120 milhões de pessoas com acesso à web, essa conexão é marcadamente desigual. Dados recentes apontam para um panorama preocupante de baixas habilidades digitais: apenas 24% dos brasileiros possuem habilidades digitais básicas (ANATEL, 2023). Uma pesquisa de 2025 do Indicador de Alfabetismo Funcional (INAF) mostra que só um em cada quatro brasileiros (23%) de 15 a 64 anos tem altas habilidades digitais. A maioria, 53%, está no nível médio, e 25% no nível baixo, conseguindo realizar apenas um número limitado de tarefas no contexto digital (ANATEL, 2023).

Apesar do avanço na conectividade, milhões de brasileiros ainda não têm acesso à internet ou o têm de forma precária. O IBGE (2023) aponta que cerca de 5,9 milhões de domicílios ainda não possuem acesso à internet.

Mesmo entre os analfabetos funcionais (aqueles que, embora saibam assinar o nome, não têm instruções básicas para ler e escrever), a pesquisa do INAF, de 2025, revela que apenas 3% têm nível alto de habilidades digitais. Isso indica uma "dupla exclusão" para esses indivíduos (INAF, 2025). O acesso e a qualidade da internet, bem como a apreensão do conteúdo digital, ainda dependem fortemente de questões regionais, econômicas e sociais. Grandes centros podem ter infraestrutura avançada, enquanto áreas rurais e periféricas enfrentam limitações severas de conectividade.

O Brasil tem um baixo desempenho em *rankings* de alfabetização digital, como o "The Inclusive Internet", de 2021, ocupando a 80ª posição entre 120 países, o que afeta diretamente o desenvolvimento profissional e a competitividade do País. Por outro lado, o Brasil ocupa hoje a segunda posição no *ranking* mundial de ataques digitais, com mais de 700 milhões de tentativas registradas em apenas um ano, segundo o "Panorama de Ameaças para a América Latina 2024", realizado pela Kaspersky (UOL, *online*, 2025). Apesar de parecer um problema distante, os números mostram que a ameaça é real. Um levantamento do Instituto DataSenado revelou que 24% dos brasileiros com mais de 16 anos já foram vítimas de algum tipo de golpe online: isso equivale a mais de 40 milhões de pessoas (Senado Federal, 2025).

Portanto, apresentar as características que Wihelm traz (*apud* Oliveira, 1999), são próximas do perfil das vítimas analfabetas digitais que têm dificuldade em navegar na rede.

A vítima classificada como primária consiste em determinada pessoa que sofre diretamente o delito; em secundária, consiste em ser vítima um grupo específico ou de parte da comunidade, como exemplificados os crimes praticados contra uma instituição bancária, em que são vários os correntistas lesados; vítima terciária consiste na vitimização difusa, em que não se sabe com exatidão o número de lesados; vítima mútua é aquela em que ambos os integrantes da relação criminosa podem ser ao mesmo tempo autor e vítima, como ocorria em crimes de adultério ocorridos por intermédio da *Internet*, antes da revogação do art. 240 do Código Penal Brasileiro, pela Lei nº 11.106/2005; vítima em crime sem vítima é a que a vítima é cliente do autor do ilícito, como se exemplifica com crimes de agiotagem virtual (Torsten Sellin; Marvin Wolfgang *apud* Oliveira 2005).

A vítima também pode ser classificada em programadora, precipitadora, de caso fortuito e de força maior. Nessa classificação, fica mais visível a presença das condutas dos criminosos e das vítimas no ambiente cibernético (Oliveira, 2005).

A vítima precipitadora é aquela que colabora com a ação do autor, subdividindo-se em vítima de culpa exclusiva, vítima concorrente e vítima de culpa recíproca. A vítima de culpa exclusiva impede a configuração do nexo causal em que se justifica a conduta do autor da infração, resultando em sentença penal absolutória.

A vítima concorrente interfere eventualmente na conduta do criminoso, como, por exemplo, caixa de banco que efetua pagamento de cheque falsificado. Ao passo que a vítima recíproca não age com cautela, assumindo de forma tácita a responsabilidade do resultado, facilitando a conduta do delinquente.

É interessante observar que muitos crimes virtuais não são noticiados à autoridade policial. Instituições financeiras, ao terem seus bancos de dados atacados em face das reclamações de correntistas, por vezes, preferem manter em sigilo a conduta dos *crackers*, com a reparação dos danos materiais e o estudo de implementação de medidas preventivas[32].

32 Superior Tribunal de Justiça (STJ), a Súmula 479, definiu que "as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias".

Outras condutas não são rastreadas pela dificuldade de se encontrar as vítimas. Não se sabe exatamente quem são, quantas são, onde estão ou estiveram e quando foram lesadas. Portanto, resta como política criminal, no meio virtual, medidas de ordem preventivas como o melhor meio de não se tornar uma vítima.

3.3. A prova no processo penal

Segundo Silva (1987, p. 491), a palavra prova é derivada do "latim *proba*, de *probare,* significa demonstrar, reconhecer, formar juízo a respeito de alguma coisa". No sentido jurídico, essa demonstração é feita por intermédio dos meios legais em direito admitidos, com o objetivo de confirmar a existência ou veracidade de um fato material ou de um ato jurídico, para que os sujeitos processuais envolvidos possam ter fundamento para defender ou acusar alguém de ter ou não praticado um crime (Silva, 1989).

Quanto ao ônus da prova, "a palavra ônus tem origem latina (*onus*), significando fardo, carga, peso, imposição etc. Daí por que ônus da prova (*onus probandi*) representa a necessidade de provar para ver reconhecida judicialmente a pretensão manifestada (Aranha, 2006, p. 7).

No direito processual penal, é preciso estar atento a um dos institutos mais importantes para o processo e para quem está sendo processado, o acusado. O julgador deve, antes de proferir a decisão, ter ciência das provas produzidas no decorrer da instrução processual. Assim,

> Provar significa, substancialmente, induzir o juiz ao convencimento de que o fato histórico aconteceu de um determinado modo. O fato histórico deve ser `representado` ao juiz por meio de outros fatos. A prova é, nesse sentido, o procedimento lógico por meio do qual a partir de um fato conhecido deduz-se a existência do fato histórico a ser provado e suas circunstâncias (Tonini, 2002, p. 49).

Nas lições do mestre Carnelutti (2005, p. 17), "as provas são, pois, os objetos mediante os quais o juiz obtém as experiências que lhe servem para julgar". Por sua vez, Mittermaier (2004, p. 74) assevera que

> Todas as vezes que um indivíduo aparece como autor de um fato, que é, por força de lei, de consequências aflitivas, e que se trata de lhe fazer a aplicação devida, a condenação repousa sobre a certeza dos fatos, sobre a convicção que se gera na consciência do juiz. A soma dos motivos geradores dessa certeza chama-se prova.

Malatesta (2004, p. 87) explica a acepção de prova como "a relação concreta entre a verdade e o espírito humano nas suas especiais determinações de credibilidade, probabilidade e certeza". Todavia, Lopes Júnior (2016) diferencia os meios de prova dos meios de obtenção da prova. Os meios de prova são aqueles que o magistrado utiliza dos resultados probatórios, a exemplo do interrogatório e da prova pericial como fundamentos na decisão. Ao contrário dos meios de obtenção da prova, que funcionam como caminhos para se ter a prova, a exemplo da delação premiada e interceptação telefônica.

A Carta da República prevê no art. 5º, inciso LVI, a produzibilidade no processo, das provas lícitas, excluindo da apreciação do magistrado aquelas provas derivadas de atos ilícitos ou que sejam ilícitas

O Código de Processo Penal, Decreto-Lei n. 3.689, de 3 de outubro de 1941, destinou noventa e cinco artigos para a realização e produção de prova, iniciando no artigo 155 e findando no artigo 250. Entretanto, esses dispositivos legais não excluem outros meios de prova, que podem ser encontrados no inciso VII do art. 6º do CPP ao tratar da perícia realizada no inquérito policial e a delação premiada prevista no art. 13 da Lei nº 9.807/1990 (Brasil, 2016).

Vige no processo penal brasileiro o princípio da liberdade da prova, desde que tenham pertinência à convicção do juiz (Lopes Jr, 2016; Rangel, 2015; Marcão, 2020). Em regra, todos os fatos devem ser provados, com a ressalva de intuitivos ou evidentes, presunções legais, fatos inúteis e notórios. Fatos intuitivos ou evidentes, também chamados axiomáticos, são aqueles que são evidentes por si mesmos. Por exemplo, o caso de um álibi, ao comprovar que o acusado estava em local diverso de onde ocorreu o fato, excluindo-se a necessidade de demonstrar que ele não estava no local do crime (Mirabete, 2025).

Presunções legais, ou fatos presumidos, são aqueles que não precisam ser comprovados por sua ocorrência ser natural. Ou seja, seu conhecimento decorre da ordem natural das coisas ou de previsão legal, dividindo-se em presunções legais absolutas (*juris et de jure*) ou relativas (*juris tantum*). As presunções legais absolutas não admitem prova em contrário (por exemplo, demonstrar que o acusado menor de dezoito anos não tinha, ao tempo do fato, capacidade de entendimento do ilícito). Já as presunções legais relativas são aquelas em que pode ser afastada quando existe prova que a contradiz, como o art. 224 do Código Penal, que prevê a existência de violência presumida em determinados crimes contra os costumes (Mirabete, 2025).

Fatos inúteis, por sua vez, são aqueles em que não se encontra nenhuma relevância processual, e notórios são os fatos de verdade sabida, que não precisam ser provados. Nesse caso, aplica-se o princípio do *notorium non eget probatione* (o notório não necessita de prova), em que todos sabem do fato por fazer parte da cultura do meio social, como, por exemplo, a comemoração natalina no Brasil, que é realizada no dia 25 de dezembro (Pacelli, 2015).

Para melhor compreensão do tema, faz-se necessário discorrer sobre fontes e meios de prova, o que se fará no restante deste capítulo.

3.4. As fontes, os meios de prova e algumas classificações de prova

Fontes de prova são "tudo que se pode ministrar de indicações úteis que necessitam de comprovação" (Tourinho Filho, 2002, p. 219). Apesar de o instituto ser parecido com os meios de prova, com ele não se confunde. Enquanto a fonte de prova é o próprio fato ou circunstância que se pretende provar, o meio de prova é a forma como as provas são inseridas no corpo do processo. Nesse diapasão, pode-se dizer que "meio de prova é o instrumento processual que permite a aquisição de um elemento de prova" (Tonini, 2002, p. 108).

Assim, as fontes se equivalem ao objeto da prova, e os meios às formas da prova (Aranha, 2006; Mirabete, 2025). Vislumbra-se, ainda, o posicionamento de que "o objeto da prova é o fato cuja existência deseja-se ver reconhecida" e a prova quanto "*à forma pode ser testemunhal, documental* e material" (Aranha, 2006, p. 24-25).

Por sua vez, o Código de Processo Penal admite vários meios de prova, uma vez que prevalece no sistema processual o princípio da verdade real. Esse princípio permite aos sujeitos processuais – acusação e defesa – ampla liberdade na produção das provas.

Mirabete (2025) assevera que essa liberdade é explicada em face da função preventiva e repressiva do delito. Nesse diapasão, a limitação da liberdade da prova prejudicaria a obtenção da verdade e a consequente aplicação correta e justa da lei. Portanto, é bem amplo o campo da investigação da verdade material tanto na fase procedimental (investigação) quanto na processual (instrução). (Marques, 2003, p. 351). Marques (2003, p. 352) explica que,

> Em juízo, por outro lado, não há restrições na exploração das fontes e meios de provas, como se deduz, a *contrário sensu*, do que preceitua o art. 155 do Código de Processo Penal. Qualquer diligência probatória, que possa esclarecer a verdade, é admissível no juízo penal e na fase preparatória da investigação levada a efeito pela Polícia Judiciária.

Todavia, o princípio da verdade real, da verdade material ou da verdade substancial não pode mais ser visto como absoluto, tendo em vista o sistema constitucional vigente.

É inadmissível, na justiça penal, a adoção do princípio de que os fins justifiquem os meios na tentativa de se fazer legítima a busca da verdade por intermédio de qualquer fonte probante. A tortura e todas as formas de violência física que ofendam a integridade corporal, a captação clandestina de telefonemas, o emprego de microfones dissimulados e o registro em aparelhos eletrônicos, de conversas íntimas, o emprego da hipnose e da narcoanálise[33] como meio de se obter a confissão de uma pessoa suspeita, o emprego do *lie-detector (*aparelho que é colocado no corpo do acusado para medir a pressão sanguínea, a respiração e os movimentos do pulso, mais conhecido como detector de mentiras*)* são limitações à investigação e à prova, ou seja, restrições decorrentes dos princípios constitucionais de proteção e garantia da pessoa humana (Marques, 2003).

Sob o ponto de vista principiológico, verifica-se que o magistrado tende a ficar próximo ao fato, mas é quase impossível reconstituí-lo na sua completude (Barros, 2002). Complementa Ferrajoli (2010) que o rito e o método legal de formação de provas configuram garantia processual apta a satisfazer o controle de todas as outras garantias no desenvolvimento das atividades judiciárias, principalmente as probatórias, segundo as formas e os procedimentos previstos em lei. Dito de outro modo, é dar ao acusado e à vítima a clareza de quais são os meios de provas lícitos e como serão produzidos durante a instrução processual.

Daí a necessidade de a coleta das provas estar em consonância com a Constituição da República, uma vez que o princípio da verdade real é excepcionado em vários pontos, como, por exemplo, no art. 5º, inciso LVI, ao vedar que se aceite no processo penal provas de origem ilícita.

Apesar de o Código de Processo Penal dispor sobre várias modalidades de provas, é apenas um rol exemplificativo, admitindo-se outras diversas daquelas dispostas na lei em vigor. Nem poderia ser

33 Narcoanálise consiste em um processo de investigação psicanalítica com a inserção de narcótico euforizante no organismo do paciente, que provoca a supressão do controle, com a evocação do passado, de experiências e conflitos (Ferreira, 1986, p. 1180).

diferente, se o sistema acusatório permite a liberdade das provas, não havendo ditame constitucional de forma contrária, as provas previstas na legislação ordinária não têm o condão de exaurir as espécies previstas.

Melhor explicando, as provas previstas na legislação processual penal são legais e podem ser largamente utilizadas tanto pela acusação quanto pela defesa, nos limites constitucionais, sem olvidar de outras modalidades de provas não constantes na legislação ordinária, desde que compatíveis com o sistema processual constitucional.

As provas admissíveis no Código de Processo Penal são: exame de corpo de delito e outras perícias (arts. 158-184); interrogatório do acusado (arts. 185-196); confissão do autor do fato (arts. 197-200); declarações do ofendido (art.201); depoimento das testemunhas (arts. 202-225); reconhecimento de pessoas e de coisas (arts. 226-228); realização de acareação (arts. 229-230); juntada de documentos (arts. 231-238); indícios (art. 239); e busca e apreensão de coisas e pessoas (arts. 240-250) (Brasil, 1940).

Contudo, com a difusão de documentos produzidos na internet, surgiram outras formas de provas que podem ser admitidas, como, por exemplo: ata notarial que descreva mensagens trocadas no *WhatsApp*; mensagens e/ou conteúdos obtidos em redes sociais como *Facebook*, *Instagram*, *Telegram* e outros; transcrição de áudios obtidos na internet e/ou reprodução de vídeos; provas de geolocalização; prova de existências de sites, dentre outras (Azevedo e Souza; Munhoz; Carvalho, 2024).

No tocante às espécies das provas, os autores não são unânimes em fazer uma classificação. Para Carnelutti (2005, p. 32), "as provas podem ser classificadas em provas históricas, críticas, pessoais e reais". Segundo o mesmo autor, as provas históricas seriam aquelas em que a prova consiste em um fato representativo de outro fato. Ou seja, representado por uma experiência do fato, como, por exemplo, o documento em que se faz uma representação do fato na ausência do destinatário e na presença do fato representado (documento) e na presença do destinatário e na ausência do fato representado (testemunha).

As provas críticas indicam a direção que uma coisa imprime ao pensamento que faz de outra coisa e fundamentam a natureza do fato naquilo que a prova consiste, subdividindo-se em contrassenhas e indícios. As contrassenhas não são muito difundidas pela doutrina corrente e significam "uma senha que se põe sobre a coisa ou que de alguma maneira vai unida à coisa" (Carnelutti, 2005, p. 54).

Como exemplo de contrassenha, o autor cita o nome para se identificar uma pessoa. Isto é, pelo nome, ou, se porventura tiver uma marca que o identifique, como uma cicatriz, uma tatuagem, ou um apelido, pode revelar ao juiz a identidade do acusado.

Já os indícios ou as presunções estão previstos no Código de Processo Penal, art. 239, aos quais Carnelutti (2005) denomina de provas críticas naturais que, comparadas a outros tipos de prova, apresentam uma heterogeneidade típica, podendo ser aplicadas a qualquer tipo de coisa ou fato.

As provas pessoais são aquelas em que se observa o comportamento do acusado enquanto presta seu depoimento (prova proporcionada pelo imputado) e ainda pela acareação e reconhecimento de terceiros (entre testemunhas). Já as provas reais relativas às coisas podem ser tanto reais históricas (do-

cumentos), quanto reais críticas (que compreendem os indícios e as contrassenhas) (Carnelutti, 2005).

Clássica é a classificação de Malatesta elogiada por Aranha (2004, p. 23), *verbis*:

> A respeito da classificação da prova encontramos na doutrina várias exposições, baseadas em critérios diferentes, todas elas excelentes não somente em razão de seu conteúdo científico como também pelo brilhantismo dos autores. Numa linha de frente merecem citações as classificações de Carnelutti, Benthan, João Monteiro, Neves e Castro, Moraes Carvalho, Melo Freire, Lobão, Ribas, Ramalho, etc. Porém, entre todas as classificações existentes, induvidosamente merece um destaque todo especial a formulada por Framarino Malatesta [...].

Na visão de Malatesta (2004), a prova pode ser classificada quanto ao objeto ou conteúdo, quanto ao sujeito e quanto à forma.

Quanto ao objeto ou conteúdo, divide-se em direta ou indireta. A prova direta se refere diretamente ao fato *probando*, como, por exemplo, depoimento de uma testemunha que afirma ter visto o acusado matar a vítima. A prova indireta se refere aos indícios e às presunções (Aranha, 2006). Quanto ao sujeito, divide-se em duas classes, sendo "prova pessoal ou verificação de pessoa e prova real ou verificação de coisa" (Malatesta, 2004, p. 118). Quanto à forma, subdivide-se em "prova testemunhal, prova documental (escrituras) e prova material (exames)" (Malatesta, 2004, p. 119).

Outra classificação que não poderia ser excluída é a de Paulo Tonini (2002, p. 108), para quem o "meio de prova é o instrumento processual que permite a aquisição de um elemento de prova".

Tonini (2002), fazendo menção ao Código de Processo Penal italiano, classifica em sete os meios de prova típicos, porque estão regulamentados em lei. Exemplifica-os como sendo: testemunhal, oitiva das partes, acareações, reconhecimentos, reconstituições judiciais, perícia e prova documental.

Além das provas típicas, o Código de Processo Penal italiano permite outros tipos de prova em face do uso da liberdade de produção de provas. Essas provas seriam "[...] provas atípicas e só seriam permitidas quando tivessem idoneidade para a comprovação dos fatos e não causassem prejuízos à liberdade moral da pessoa" (Tonini, 2002, p. 108).

Essa atipicidade pode ser percebida sob três enfoques. O primeiro, de que a atipicidade da prova se refere ao resultado e não a sua produção, sendo também chamada de prova inominada. O segundo, de que a divergência é a forma da produção da prova. Ou seja, se o rol das provas não é taxativo, muito menos é o seu meio, que a eles se amolda. O terceiro enfoque é de que a prova atípica é a que tem como finalidade por intermédio de uma prova típica o resultado de um outro meio, ainda que típico. O autor faz referência ao uso frequente, em audiência, de maneira informal, do chamamento de uma testemunha para reconhecer a pessoa do acusado (Tonini, 2002).

Quanto aos meios de prova, é o "meio através do qual se oferece ao juiz meios de conhecimento, de formação da história do crime, cujos resultados probatórios podem ser utilizados diretamente na decisão. São exemplos de meios de prova: a prova testemunhal, os documentos, as perícias, etc." (Lopes Júnior, 2017, p. 352).

Nesse contexto, verifica-se que, no direito processual penal pátrio, os meios de provas são exemplificativos (ordinários), não contendo a lei processual brasileira um rol taxativo, motivo pelo qual são previstos outros meios de prova, desde que compatíveis com o sistema processual constitucional (extraordinários).

De forma genérica, pode-se afirmar que são inadmissíveis os meios de prova proibidos por lei e incompatíveis com o sistema processual penal vigente, e que os meios de prova previstos em lei são denominados de nominados, e os não previstos, como inominados (Marcão, 2020).

3.5. O princípio do *ônus probandi* no direito brasileiro

Ônus advêm "do latim ônus, que significa carga, peso, obrigação, o que se entende por todo encargo, dever, ou obrigação que pesa sobre uma coisa ou uma pessoa, em virtude do que está obrigada a respeitá-los ou cumpri-los" (Silva, 1989, p. 282).

Quanto ao ônus *probandi* reitera Silva (1989, p. 283) que

> É o ônus ou o encargo da prova, nas questões judiciais. Sem fugir, pois, ao sentido literal do vocábulo (ônus), exprime a locução: a obrigação de provar. Neste particular está certo e afirmado o princípio, de que a obrigação de provar cabe a quem alega ou diz: *onus probandi incumbit ei quit dicit*. E, daí, se gera o provérbio: *Actor probat actionem, reus exceptionem*.

No direito processual penal brasileiro, devido ao sistema acusatório em que está inserido, dada a atribuição constitucional ao órgão ministerial ser a acusação oficial, ressalvadas as hipóteses em que a vítima figura como acusadora, o ônus *probandi* cabe a quem alega, conforme reza o art. 129, inciso I, da Constituição Federal. Ou seja, em cumprimento ao princípio da presunção da inocência e do in *dubio por reo*, o ônus probatório cabe ao acusador (Marcão, 2020).

Enquanto cabe à acusação provar o alegado, à defesa é facultado o ônus de produzir a prova em seu favor. À acusação cabe demonstrar

> [...] a existência do fato penalmente ilícito; a autoria; a relação de causalidade; a culpa (dolo/presumido) e (*culpa strictu sensu*/deve ser provada). À defesa cabe demonstrar os fatos extintivos como a prescrição, decadência, pagamento posterior etc., e fatos impeditivos como a exclusão da vontade, exclusão da culpa e os fatos modificativos como a exclusão da antijuridicidade, causas supralegais (Aranha, 2006, p. 14).

Enquanto o direito à defesa constitui uma obrigação legal sob pena de nulidade, a produção da prova por parte da defesa constitui um ônus, uma faculdade que, não sendo utilizada, perde-se a oportunidade de produção da prova com a preclusão do direito correspondente.

O princípio do contraditório e da ampla defesa confere ao acusado a paridade de armas em relação à acusação. Tanto é ônus que o acusado não tem a obrigação de responder às perguntas que lhe forem formuladas em relação aos fatos, o que não acarreta prejuízo em seu desfavor. De outro modo, se o acusado preferir confessar, poderá receber a atenuante em caso de condenação criminal.

Além dos momentos processuais acima citados, caso o acusado queira, por exemplo, complementar sua versão na via judicial, a defesa poderá requerer um novo encontro à presença do magistrado.

Outro ponto que merece relevo é o álibi utilizado pela defesa, desde que haja conexão com a prova produzida e com os fatos que se pretendem provar em favor do acusado. Todavia, a produção de qualquer tipo de prova deve ser ponderada.

Portanto, a defesa tem a faculdade de apresentar as provas que melhor lhe aprouver, sopesando a conveniência de que cada caso possui peculiaridades específicas, ressalvadas as hipóteses que lhe cabe apresentar a prova para provar o alegado para a tão almejada absolvição. Essa hipótese pode ser realizada, inclusive, na revisão criminal, em que há necessidade de se propor a justificação prévia para judicializar as novas provas para que possam ter valor na apreciação.

3.6. Procedimento probatório

O procedimento da prova, ou probatório, "vem a ser a marcha dos atos processuais relativos à prova, na forma prevista pela lei, e de maneira coordenada e concatenada" (Aranha, 2006, p. 35).

Os doutrinadores não são uníssonos em dividir o procedimento probatório. Para Camargo Aranha e José Frederico Marques, o procedimento divide-se em propositura, admissão e execução da prova, enquanto Renato Marcão e Paulo Rangel asseveram que a divisão seja a proposição ou indicação, admissão, produção e valoração (Aranha, 2006; Marcão, 2020; Rangel, 2015).

A propositura diz respeito ao instante processual adequado em que a prova é produzida. Regra geral, é com a denúncia, ou queixa-crime, que se especificam as primeiras proposições de prova a serem produzidas em juízo com a indicação do rol de testemunhas, no art. 41 do Código de Processo Penal.

A admissão é feita pelo juiz que analisa as provas propostas pela acusação e defesa para serem ou não produzidas em juízo. É ainda "[...] conhecida como recepção, primeiro contato do juiz com as provas, momento em que o magistrado se manifesta sobre a admissibilidade" (Aranha, 2006, p. 38).

As provas requeridas pelas partes devem ser deferidas, sob pena de se constituir ofensa à ampla defesa (em caso de ser proposta pela defesa) e de acarretar a nulidade processual. Em caso de indeferimento, a decisão deve ser motivada, nos ditames do art. 93, inciso X, da Constituição Federal, como em hipóteses em que não são pertinentes, não são admissíveis e não se referirem a fatos intuitivos, resultantes de presunção legal, inúteis ou notórias (Aranha, 2006).

Na ação penal de iniciativa privada, em que cabe ao ofendido, ora querelante, oferecer a queixa crime, como nas infrações de propriedade imaterial, a exemplo de violação de programas de computador, a peça acusatória não pode ser rejeitada quando estiver instruída com o laudo pericial. Essa prova deve ser requerida, em procedimento prévio de ação cautelar de produção de provas ou de busca e apreensão, configurando como condição de admissibilidade da ação, conforme reza o art. 13 da Lei nº 9.609, de 19 de fevereiro de 1998[34]. Outras provas são produzidas antes do oferecimento da denúncia ou da queixa, como exemplo, ilícitos praticados por funcionários públicos, art. 513 do CPP.

34 A Ação penal e as diligências preliminares de busca e apreensão, nos casos de violação de direito de autor de programa de computador, serão precedidas de vistoria, podendo o juiz ordenar a apreensão das cópias produzidas ou comercializadas com violação de direito de autor, suas versões e derivações, em poder do infrator ou de quem as esteja expondo, mantendo em depósito, reproduzindo ou comercializando.

Há ainda outros meios de prova que são produzidos em fase de investigação:

> Atos preparatórios realizam-se, por isso, na fase investigatória destinados a obter essas provas e indícios. Daí os exames de corpo de delito, as inquirições testemunhais do inquérito policial, e certas providências cautelares efetuadas extrajudicialmente para assegurarem e preservarem elementos probatórios e indiciários de grande valor (Marques, 2003, p. 369).

Frise-se que as providências cautelares, após o advento da Constituição de 1988, devem ser precedidas de autorização judicial, salvo em hipóteses de flagrante delito.

Vige, no Brasil, em regra, o sistema da livre convicção, também denominado de verdade real, do livre convencimento ou da persuasão racional, porque o juiz não fica adstrito a critérios legais de prefixação de valores probatórios. O sistema da certeza moral do juiz ou da íntima convicção é exceção no julgamento proferido pelo júri.

Daí concluir que, no Brasil, o procedimento probatório do direito processual penal é dividido em várias fases que, às vezes, se interagem, como, por exemplo, valoração e produção da prova, deferimento de uma prisão preventiva, em que o magistrado analisa a presença dos requisitos do art. 312 e seguintes da lei processual penal que, com o encarceramento do acusado, facilita a realização da prova.

Por sua vez, em regra, a acusação propõe ou indica provas que pretende produzir, o juiz admite sua execução, enquanto a defesa tem o ônus de produzir as provas que entender oportunas, para, no *decisum*, serem valoradas.

3.7. O aspecto da licitude das provas

A Constituição Federal, ao dispor de forma expressa no art. 5º, inciso LVI, que "são inadmissíveis, no processo, as provas obtidas por meios ilícitos", impõe limites na busca da verdade a qualquer preço.

A proibição da prova a que a Carta da República se refere é "toda aquela que é defesa, impedida mediante uma sanção, impedida que se faça pelo direito. A que deve ser conservada à distância pelo ordenamento jurídico" (Aranha, 2006, p. 50).

No direito processual penal brasileiro, a proibição ocorre quando caracterizar violação de norma legal ou de princípios do ordenamento de natureza processual ou material (Grinover *apud* Mirabete, 2006). Grinover (2004, p. 156) destaca que,

> No campo das proibições das provas, a tônica é dada pela natureza processual ou substancial da vedação: a proibição tem natureza exclusivamente processual quando for colocada em função de interesses atinentes à lógica e à finalidade do processo; tem, pelo contrário, natureza substancial quando, embora servindo imediatamente também a interesses processuais, é colocada essencialmente em função dos direitos que o ordenamento reconhece aos indivíduos, independentemente do processo.

A Constituição Federal, ao ter elencado no art. 5º as garantias a serem observadas pelo órgão Estatal, resguardou os direitos da pessoa como inviolabilidade da manifestação de pensamento (inciso

IV), liberdade de culto (inciso VI), inviolabilidade da intimidade, da vida privada, da honra e da imagem (inciso X), inviolabilidade do domicílio (inciso XI) e das comunicações (inciso XII).

O Decreto n. 4.388, de 25 de setembro de 2002, aprovado pelo Decreto Legislativo n. 112, de 6 de junho de 2002, promulgado em 25 de setembro do mesmo ano, pelo então Presidente Fernando Henrique Cardoso, conhecido como Estatuto de Roma do Tribunal Penal Internacional, no art. 69, em que trata das provas, item n. 7, estatui:

> Não serão admissíveis as provas obtidas com violação do presente Estatuto ou das normas de direitos humanos internacionalmente reconhecidas quando: a) essa violação suscite sérias dúvidas sobre a fiabilidade das provas; ou b) a sua admissão atente contra a integridade do processo ou resulte em grave prejuízo deste.

Por outro turno, a Convenção Americana sobre Direitos Humanos (Pacto de *San* José da Costa Rica), ratificado pelo Brasil em 25 de setembro de 2002, na mesma época do Estatuto de Roma, vislumbra o respeito aos direitos da intimidade da pessoa, *in verbis*: "ninguém poderá ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação" (arts. 9º e 11).

A Constituição Federal utiliza a terminologia "ilícitos" em sentido amplo, abarcando tanto as provas ilícitas quanto as ilegítimas. Esse é também o entendimento da maioria dos doutrinadores (Grinover, 2004; Avena, 2012; Rangel, 2015; Lopes Jr., 2016). Nesse entendimento, são consideradas provas ilícitas aquelas produzidas com violação do direito material, mediante a prática de ilícito penal ou de contravenção penal, princípios constitucionais, como, por exemplo: coleta da confissão (prova) mediante a prática de tortura (fato considerado como crime, nos termos da Lei n. 9.455/1997); apreensão de documento (prova) mediante violação de domicílio (fato considerado como crime, art. 150 do Código Penal); e apreensão de correspondência (prova) mediante violação da intimidade (fato considerado como crime art. 151 do Código Penal).

De outro modo, são consideradas provas ilegítimas aquelas produzidas com violação de norma processual, como, por exemplo: juntada de documentos (que podem ser autos, papéis, jornais ou periódicos ou qualquer outro fato considerado como prova como uma exibição de uma arma em plenário) sem que se faça o requerimento prévio, observando-se o tríduo legal previsto no art. 479 do Código de Processo Penal; depoimento de testemunha que tenha obrigação de guardar segredo, nos termos do art. 207 do Código de Processo Penal; e não cumprimento da juntada de laudo pericial em crimes que deixam vestígios, art. 158 do Código de Processo Penal.

Em sentido contrário, Nucci (2008) e Marcão (2020) explicam que, após a modificação do art. 157 CPP pela Lei nº 11.690/2008, não existe diferenciação entre provas ilícitas e ilegítimas. Os autores se baseiam no argumento de que a norma processual se adequou ao comando constitucional, em que, após o advento desse dispositivo legal, prova ilícita é aquela que viola normas constitucionais ou infraconstitucionais.

No Brasil, o entendimento da doutrina é no sentido de que as provas produzidas com violação de direito material ou processual não podem ser utilizadas para prejudicar o acusado. A contrário *sensu*, a defesa tem se utilizado de tais provas, em face do princípio do *favor rei (*Mirabete, 2006).

Diante da problemática existente e da dissidência dos julgamentos nos tribunais, o princípio da proporcionalidade tem, em alguns casos, tido relevância, quando existe uma antinomia entre princípios. Todavia, é preocupante a questão de se valorar subjetivamente no caso concreto princípios que, aparentemente, estão colidindo entre si. E, portanto, os tribunais têm aplicado o princípio da proporcionalidade *in dúbio pro reo* ou em favor do réu. De outro modo, a *aplicação in dúbio pro societate* ou em defesa da sociedade pode abrir brechas para o uso indiscriminado de provas colhidas com afronta direta à norma material e processual, retrocedendo ao antigo discurso da corrente da Lei e Ordem[35], que o utiliza para minimizar algumas práticas avançadas e modernas de novas infrações que ficam impunes por serem de difícil elucidação.

Quanto aos ilícitos praticados na *Internet*, o Governo Americano, valendo-se do estado de alerta aos ataques terroristas ocorridos em Nova York, em 11 de setembro de 2002, com a queda das torres gêmeas e a morte de milhares de pessoas, fez, com o apoio da população, interceptações de mensagens via *e-mail*, de pessoas suspeitas de terrorismo em ação na *Internet.* A Lei de 1978, denominada FISA (*Foreign Intelligence Surveillance Act*), trata da questão de espionagem de suspeitos a serviço de potências estrangeiras.

Da mesma forma, a Convenção sobre *Cybercrimes*, de Budapeste, nos artigos 19, 20 e 21, autoriza os serviços de segurança, no curso de suas investigações, para se ter acesso aos registros mantidos pelos provedores, estender as buscas a outros computadores (se necessário) e ter informações "*real-time*" sobre conexões e trânsito em *websites*[36].

No entanto, percebe-se um verdadeiro retrocesso, principalmente no que diz respeito aos ilícitos digitais, uma vez que, em âmbito internacional, a polícia, com apoio do governo, tem se valido de meios ilícitos, sob o pretexto da utilização do princípio da proporcionalidade, apenas para atingir o interesse público em questão, esquecendo-se de que tais meios devem ser considerados como provas ilícitas em face das balizas constitucionais.

Portanto, a observância do aspecto da licitude das provas é uma preocupação dos profissionais do Direito, sobremaneira quando se trata de provas produzidas no direito processual penal. Ou seja, a liberdade do acusado depende da produção probatória vedada a sua produção a qualquer preço sob a assertiva da obtenção da verdade.

---

35 Por unanimidade, a Segunda Turma do Supremo Tribunal Federal (STF) negou provimento ao Recurso Ordinário em Habeas Corpus (RHC) 132115, impetrado por L. O. L. condenada pelo envolvimento na prática de irregularidades vinculadas a duas Organizações da Sociedade Civil de Interesse Público (Oscip) com sede em Curitiba (PR). No julgamento, os ministros confirmaram entendimento da Corte segundo o qual o sigilo da comunicação de dados por meios telemáticos (e-mail), assim como os demais direitos individuais, não é absoluto. No STF, a defesa sustentou, entre outros argumentos, a ausência de fundamentação da decisão do juízo da 2ª Vara Criminal Federal de Curitiba que autorizou a realização de interceptações telefônicas. Alegou que as diligências foram realizadas sem investigação preliminar e baseadas somente em denúncia anônima. Pediu ainda a nulidade das interceptações telemáticas sob o argumento de que o parágrafo único do artigo 1º da Lei 9.296/1996 seria incompatível com o sigilo da correspondência (artigo 5º, inciso XII, da Constituição Federal). Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=368918.

36 O Conselho Europeu considerava a Diretiva sobre Proteção de Dados e Informações nas Telecomunicações com uso da eliminação automática dos registros de conexão `a *Internet* que, em face da pressão do Governo Americano, aprovou em 30 de maio de 2002 uma emenda à Diretiva em que, no art. 15.1, todos os governos dos países membros deverão obrigar provedores de *Internet* e companhias de telefone a reter todos os registros de *e-mail* e transmissões de informações na rede que transitarem em seus sistemas, para garantir livre acesso à polícia e ao judiciário. Revista Consultor Jurídico. *Internet* e 11/9, 12 de set. de 2002, disponível em <http://conjur.estadao.com.br/static/text/27794,1>. Acesso em: 21 mar. 2025.

4. PROVIDÊNCIAS ACAUTELADORAS DE PROVA

O direito processual penal permite, em procedimento preparatório investigativo, a possibilidade de a autoridade policial utilizar-se de vários meios de prova denominados de providências acauteladoras de prova, com o objetivo de não perder de vista elementos importantes da prática do fato ilícito.

Para Ferreira (2004), acautelar significa prevenir, precaver-se, usar de cautela, resguardar-se. Silva (1989, p. 171) assevera que acautelar, "em sentido amplo, entende-se, na terminologia processual, todo e qualquer ato forense ou processo intentado por uma pessoa, em justiça para prevenir, conservar, ou defender direitos".

A cautela é espécie de tutela jurídica, a fim de tutelar um direito de proteção da sociedade e ver aplicada a lei de forma justa. Para tanto, fazem-se necessários meios, entre os quais, a cautela penal para viabilizar a produção dos meios probatórios (Barros, 1987).

Tendo notícia do crime, o delegado de polícia tem o dever de iniciar as investigações para a busca de materialidade e autoria do delito. O objeto da *persecutio criminis* é preparar a acusação para que o Ministério Público (se a ação penal for pública) ou o ofendido (se a ação penal for privada) tenham elementos suficientes para proporem a ação penal.

Todavia, há casos em que se prescinde de providências urgentes que tenham a finalidade de conservar provas e a utilização delas pelo titular da ação penal em momento oportuno. Em outras palavras, é dizer que, sem elas, torna-se praticamente impossível o oferecimento da denúncia ou da queixa.

O art. 6º do Código de Processo Penal enumera, em nove incisos, as diligências às quais, de forma discricionária, a autoridade deverá proceder de acordo com o caso concreto. Nesses termos, a primeira medida descrita na norma, prevista no inciso I, é no sentido da preservação e da não alteração das coisas até a chegada dos peritos criminais.

De igual modo, o art. 169 da mesma norma processual prevê:

> Para o efeito de exame do local onde houver sido praticada a infração, a autoridade providenciará imediatamente para que não se altere o estado das coisas até a chegada dos peritos, que poderão instruir seus laudos com fotografias, desenhos ou esquemas elucidativos (Brasil, 1940).

Importante modificação feita no Código de Processo Penal que merece ser lembrada foi a inclusão da cadeia de custódia no art. 158-A a 158-E, que impõe regras para "a lisura da produção da prova, em particular, a pericial" (Nucci, 2020).

O conceito da cadeira de custódia está no art. 158-A:

> Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.

Cunha (2020) explica que a utilização fidedigna da cadeia de custódia por peritos e servidores do sistema de justiça criminal reduz a probabilidade de contaminação das amostras dando maior garantia da autenticidade do elemento da prova. Para que isso ocorra, faz-se necessário observar duas fases, a seguir descritas.

Fase externa: a) preservação do local do crime; b) cuidado nas diligências realizadas pelos policiais que são, geralmente, os primeiros a chegarem no local do crime; c) isolamento; d) fixação e coleta; e) acondicionamento do objeto a ser periciado; f) transporte; g) recebimento do vestígio.

Fase interna: a) recepção; b) conferência; c) classificação; d) guarda ou distribuição do vestígio; e) análise pericial; f) guarda ou devolução do vestígio de prova; g) guarda de vestígios para contraperícia; h) registro da cadeia de custódia.

Alinhavando os meios de provas que podem ser requeridas ao juiz, o Código de Processo Penal não possui uma estrutura coerente ao mesclar, em um primeiro momento, no art. 6º, incisos I a IX, a obrigação da autoridade policial de apreensão dos instrumentos e todos os objetos que tiverem relação com o fato sem mencionar o procedimento correspondente e, em outro, adotar medidas em relação ao que seja considerado como prova, por exemplo, busca e apreensão, arts. 240 a 250 do mesmo diploma legal.

No Livro I, título II, ao tratar sobre o inquérito policial, como já dito, há inúmeras diligências que podem ser realizadas pelo delegado de polícia, que são previstas posteriormente no capítulo V, como a restituição das coisas apreendidas, arts. 118 a 124, e, no capítulo VI, as medidas assecuratórias de natureza real. Essa ilogicidade pode ser vista na disposição topográfica do *codex* sobre a restituição em momento anterior ao da busca e apreensão, como se vê no capítulo XI, arts. 240 a 250, do Código de Processo Penal. Isso porque, primeiro, se apreende, depois se restitui.

Para tanto, cabe à autoridade fazer uma interpretação correta da legislação processual penal para acautelar corretamente coisas em situações derivadas de ilícito virtual. Essa providência implica aplicar a medida apropriada como meio de prova. Pode ocorrer que a notícia do crime seja daquelas em que o flagrante não é possibilitado, máxime, em alguns casos de condutas praticadas na rede mundial de computadores.

É de se verificar que o Código de Processo Penal, de 1940, não está apto a tratar do *modus procedendi* da moderna prática do ilícito virtual. Ao terem conhecimento do fato, que ocorre em muitos locais ao mesmo tempo, a exemplo dos crimes plurilocais, a autoridade deve investigar com o aparato legal em vigor. De outro modo, o delegado deve coletar a prova em crimes cometidos a distância ou em espaço máximo, o que dificulta o seu trabalho, haja vista que necessita de colaboração das autoridades de outros países.

Assim, primeiramente, analisar-se-ão algumas medidas acauteladoras previstas em lei, que têm sido largamente utilizadas pelos órgãos responsáveis na missão de investigação, em especial no tocante aos ilícitos praticados na *Internet,* quando as provas colhidas na fase de investigação são daquelas não renováveis.

4.1. Da busca e apreensão

A busca diverge da apreensão. Só se apreende quando se busca e se encontra alguma coisa. Busca é instrumento e, apreensão, garantia da prova (Lopes Júnior, 2016). Tanto é que pode haver apreensão sem necessidade da busca. Basta que o detentor da coisa que se pretende apreender a entregue espontaneamente, dispensando a busca. E pode também ter a busca sem apreensão, porque o objeto buscado não foi encontrado.

O art. 240 do Código de Processo Penal estabelece que a busca poderá ser domiciliar ou pessoal. A busca domiciliar será procedida para prender pessoas suspeitas de terem cometido crimes, apreender coisas achadas ou obtidas por meios ilícitos, apreender instrumentos de falsificação ou de contrafação e objetos falsificados ou contrafeitos, apreender armas e munições, instrumentos utilizados na prática do crime ou destinados a fim delituoso, descobrir objetos necessários à prova de infração ou à defesa do réu, apreender pessoas vítimas de crimes e colher qualquer elemento de convicção para a elucidação do fato.

A busca e apreensão podem ocorrer *ex officio* ou requeridas pela acusação ou defesa. Não existe momento específico para a busca e a apreensão de coisas e pessoas, podendo ocorrer antes, durante ou no decorrer da ação penal. Todavia, o bom senso recomenda que seja realizada antes ou durante a instauração do inquérito policial.

Para que a autoridade policial possa buscar e apreender objetos e coisas que tenham relação com os ilícitos digitais, ressalvadas as hipóteses da prisão em flagrante, dispostas nos arts. 301 e seguintes do Código de Processo Penal, só poderá fazê-lo munido de autorização judicial. Trata-se de uma garantia constitucional que, nas hipóteses dos ilícitos digitais, tem sido amplamente discutida pela doutrina. Se, por um lado, evita que domicílios sejam invadidos sem que a autoridade esteja munida de mandado, fortalecendo a inviolabilidade de domicílio e da privacidade, por outro lado, dificulta a execução eficaz da medida acauteladora em crimes digitais em face da instantaneidade das informações armazenadas (Góis Júnior, 2002; Drummond, 2003; Aranha, 2006).

É um meio de prova coercitivo, acautelador e que se realiza *inaudita altera pars*. É uma medida cautelar de natureza real que visa assegurar a obtenção e perpetuação de uma prova (Aranha, 2006). Ou seja, o acusado não tem ciência prévia de que serão apreendidos objetos relacionados com o suposto ilícito praticado porque, se acaso souber da diligência com antecedência e deixar que tais objetos sejam alvos da polícia, colaborará com a acusação.

Como se trata de mero procedimento administrativo, quando realizado em sede de inquérito policial, o investigado não tem o conhecimento prévio de que será abordado em sua casa ou em seu local de trabalho, para ter seu computador ou outros objetos apreendidos.

Nos ilícitos digitais, a medida coercitiva e cautelar serve para apreender computadores, aparelhos de telefones celulares, mídias relacionadas ao uso da informática, como *CDs*, *DVDs*, *Zip disks*, disquetes, memória *flash*, cartões *smart media*, monitores, impressoras, *chips*, *notebooks, palmtops*, *pen drives*, dentre outros.

Essas são medidas importantes que poderão ensejar propositura da ação penal derivada de investigação efetiva que resultou na existência de elementos de convicção para a formação da *opinio delicti.*

Na conformidade do art. 12 da Lei nº 9.610, de 19 de fevereiro de 1998, em crimes praticados com violação de programa de computador, a medida deverá ser efetuada mediante o acompanhamento de perito oficial nomeado pelo juiz. Porém, quanto aos crimes praticados com o uso da *Internet*, a lei não faz menção da necessidade de os policiais estarem acompanhados de especialistas na matéria. Todavia, a operação de busca e apreensão pode ou não possibilitar o êxito de exame do material ou equipamento apreendido em casos concretos em que há a ausência de comprovação da conduta ilícita (Costa, 2003).

Em cada sistema operacional informático existe uma técnica para que o computador seja desligado normalmente sem prejuízo dos dados ali inseridos e armazenados. Caso a pessoa responsável por fazer a apreensão da máquina computacional seja despreparada tecnicamente, como, por exemplo, desligar o computador sem a observância dos comandos ao sistema em que estava ligado, pode acarretar sérios prejuízos em momento posterior, e inviabilizar o laudo pericial. Na abordagem sobre as perícias realizadas nos ilícitos digitais, a matéria será amplamente discutida no item "6.7", .

4.2. Das medidas cautelares de natureza pessoal

Além das medidas assecuratórias de natureza real, há outras de natureza pessoal que são as três prisões de natureza processual: prisão em flagrante, prisão temporária e prisão preventiva, as quais podem ser utilizadas em crimes virtuais. Como já visto alhures, o atacante da rede que comete ilícitos, via de regra, permanece muito tempo no anonimato, devido às técnicas mais comuns por eles utilizadas.

As autoridades, ao terem conhecimento de uma *notitia criminis* de fatos envolvendo ilícitos digitais, devem ter o cuidado para não perder de vista o sujeito que esteja supostamente envolvido. A prisão em flagrante, prevista no art. 301 e 302 do Código de Processo Penal, tem relevância com o tema abordado porque, na hipótese de o suposto autor da infração ser pego em flagrante delito, seja no flagrante próprio (incisos I e II), impróprio (inciso III) ou presumido (inciso IV) do art. 302 do CPP, além de se apreender a pessoa, geralmente, tem-se a possibilidade de apreender coisas que tenham relação com o ilícito. Com a prisão da pessoa e a apreensão de instrumentos, armas, objetos ou papéis que presumam ser a autora da infração, outras modalidades de prova poderão ser obtidas a partir do flagrante.

Lamentavelmente, as prisões realizadas nas madrugadas de finais de semana e em ocasiões similares fragilizam o estado físico e psicológico do preso, e uma confissão pode ser obtida com mais facilidade. Mesmo que essa confissão não tenha valor probatório se não for ratificada em juízo, o simples registro nos autos acarretará prejuízos ao indiciado, se for corroborada por outras provas trazidas a lume ao processo penal. Essas outras provas vêm aderidas com a prisão do suposto autor do fato, como, por exemplo, a apreensão de uma arma, que será endereçada à perícia.

Nos ilícitos digitais, em que os suspeitos estiverem sendo investigados pela polícia, não havendo certeza de uma situação de flagrância, a medida a ser pleiteada pela autoridade policial é a representa-

ção ao juiz competente para a possibilidade de deferimento das medidas cautelares de natureza processual em regra, como a prisão preventiva e a prisão temporária.

A prisão preventiva é cabível em qualquer fase do inquérito policial ou da instrução criminal, podendo ser decretada de ofício pelo magistrado, a requerimento do ministério público ou do querelante e mediante representação da autoridade policial, como se depreende da redação do art. 311 do CPP.

A previsão do art. 312 do Código de Processo Penal exige a presença dos requisitos para decretação da medida, quais sejam o *fumus boni iuris* e o *periculum libertatis* (Lopes Júnior, 2017).

O primeiro requisito diz respeito à prova da existência do crime e aos indícios suficientes de autoria, enquanto o segundo está ligado às quatro hipóteses fáticas dispostas no art. 312 do CPP. Antes do ingresso ao segundo requisito, analisar-se-á a questão do *fumus boni iuris*. Se o primeiro requisito está ligado diretamente à prova da existência do crime e, nos crimes virtuais, são daqueles que deixam vestígios, verificar-se-á que a autoridade policial poderia representar pela medida extrema, instruindo o pedido com a prova pericial (De Lima, 2020).

Todavia, na prática, as dificuldades para coleta dos objetos a serem periciados são de grande monta, porque, em alguns casos de difícil elucidação, o que se verifica é exatamente o contrário. Após cumprimento do mandado de prisão preventiva e de busca e apreensão dos computadores e outros objetos é que a polícia tem em mãos os elementos concretos para serem enviados à perícia.

Ou seja, a perícia se constitui como fundamento essencial para que se decrete o segregamento da liberdade do acusado. No entanto, o que se vê é que a perícia geralmente é trazida a exame em momento posterior, após o cumprimento do mandado da prisão preventiva, nos termos do inciso III, do art. 312 do CPP.

Para que a autoridade policial possa representar pela prisão preventiva, deverá, no entanto, fazer juntada de outras provas que indiquem a existência do crime, que, nos ilícitos que deixam vestígios, dar-se-á de outras formas, como, por exemplo, o requerimento da vítima mediante reclamação administrativa feita ao banco informando o desaparecimento de valores na conta corrente ou aplicações financeiras. Essa prova pode ser carreada aos autos mediante a juntada do requerimento escrito da vítima – cliente do banco, bem como a conferência dos extratos bancários.

Portanto, a análise do inciso III do art. 312 do CPP, é de fundamental importância, uma vez que, cumprido o mandado de prisão preventiva e apreendidos os objetos que tenham relevância com o fato que se pretende provar de ilícitos cometidos na *Internet*, ter-se-á maior probabilidade de êxito na coleta da prova. No dizer de Barros (1987, p. 200-201),

> A conveniência da instrução criminal tem função dúplice: a) utilizar do acusado como prova no processo; b) evitar que ele prejudique a colheita da prova, dificultando a descoberta da verdade. No primeiro aspecto, não se apresenta mais qualquer dúvida de que o acusado é também prova no processo, não só pelo que possa dizer, cooperando com o juiz na reconstrução fática; mas também pelo seu próprio aspecto somático, bastando pensar num reconhecimento de pessoa, o qual não se realiza sem a sua presença.

O art. 5º, inciso LVII, da Constituição Federal estabelece que, se o acusado estiver preso e comparecer perante o juiz em interrogatório, não terá a obrigação de responder às perguntas que lhe forem formuladas a respeito dos fatos e, muito menos, de dizer a verdade, art. 5º, inciso LVII, o que implica na não cooperação, como relata Barros (1987). Porém, não se pode olvidar que com a efetivação da prisão preventiva abre-se para o órgão persecutório maiores chances de obter as provas dos fatos relacionados com o ilícito investigados pela autoridade policial.

São exemplos de meios de provas relacionadas à instrução criminal: a presença do depoimento de testemunhas que não tenham sido afugentadas (corrupção ou suborno) ou amedrontadas (ameaça/coação); acareação entre testemunhas e entre testemunhas e o preso.

Relevante a opinião de Oliveira (2005, p. 422), ao afirmar que

> Por conveniência da instrução criminal há de entender-se a prisão decretada em razão da perturbação ao regular andamento do processo, o que ocorrerá, por exemplo, quando o acusado, ou qualquer outra pessoa em seu nome, estiver intimidando testemunhas, peritos ou o próprio ofendido, ou ainda está provocando qualquer incidente do qual resulte prejuízo manifesto para a instrução criminal.

Questão relevante diz respeito à prisão temporária, prevista na Lei n. 7.960, de 21 de dezembro de 1989, ao listar no art. 1º os requisitos da prisão e por quais ilícitos poderá ser decretada. Segundo o doutrinador, "Trata-se de medida acauteladora, de restrição da liberdade de locomoção, por tempo determinado, destinada a possibilitar as investigações a respeito de crimes graves, durante o inquérito policial" (Mirabete, 2025, p. 392).

A prisão temporária tem sido utilizada em grandes operações policiais, a exemplo da Operação Lavajato, deflagrada pela Polícia Federal, para investigar desvio de recursos públicos relacionados à Petrobrás, empresa brasileira, estatal de economia mista, responsável pela exploração, produção, refino, comercialização e transporte de petróleo, gás natural e seus derivados.

Prisões temporárias para apuração de crimes digitais também têm sido decretadas no Brasil. Exemplo disso, é a notícia veiculada na internet pela Polícia Federal que deflagrou em 13/5/2025 a operação "Face Off", com o objetivo de desarticular uma associação criminosa especializada em fraudar contas digitais vinculadas à plataforma GOV.BR, utilizando técnicas avançadas de alteração facial para burlar sistemas de autenticação biométrica (Polícia Federal, on line, 2025).

Nessas hipóteses, são três os fundamentos exigidos no art. 1º para o cabimento da medida, os quais são: imprescindibilidade para as investigações do inquérito policial; quando o indiciado não tiver residência fixa ou não fornecer elementos necessários ao esclarecimento de sua identidade; e quando houver fundadas razões, de acordo com qualquer prova admitida na legislação penal, de autoria ou participação do indiciado em tipos penais especificados nas alíneas de "a" a "o" do inciso III do art. 1º da lei.

Tourinho Filho (2002, p. 471) entende que

> A exigência de fundadas razões quanto à autoria ou participação é necessariamente imprescindível, visto não existir cautelaridade sem esse requisito. O *periculum in mora*, ou *libertatis*, consistirá na circunstância de ser a medida "imprescindível

> às investigações policiais", tenha ou não o indiciado residência fixa, crie ou não embaraços à colheita de dados para esclarecer sua identidade, ou, finalmente, ainda que não imprescindível às investigações, "se o indiciado não tiver residência fixa" ou "não fornecer elementos necessários ao esclarecimento de sua identidade".

No caso em tela, das quatorze hipóteses de crimes, aquela que terá vinculação maior aos ilícitos digitais é a alínea "l", que trata da formação de associação criminosa, art. 288 do Código Penal Brasileiro. Ou seja, a prisão temporária nos ilícitos digitais pode ser decretada quando houver a participação de mais de três pessoas configurando esse crime. Caso contrário, a medida cautelar poderá ser decretada em situações a ela relacionadas e devidamente fundamentada.

Da mesma forma que na prisão preventiva, art. 311 do CPP, a autoridade policial pode representar ao magistrado para a decretação da prisão temporária, art. 2º da Lei nº 7.960/1989. Entretanto, ao contrário da prisão preventiva, a temporária não pode ser decretada de ofício pelo juiz e só ocorre na fase investigativa (inquérito policial).

Em suma, o que se destaca é que, com a ocorrência das três modalidades de prisão processual – flagrante, preventiva e temporária – é possível que se originem outras provas que podem ser produzidas, principalmente na fase investigativa, sendo estas: inquirição de testemunhas, apreensão de objetos, acareações entre pessoas, confissão do indiciado, prova pericial derivada da apreensão dos computadores e objetos apreendidos.

4.3. Da previsibilidade e da possibilidade probatória de outras medidas utilizáveis nos ilícitos digitais

Além das espécies de meios de prova de natureza cautelar já explicitados, o Código de Processo Penal prevê outras, também conhecidas como nominadas ou típicas, quais sejam: interrogatório do acusado, oitiva das testemunhas, acareações, reconstituição de crime, entre outras.

A Lei n. 9034, de 3 de maio de 1995, dispõe sobre a utilização de meios operacionais para prevenção e repressão de ações praticadas por organizações criminosas.

O Brasil assinou em 2000 a Convenção da ONU sobre delinquência organizada transnacional, em que se procura definir o que seja crime organizado: composto por mais de três pessoas, com estabilidade, com intenção de cometer crimes graves, com pena cominada em abstrato, no grau máximo, igual ou superior a quatro anos e intuito de obter lucros. O art. 2º da Convenção prevê que a organização deve envolver mais de um país para ter o caráter transnacional.

Nos crimes digitais, nos termos do §1º do art. 1º da Lei nº 12.850/2013, organização criminosa é configurada como

> "[...] associação de quatro ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional.

Nesses casos, o uso de uma investigação mais aprofundada é permitido desde que haja autorização judicial prévia. As medidas devem ser autorizadas pelo magistrado, e exige muito preparo das autoridades policiais, ainda mais se tratando de ilícitos digitais em que algumas informações se revestem de instantaneidade, o que obsta a busca da materialidade e da autoria.

Com a modificação dessa Lei pela *novatio legis in pejus*, Lei n. 13.0964/2019, outros institutos importantes foram incluídos, como colaboração premiada e ação controlada da polícia, que consiste em "retardar a intervenção policial ou administrativa relativa à ação praticada por organização criminosa ou a ela vinculada, desde que mantida sob observação e acompanhamento para que a medida legal se concretize no momento mais eficaz à formação de provas e obtenção de informações" (Brasil, 2013).

5. A INTERCEPTAÇÃO TELEFÔNICA

A Constituição Federal, art. 5º, inciso XII, prevê a respeito da inviolabilidade do sigilo de correspondência e das comunicações telegráficas, de dados e telefônicas, com a ressalva da permissão de suas obtenções por intermédio de autorização judicial nas hipóteses estabelecidas em lei para fins de investigação criminal ou instrução processual penal.

A Lei n. 9.296, de 24 de julho de 1996, regulamentou a parte final do inciso XII, e entrou em vigor na data de sua publicação. O art. 1º da referida lei estabeleceu que a interceptação de comunicações telefônicas de qualquer natureza somente poderá ser aceita como prova se houver autorização judicial, em obediência aos dispositivos legais.

Com a Lei n. 9.296/1996, cessou a discussão existente na doutrina e nos tribunais sobre a receptividade do antigo Código Brasileiro de Telecomunicações, que fazia menção à autorização judicial, mas não especificava hipóteses e forma de sua realização (Fernandes, 1996)[37].

Para entender melhor a matéria, é preciso que se conceituem os institutos previstos na mencionada legislação, a começar pelo conceito de interceptação: "Ato ou efeito de interceptar (*de inter e capio*), tem, etimologicamente, entre outros, os sentidos de: ´1. interromper no seu curso; deter ou impedir passagem; 2. Cortar, interromper: interceptar comunicações telefônicas" (Holanda, 1986, p. 957).

Outra definição é do que seja interceptação telefônica: "captação feita por terceira pessoa de comunicação entre dois (ou mais) interlocutores sem o conhecimento de qualquer deles" (Rangel, 2015, p. 80). As interceptações podem ser divididas em *latu sensu* e *strictu sensu*. A interceptação *latu sensu* pode ser entendida como "ato de interferência nas comunicações telefônicas, quer para impedi-las com consequências penais quer para delas tomar conhecimento nesse caso, também com reflexos no processo" (Avolio, 2003, p. 91).

Em sentido estrito, ou *strictu sensu*, segundo Avolio (2015), pode-se resumir a interceptação telefônica como captação de uma conversa por terceira pessoa, sem o conhecimento dos interlocutores. Esse meio de prova (gravação e transcrição das conversas) é utilizado nos crimes praticados pela *Internet* para desbaratar atividades criminosas e elucidar o *modus operandi* dos autores do delito.

37 O art. 57 do Código Brasileiro de Telecomunicações, Lei n. 4.117/1962 previa que: "não constitui violação de telecomunicação: II – o conhecimento dado; e) ao juiz competente, mediante requisição ou intimação deste". Esse Código foi derrogado pela Lei de Telecomunicações, Lei n. 9.472/1997, com modificações introduzidas pela Lei n. 9.986/2000.

A doutrina classifica as interceptações da seguinte forma: em sentido estrito, escuta telefônica, interceptação ambiental, escuta ambiental e gravações clandestinas. A escuta telefônica ocorre quando um dos interlocutores consente na captação da conversa, usualmente utilizada em casos de sequestro (Capez, 2005; Aranha, 2006; Avolio, 2015).

Por sua vez, a interceptação ambiental ou interceptação entre presentes ocorre com a captação de conversa entre pessoas de um mesmo local, que, sem o seu conhecimento, é realizada por terceiro (Souza, 2020). No Brasil, a interceptação ambiental está regulamentada no art. 10-A da Lei nº 9.296/1996 como crime se for realizada sem autorização judicial: "realizar captação ambiental de sinais eletromagnéticos, ópticos ou acústicos para investigação ou instrução criminal sem autorização judicial, quando esta for exigida" (Brasil, 1996).

A Constituição Federal assegura a privacidade e a imagem dos indivíduos, mas esses direitos fundamentais não são absolutos, permitindo exceções para sua flexibilização. Uma dessas exceções, introduzida pela Lei nº 13.964/2019 ("Pacote Anticrime"), está no art. 8º-A, parágrafo 4º, da Lei nº 9.296/1996. Essa disposição permite o uso de captações ambientais de sons ou imagens feitas por um dos interlocutores, mesmo sem o conhecimento da polícia ou do Ministério Público, como prova de defesa, desde que a integridade da gravação seja comprovada.

Adicionalmente, o art. 10-A da Lei nº 9.296/1996, também incluído pelo Pacote Anticrime, esclarece que a captação ambiental sem autorização judicial (quando exigida) constitui crime, exceto quando a gravação é feita por um dos interlocutores. O ministro Ribeiro Dantas observou que as mudanças trazidas pelo Pacote Anticrime geraram discussões sobre novos parâmetros para a admissão de gravações ambientais clandestinas, especialmente quando se pretende usá-las como prova de acusação. Ele explicou ainda que, apesar da redação do art. 8º-A, parágrafo 4º, a doutrina majoritária defende a licitude de tal prova tanto para a acusação quanto para a defesa. Essa posição é fundamental para manter os princípios da paridade de armas, da lealdade, da boa-fé objetiva e da cooperação entre os sujeitos processuais. Assim, essa nova regulamentação não abrange apenas o direito de defesa, mas também beneficia as vítimas de crimes (STJ, 2025).

A escuta ambiental é aquela em que a interceptação da conversa entre presentes é realizada por terceiro em local público ou privado, com o conhecimento de um ou alguns (De Lima, 2020).

A gravação telefônica ou clandestina é a realizada pelo interlocutor ao registrar a conversa telefônica em que há o desconhecimento da outra parte (De Lima, 2020). Ou seja, quem detém o controle da informação é quem realiza a gravação da conversa[38].

Por seu turno, na ótica de Aranha (2004), a classificação ocorre com a divisão em gravação e da interceptação telefônica. A gravação telefônica pode ser feita com o conhecimento de ambos os interlocutores ou sem o conhecimento de um dos interlocutores, sendo permitida apenas a primeira. Já a interceptação telefônica é o gênero em que, se houver o conhecimento de um dos interlocutores, denomina-se escuta telefônica. Se os interlocutores não tiverem conhecimento, denomina-se interceptação telefônica.

38 Em RO de n. 21543/00 oriundo da 3ª. Região do TRT, o Ministro Relator Paulo Maurício Pires da 3ª Turma entendeu que a gravação telefônica deve ser desconsiderada porque é prova ilícita, uma vez que não teve autorização judicial.

Depreende-se que a interceptação, para ser considerada prova ilícita, deve estar fora dos padrões elencados na Lei nº 9.296/1996 e do art. 5º, X, da Constituição Federal, o que se verá a seguir no próximo tópico.

5.1. As vedações legais de admissão da interceptação telefônica

O art. 2º da Lei nº 9.296/1996 trouxe, em forma de negativa, as hipóteses em que não será admitida a interceptação telefônica com má técnica legislativa. Da mesma forma que o Código de Processo Penal optou por especificar quais são os casos em que não será admitida a fiança, o legislador o fez na Lei de Interceptação Telefônica. Realmente, há de se concordar com De Lima (2020) e Aranha (2004) de que o texto não é claro quando não lista as hipóteses em que a interceptação telefônica é admissível.

A primeira vedação diz respeito à não existência de indícios razoáveis da autoria ou participação em infração penal. O primeiro requisito diz respeito ao autor do fato, remetendo ao art. 3º, inciso I, da Lei nº 9.296/1996. Ou seja, geralmente, a interceptação telefônica é requerida pelo Delegado de Polícia, para dar suporte à investigação criminal já instaurada, ou pelo representante do Ministério Público na investigação criminal e na instrução penal.

Nessa primeira hipótese, vislumbra-se a preocupação do legislador em inibir ações investigativas em que se busca a medida cautelar, antes mesmo de haver qualquer tipo de notícia do crime, para facilitar o procedimento policial. O requisito do *fumus boni juris*, que, diga-se de passagem, é comum a todas as medidas cautelares, deve estar presente para que o magistrado possa conceder a medida cautelar de interceptação telefônica.

A famigerada interceptação de prospecção, apesar de combatida pelos juristas, lamentavelmente ainda é utilizada na prática policial na escuta de aparelhos celulares, com o intuito de descobrir se uma pessoa está ou não envolvida em fato que constitua infração penal (Gomes *apud* Avolio, 2003).

Em suma, a medida pode ser concedida havendo fato determinado como crime e que necessite ser investigado e demonstrado, devendo existir ocorrência concreta, jamais cogitação, admitindo-se a interceptação pós-delitual, e não pré-delitual.

A segunda exigência contida no inciso II do art. 2º da Lei nº 9.296/1996, estabelece que a interceptação só será admitida se não houver outro meio disponível para a obtenção da prova.

Quando a lei deixa claro que a interceptação é exceção, e não regramento, a sua concessão como medida extrema pode ser admitida se não puder se realizar de outro modo. Mas, que outros modos seriam estes?

No entender de Greco Filho (2005, p. 29), "além do aspecto subjetivo que a ideia encerra, o ´não estar disponível´ pode significar, na verdade, estar oculta (inconsciente ou propositadamente) ou, simplesmente, não haver interesse de se investigar por outro meio".

A melhor interpretação desse requisito faz alusão ao art. 4º da mesma lei, em que o pedido deve ter demonstrado a real necessidade da apuração da infração penal. Por outro lado, o juiz, ao concedê-la,

deve fundamentar, dada a peculiaridade do caso concreto, analisando pormenorizadamente a existência do perigo da demora.

A terceira e última exigência, disposta no inciso III do art. 2º da Lei nº 9.296/1996, especifica que a interceptação telefônica não será admitida se o fato investigado constituir infração penal punida, no máximo, com pena de detenção.

Inicialmente, cumpre esclarecer que o critério objetivo de vedação de se realizar interceptações telefônicas é muito criticada na doutrina (Avolio, 2003; Greco Filho, 2005). Assim, as contravenções penais abrangidas pelas Leis 9.099/1995 e 10.409/2002, bem como os crimes de pequeno potencial ofensivo, não poderão ser objeto da medida cautelar.

Por outro lado, vincular a possibilidade de se fazer a interceptação telefônica em rol taxativo de crimes punidos com pena de reclusão ofende sobremaneira o princípio da proporcionalidade. Justifica Avólio (2003) que, nessa seara, o legislador esqueceu-se de que a concessão somente poderia ser admitida em face da excepcional gravidade dos crimes ou da forma particular da execução de outros, ainda que punidos com penas de detenção.

A Lei nº 13.964/2019 (Pacote Anticrime) incluiu o art. 8º-A na Lei nº 9.296/1996, que trata da captação ambiental de sinais eletromagnéticos, ópticos ou acústicos (similar à interceptação, mas de conversas no ambiente, não telefônicas). Para a captação ambiental, a lei estabelece que ela pode ser autorizada para "infrações penais com pena máxima superior a 4 (quatro) anos, ou em infrações conexas". Isso também exclui, em regra, crimes punidos apenas com detenção, a menos que sejam conexos a outros crimes mais graves.

Fazendo uma análise das três hipóteses obstativas do art. 2º da Lei nº 9.296/1996, no tocante aos crimes digitais, fica clara a existência da restrição judicial na apuração de crimes dessa natureza, porque, como visto no item 2.1.2, vários deles são punidos com pena de detenção.

5.2. A (im)possibilidade da interceptação telemática e dos dados na rede mundial de computadores

A inconstitucionalidade do parágrafo único do art. 1º da Lei nº 9296/1996 é levantada no que se refere à interceptação de fluxo de comunicações em sistemas de informática e telemática, ao ser confrontado com o inciso XII, do art. 5º da Constituição Federal, em ressalvar expressamente, ao último caso, a possibilidade de interceptação mediante ordem judicial, referindo-se às comunicações telefônicas (Greco Filho, 2005).

O problema é terminológico. Em primeiro lugar, o que significa interceptação de qualquer natureza prevista nos arts. 1º e 8º da Lei nº 9.296/1996?

Tem-se que verificar se a interceptação pode ser aplicada a qualquer tipo de comunicação via telefone, ou apenas às conversações telefônicas (Avolio, 2003). É uma pergunta difícil de ser solucionada, tendo em vista as mais variadas interpretações, sendo elas de cunho teleológico, técnico, lógico ou científico, uma vez que a lei não conceituou o que seja sistema de informática e telemática.

Enquanto a telemática "é a ciência que trata da manipulação e utilização da informação através do uso combinado de computador e meios de telecomunicação" (Ferreira, 1986, p. 1.658), a informática, em sentido próprio, pode ser concebida como "o processamento eletrônico da informação, na medida em que esteja correlacionado com determinado tipo de técnica documentária" (Pimentel, 2000, p. 38).

A palavra sistema, que antecede a informática e a telemática, vem inserir os dois institutos em uma ideia de todo, em que os elementos organizados entre si podem funcionar em uma estrutura organizada. Sistema é "um conjunto físico ou conceitual composto de partes interdependentes, que interagem dentro de interfaces definidas para que se atinja um determinado objetivo ou objetivos comuns" (Camarão, 1994, p. 574).

O assunto é polêmico, e daí a ocorrência de duas correntes que serão abordadas a seguir.

a) Luiz Flávio Gomes (ano 2011, p. 40) parte da evolução conceitual de telecomunicação desde o Código Brasileiro de Telecomunicações, art. 60, §1º, da Lei nº 9.472/1997, *in verbis*: "[...] telecomunicação é a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza".

Segundo o autor, é perfeitamente aceitável, sem qualquer afronta à Lei Maior, que o juiz possa autorizar interceptação de qualquer tipo de comunicação telefônica, em conjunto ou não com a informática, compreendendo as espécies diretas como *fax* e *modem*, e as indiretas como *Internet, e-mail* e correios eletrônicos (Avolio *apud* Gomes, 2003, p.165).

b) Geraldo do Prado (1997) aborda a questão com critério técnico, de forma diferenciada, dando ênfase à instantaneidade das comunicações telefônicas, ou seja, somente as comunicações de dados podem ser interceptáveis, ao contrário dos bancos de dados.

Prado (1997), faz referência a Tércio Sampaio Júnior para confirmar sua tese, explicando que, dos quatro meios de comunicação (correspondência, telegrafia, dados e telefonia), só o último se reveste de instantaneidade. Finaliza aduzindo que os outros meios podem ser apreendidos, e que o último, dada sua natureza, se não for interceptado, perderá no tempo, em face de seu desaparecimento imediato em sua concretude. *In verbis*:

> Quando os dados informáticos repousarem em bancos de dados, a sua comunicação não poderá ser objeto de interceptação, pois assim estaria sendo violada a Constituição. Porém, interpretada sistematicamente e teleologicamente não haverá contraste com a norma de garantia a interceptação determinada à luz do devido processo legal, para fins de instrução criminal ou investigação da mesma natureza, se se tratar de dados transmissíveis de modo a não repousarem em banco de dados ou forma similar, que permita a apreensão (Prado, 1997, p. 14).

Conclui que o objeto da proteção da Carta da República é o agir comunicativo; que, em determinadas situações, a comunicação telefônica não está inserida nessa proteção. Como exceção, cita a instantaneidade da comunicação telefônica, uma vez que não se permite a apreensão da informação,

para os fins da prova; que a comunicação de dados, por qualquer meio automatizado, não pode ser interceptada se tais dados repousarem em bancos de dados, ressalvando, porém, que nem todos os dados informáticos repousam ao final em processo comunicativo de dados. Finaliza, no último caso, sem explicar como que, se os dados informáticos não repousarem em bancos de dados, podem ser interceptados estando preenchidos os mesmos requisitos da interceptação telefônica (Prado, 1997).

c) Damásio E. de Jesus (2000) interpreta a norma ordinária de modo prático, fazendo-o de forma sistemática. Esse autor defende a constitucionalidade da interceptação de qualquer espécie de comunicação telefônica, ressalvados os realizados via cabo ou rádio, nos termos da Lei n. 9.296/1996. Ironiza ao dizer que o legislador não seria negligente a ponto de prever a possibilidade de se interceptar apenas uma conversa verbal, pois, sendo assim, para não ser interceptado, bastaria alguém "*digitar*" ao invés de "*falar*".

d) Luiz Francisco Torquato Avolio (2003), ao tratar dos posicionamentos acima alinhavados, afirma que os argumentos tanto de Gomes quanto de Damásio e Prado não merecem guarida porque, partindo da análise de Prado, a Constituição Federal "trata da inviolabilidade da comunicação de dados, e não do sigilo dos bancos de dados" (Avolio, 2003, p. 173). Complementa que a comunicação de dados é colocada pelo legislador constitucional em nível de proibição absoluta, ressalvando, porém, que o sigilo dos bancos de dados é exceção à vedação da Constituição.

Ao criticar Damásio, Avolio (2003) atenta para a possibilidade de se interceptar telefones celulares que operam por rádio frequência, modalidade usual nos presídios brasileiros. Todavia, enfatiza que a Carta Magna deve ser interpretada restritivamente, ainda mais em se tratando de regras limitadoras das liberdades, aduzindo ainda que "interceptar dados escritos ou informatizados equivale a uma violação de correspondência, ou de um diário íntimo, que, atualmente, se afiguram instransponíveis pela dicção constitucional, salvo pela aplicação do princípio da proporcionalidade" (Avolio, 2003, p. 168).

Quanto à adoção do referido princípio, no caso concreto, Avolio não traz uma solução definitiva para o problema, direcionando-o ao magistrado, que dada a gravidade do fato, pode utilizar-se da intromissão nos meios de comunicação distintos da interceptação telefônica.

e) Vicente Greco Filho (2005) é incisivo ao defender a inconstitucionalidade do dispositivo legal, porque a Constituição somente autoriza a interceptação das comunicações telefônicas, ficando excluída a de dados e as telegráficas. Leciona que,

> [...] em nosso entendimento, é inconstitucional o parágrafo único do art. 1º. da lei comentada, porque não poderia estender a possibilidade de interceptação do fluxo de comunicações em sistemas de informática e telemática. Não se trata, aqui, de se aventar a possível conveniência de se fazer interceptação nesses sistemas, mas sim de interpretar a Constituição e os limites por ela estabelecidos à quebra de sigilo (Greco Filho, 2005, p. 17-18).

Antes, porém, explica que se pode interpretar a aplicação da ressalva "no último caso", circunscrita no inciso XII do art. 5º da Constituição Federal em duas situações, a saber: às comunicações telegráficas, de dados e das comunicações telefônicas, ou apenas às comunicações telefônicas. Argumenta

que, na primeira situação, o texto da constituição previu duas espécies de sigilo: "da correspondência, de um lado, e o dos demais sistemas de comunicação (telegrafia, dados e telefonia), de outro". Arremata aduzindo que, sendo assim, "a possibilidade de quebra de sigilo referir-se-ia à segunda situação, de modo que *ú*ltimo caso corresponderia aos três últimos instrumentos de transmissão de informações" (Greco Filho, 2005, p. 14-15).

A segunda situação, que o autor denomina de segunda hipótese interpretativa, o sigilo abarca quatro situações: a correspondência, as comunicações telegráficas, as de dados e as telefônicas. A ressalva "*último caso"* somente poderia ser aplicada para as comunicações telefônicas[39]. O autor interpreta os vocábulos do inciso XII do art. 5º do texto constitucional, ao especificar a respeito da redação "no último caso", colocado ali pelo legislador de forma expressa. Assevera que, "por outro lado, a garantia constitucional do sigilo é a regra e a interpretação a exceção, de forma que a interpretação deve ser restritiva quanto a esta (*exceptiora non sunt amplianda*)" (Greco Filho, 2005, p. 17).

O autor lista três razões para justificar seu entendimento de que a interpretação deve ser estendida, ao "último caso", apenas às comunicações telefônicas, quais sejam: a) o legislador foi direto ao utilizar-se da expressão "no último caso", que significa derradeiro, o que encerra; b) a garantia do texto constitucional é de que a interceptação é a exceção, enquanto o sigilo é a regra. A Constituição Federal apenas autoriza a interceptação das comunicações telefônicas, excluindo-se a de dados e as telegráficas; c) tecnicamente, a comunicação telefônica não pode ser equiparada como outros conteúdos de comunicação de dados, imagem, entre outros, porque a primeira se caracteriza como transmissão de voz entre os interlocutores.

Camargo Aranha (2004, p. 306), ao analisar a matéria, conceitua "*dados*" como sendo

> [...] elementos informativos coletados num aparelhamento de informática, de forma a serem aptos a um imediato processamento, conhecimento ou comunicação. São os conhecidos computadores que armazenam informações por *modems*, para pronto e imediato conhecimento, como também fazem sua comunicação por *e-mail* ou outro sistema assemelhado.

Após exposição do autor sobre o que sejam dados, ele os classifica em três espécies (bancos de dados públicos pertencentes aos órgãos públicos, bancos de dados de caráter público com informações terceirizadas e bancos de dados particulares). Posteriormente, divide o problema em dois focos: "os bancos de dados, que são os meios nos quais referidos dados repousam, e a possibilidade de sua interceptação quando transmitidos, quando em movimentação" (Aranha, 2006, p. 306).

Assim, interpreta a Carta da República de forma a contrariar a posição de Avolio (2003), no sentido de que os dados não podem, em nenhuma hipótese, ser violados. Nem quando estiverem armazenados em arquivos estanques, quanto mais à interceptação quando estiverem em movimento. Conclui ensinando que o texto constitucional protegeu de forma expressa o direito à intimidade, razão pela qual entende que os dados representam elementos integradores da intimidade da pessoa (Aranha, 2006).

---

39 O Ministro Marco Aurélio de Melo, do STF, na petição n. 577, em 25.03.92, entendeu que a inviolabilidade diz respeito apenas em dois casos (sigilo da correspondência e das comunicações telegráficas). Quanto aos dados e as comunicações telefônicas a inviolabilidade é relativa.

h) Ada Pellegrini Grinover, Antônio Scarance Fernandes e Antônio Magalhães Filho (2004) também têm o posicionamento de que a interceptação prevista no parágrafo único da Lei 9.296/1996 refere-se, exclusivamente, às interceptações telefônicas. *In verbis:*

> O parágrafo único do art. 1º., ao permitir a interceptação de ´fluxo de comunicações em sistemas de informática e telemática´ suscita questão de natureza constitucional. [...] Em sentido técnico, só pela telemática pode haver a comunicação do fluxo de dados via telefone, donde já se vê a impropriedade da referência da lei à informática. Mas, mesmo com relação à telemática, deve-se dizer que o texto constitucional só parece permitir a interceptação de `comunicação telefônica´ *stricto sensu* (ou seja, da voz), e não da ´comunicação via telefone´ (compreendendo a telemática). E como as regras limitadoras de direitos, sobretudo quando excepcionais, devem ser interpretadas restritivamente, poderia afirmar-se que a previsão de interceptação do fluxo de comunicações, tanto pela informática como pela telemática, é inconstitucional (Grinover *et al*, 2004, p. 218).

Diante do exposto, os doutrinadores entendem que somente as interceptações telefônicas podem ser realizadas mediante a prévia autorização judicial.

Com entendimentos contrários, citam-se três doutrinadores.

a) Paulo Rangel (2015) posiciona-se favorável à interceptação dos dados informáticos, porque a expressão "último caso" alcança o segundo grupo do inciso XII, do art. 5º da Constituição Federal (de dados e das comunicações telefônicas), estando protegido pelo sigilo o primeiro grupo (da correspondência e das comunicações telegráficas). Nesse diapasão,

> [...] a expressão "último caso" açambarcaria dados e comunicações telefônicas, pois do contrário, o legislador deveria ter dito: "sigilo das correspondências, das comunicações telegráficas, de dados e das comunicações telefônicas onde a expressão "último caso" teria como ponto de apoio somente a expressão isolada pela disjuntiva e. Porém, não foi esta a opção do legislador constituinte. Quis e permitiu a quebra do sigilo de dados sejam das comunicações telefônicas sejam outros dados de comunicação. A defendermos tese diferente estaríamos imaginando que o Constituinte somente se preocupou com a comunicação via telefone deixando de fora, a comunicação dos dados sem o uso de telefone. Ou seja, o criminoso via satélite ou da fibra óptica ou ainda o que utilizasse de infra vermelho estaria protegido diante da norma constitucional. Nada mais errado. É cediço que a interpretação literal de qualquer norma é a menos aconselhável e a pior possível. [...] A interpretação progressiva, bem como o princípio da atualidade devem ser chamados pelo intérprete da norma. Ou seja, há que se adequar a norma constitucional a realidade tecnológica atual (Rangel, 2015).

Não se pode concordar com o autor porque a norma constitucional, no que diz respeito às garantias individuais, deve ser interpretada restritivamente e, ainda, porque o princípio da atualidade deve ser imposto com cautela pelo magistrado, uma vez que a norma dificilmente acompanha as inovações tecnológicas, o que faz com que o legislador, nesta questão, fique em claro descompasso com a difusão da *Internet*.

b) Alexandre de Moraes (1997) defende a constitucionalidade do parágrafo único do art. 1º da Lei nº 9.296/1996 ao especificar que essa lei foi editada para regulamentar a determinação de interceptações telefônicas de qualquer natureza. No dizer de Moraes (1997), a violabilidade é possível, pois:

- a uma norma constitucional deve ser atribuído o sentido que maior eficácia lhe conceda, não podendo suprimir ou diminuir sua finalidade;
- a norma constitucional deve ter aplicação relativizada, a exemplo da admissão de gravação clandestina com autorização judicial, uma vez que as liberdades individuais não são absolutas;
- o simples fato de a ementa da lei especificar que regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal, não impede que a lei que veicule matéria diversa ao enunciado de sua ementa, somente por isso, ofenda postulado Constitucional (Moraes, 1997).

c) Marco Antônio de Barros (2002, p. 229) perfila na corrente da possibilidade de se interceptarem dados em sistema de informática e telemática, *in verbis*: "Defendo a violação do sigilo de dados, mediante autorização judicial, observadas todas as cautelas já mencionadas nos casos de sigilo da correspondência e das comunicações telefônicas".

Assevera o autor que a tipificação da conduta no art. 10 da Lei nº 9.296/1996 em considerar como crime a realização de interceptação do fluxo de comunicações em sistema de informática e telemática dá a entender que, a contrário *sensu*, se precedida de autorização judicial, é legal, sendo essa a tendência inovadora do legislador ordinário (Barros, 2002, p. 229-230).

A interpretação nos termos da Constituição tem duas formas: como princípio de interpretação e como técnica de controle de constitucionalidade. Quanto ao primeiro, estão presentes outros dois princípios que são o da supremacia constitucional (que lhe dá posição hierárquica superior em relação às demais normas)[40] e o da presunção da constitucionalidade (que tem a função de autolimitação da atuação jurisdicional). Quanto ao segundo, "consiste na expressa exclusão de uma determinada interpretação da norma, uma ação corretiva que importa em declaração corretiva de inconstitucionalidade sem redução de texto" (Barroso, 2003, 313-314).

Em termos técnicos, a interceptação telemática já é possível ser realizada mesmo com complexo aparato estatal em lidar com tecnologia avançada, como a Internet. Wendt e Jorge (2021) explicam que existe diferença entre interceptação telemática e afastamento do sigilo, o que gera interpretações equivocadas por parte do magistrado para o deferimento de uma medida cautelar. Segundo os autores, há casos que sequer haveria necessidade de se obter tais dados somente com a autorização judicial.

Interceptação telemática (em sentido estrito) refere-se ao monitoramento em tempo real do fluxo de comunicações. É como "ouvir" uma conversa enquanto ela acontece, mas aplicada ao ambiente

40 Para que haja harmonização no texto constitucional, o jurista pode se valer da eficácia interpretativa em que as normas de hierarquia inferior sejam interpretadas em consonância com as normas de hierarquia superior a que estiverem vinculadas. Diferentemente da eficácia negativa, que autoriza a declaração de invalidade das normas que estiverem em confronto com a Lei Maior. É a denominada revogação ou não recepção, no entendimento de Luis Roberto Barroso (2003).

digital. Por exemplo, acessar mensagens enquanto elas estão sendo digitadas e enviadas, ou monitorar a navegação de um usuário na internet no momento em que ela ocorre. Para isso, é necessária uma ordem judicial específica de interceptação, que deve cumprir os mesmos requisitos rigorosos de uma interceptação telefônica (necessidade da prova, ausência de outros meios e crime punido com reclusão, conforme a Lei nº 9.296/96).

Já o afastamento do sigilo de dados (ou requisição de dados armazenados) refere-se ao acesso a dados que já foram armazenados por provedores de conexão ou de aplicações de internet, como solicitar histórico de chamadas telefônicas já realizadas (metadados), conteúdo de e-mails já enviados e arquivados, ou mensagens de WhatsApp que já foram trocadas. Nesse caso, não há monitoramento em tempo real. O foco é nos dados passados.

A confusão entre esses dois conceitos leva a problemas práticos. Magistrados, por vezes, deferem "interceptações telemáticas" quando, na verdade, a polícia ou o Ministério Público buscam apenas o afastamento do sigilo de dados já armazenados.

Wendt e Jorge (2021) argumentam que, para o afastamento do sigilo de dados armazenados, nem sempre seria necessária autorização judicial específica nos moldes da Lei de Interceptações. Em muitos casos, a requisição administrativa direta (solicitada por autoridades policiais ou pelo Ministério Público) aos provedores de serviços, com base em outras legislações (como o Marco Civil da Internet – Lei nº 12.965/2014) ou com a justificativa da investigação, poderia ser suficiente para obter certos dados (como dados cadastrais ou registros de conexão que não revelem o conteúdo da comunicação).

Isso não significa que o conteúdo da comunicação armazenada (como o texto de um e-mail ou mensagem) possa ser acessado sem ordem judicial. O ponto de vista dos autores é que, para dados meramente cadastrais ou de conexão (metadados), que não violam o sigilo da comunicação em si, a necessidade de uma ordem judicial nos moldes da Lei de Interceptações (que é para o "fluxo" da comunicação) pode ser discutível.

Em suma, a tecnologia permite a interceptação telemática, mas a interpretação jurídica sobre o tipo de acesso necessário (se é monitoramento em tempo real ou acesso a dados armazenados) e a autorização exigida (se é judicial específica ou requisição administrativa para certos dados) ainda gera discussões e equívocos em diligências no sistema de justiça brasileiro.

5.3. O sigilo de dados, da informática e da telemática e a privacidade na rede

O sigilo dos dados, da informática e da telemática tem relação direta com a privacidade na *Internet*. A rede mundial de computadores tem a capacidade de gerar o perfil de uma pessoa em face da possibilidade de se acessar diversos bancos de dados, tais como: de instituições bancárias, de serviços de proteção ao crédito, administradoras de cartões de crédito, dentre outros.

Ensina Góis Júnior (2002, p. 103) que

> Dados tipológicos ou de identificação do nosso hipotético cidadão podem ser buscados no banco de dados do setor de identificação civil, enquanto que sua

> situação financeira pode ser conseguida nos bancos de dados da sua administradora de cartões, cruzados com os dados do banco onde mantém sua conta corrente com o SPC e SERASA. O banco de dados do departamento de veículos nos informa razoavelmente sobre os seus bens móveis assim como os arquivos da Receita e de cartórios podem ser acessados para precisar sua fortuna. A sua saúde pode ser razoavelmente avaliada comparando sua ficha no banco de dados do seu seguro-saúde, suas preferências cinematográficas com a sua vídeo-locadora e assim por diante.

Assim, a privacidade dos dados está ligada com o sigilo que lhe é inerente, sendo, pois, necessário diferenciar segredo de sigilo e conceituar estes institutos para, depois, averiguar a conexão entre eles.

O sigilo pode ser entendido como "o direito à intimidade, por sua manifesta amplitude, acolhe a preservação do segredo. Sucede que grande parte das questões a seguir ventiladas provém da proteção dada ao sigilo". Enquanto segredo "advém do latim, *secretum*, exprime o que se tem em conhecimento particular, só reserva, ou o que é oculto" (Barros, 2002, p. 224-225). Ou seja, o sigilo é o meio de que se dispõe para manter a integridade do desconhecimento de um fato.

Sigilo advém do "latim *sigilllu*, que significa segredo" (Ferreira, 1986, p. 1.583). É ainda "com maior rigor, o segredo que não pode nem deve ser violado, importando o contrário, assim, em quebra de dever imposto à pessoa, geralmente em razão de sua profissão, ou de ofício" (Silva, 1989, p. 231).

Dados são "elementos informativos coletados em um aparelhamento de informática, de forma a serem aptos a imediato processamento, conhecimento ou comunicação". E "banco de dados são os meios nos quais referidos dados repousam, e a possibilidade de sua interceptação quando transmitidos, quando em movimentação" (Barros, 2002, p. 224).

As denominações de informática e telemática já foram feitas nesta obra, dispensáveis, pois, que se repitam aqui, permitindo já o exame da relação do sigilo com a busca da verdade. Sobre as informações que permeiam a rede, os dados são de três espécies, quais sejam: de domínio público (o que não é protegido por *copyright*); de dados pessoais ou institucionais (dados sobre pessoas ou empresas disponibilizadas pelos titulares dos dados em cadastros, guias, currículos, etc.); e as confidenciais, que guardam semelhança às informações de uma correspondência tradicional (Góis Júnior, 2002, p. 100).

A Constituição Federal no art. 5º, inciso X, protegeu a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação. No inciso IV, garantiu a liberdade de manifestação do pensamento e a vedação ao anonimato, dando especial proteção à intimidade do indivíduo.

Daí decorrem duas situações: a primeira, de se saber se os dados que estão armazenados em arquivos de computador e outras mídias (antigos disquetes, *zip disks*, *CDs, pen drives, HD,* nuvem como *Google Cloud)* que tenham dados envolvendo a intimidade da pessoa podem ou não ter o sigilo violado; e a segunda, de se saber se esses dados, ao serem transmitidos na *Internet*, estão sob o manto da inviolabilidade constitucional.

Na primeira situação, desde que haja autorização judicial para a apreensão dos equipamentos e das mídias correspondentes, é perfeitamente aplicável o princípio da proporcionalidade, uma vez que o sigilo não é absoluto. Exemplo disso, é a violação do sigilo de dados referentes às informações financeiras ao ter um computador apreendido (Avolio, 2003).

Entendendo de maneira contrária, os dados em repouso e estocados no meio instrumental específico gozam de sigilo absoluto, porque a Constituição Federal não excepcionou o sigilo conforme preceitua o inciso XII do art. 5º, e porque a Lei Maior protege de forma expressa o direito à intimidade (Aranha, 2006).

Quanto à segunda hipótese, já foi dito que os dados em trâmite, ou seja, em trânsito, não podem ser violados mesmo sob ordem judicial, porque a parte final do dispositivo do inciso XII do art. 5º da Constituição Federal apenas permitiu a realização da interceptação de comunicações telefônicas, excepcionando os dados que estejam sendo transmitidos em sistema informático e telemático.

Todavia, como já posicionado, o que não se permite é a interceptação dos dados existentes em sistema informático e telemático, o que não impede que o sigilo seja violado mediante autorização judicial para que os dados sejam capturados por ordem de busca e apreensão.

5.4. A admissão do *e-mail* como prova nos crimes virtuais

O *e-mail* é uma das modalidades de se comunicar na *Internet.* Também conhecida como mensagem eletrônica, o *e-mail* constitui-se como nova forma barata e ágil de conversar com pessoas do mundo todo, em tempo real.

Castro (2003, p. 117) define *e-mail* asseverando que

> A expressão *eletronic mail* (*e-mail*) possui vários significados, podendo ser entendida como: correio eletrônico, endereço eletrônico e correspondência eletrônica. Utilizamos aqui, a última acepção da palavra, na qual o *e-mail* é uma troca de informações através da informática. É uma carta virtual digitada no computador e enviada por um programa específico.

Para que uma mensagem possa ser enviada e recebida com sucesso, via *e-mail*, faz-se necessário seu encaminhamento pelo remetente ao seu destinatário. Para tanto, é preciso que o usuário (remetente) faça uso de um computador equipado com *modem*[41] para acessar a rede e um programa de correio eletrônico, tal como o *Outlook Express da Microsoft*[42].

O destinatário deve ter um computador ou aparelho telefônico com internet que faça a conexão com o computador e/ou telefone do remetente. Além dos dois computadores ou aparelhos celulares para estabelecer a conexão, devem ter dois provedores (um provedor de origem e outro de destino), uma conta de *e-mail* no provedor de origem, uma conta no provedor de destino e a conexão entre o computador do remetente e o provedor de origem (Leitão Júnior, 2002).

41 *Modem* é um dispositivo que tem como função modular e demodular sinais e permitir transmissão de dados por um canal de comunicação de forma compatível.

42 *Outlook Express* é um programa gerenciador de *e-mail* em que se faz troca de mensagens assíncronas, de uso popular da empresa de Bill Gates da empresa americana *Microsoft. Nas* mensagens assíncronas, os sujeitos envolvidos se comunicam em tempo diverso, assemelhando-se ao correio tradicional, enquanto nas mensagens síncronas são instantâneas, como o telefone.

Segundo Leitão Júnior (2002, p. 55),

> O *e-mail* nasce com a sua feitura através de um programa, no qual se digita o texto da mensagem propriamente dita e informa-se o endereço do destinatário. Uma vez criado, é transferido, não é requisito para a sua existência o armazenamento de uma cópia sua no computador de origem.

Nesse contexto, é fácil verificar que além dos dois usuários da mensagem eletrônica (remetente e destinatário), outras pessoas terão conhecimento do inteiro teor das mensagens enviadas na rede, vulnerando a comunicação na *Internet.*

Como a *Internet* tem servido para a prática de vários tipos de ilícitos, os autores divergem sobre a admissibilidade do *e-mail* como prova porque é uma forma de comunicação insegura por percorrer uma longa trajetória, podendo sofrer, no percurso, alterações ou supressão de conteúdo.

Ora, se o texto ou arquivo percorre um longo caminho, como fazer para provar que houve prática de crime nessa trajetória? Como admitir essa prova se a mensagem pode ser adulterada no percurso?

A tarefa de responder a tais indagações não é das mais fáceis, tendo em vista o problema central que traça a possibilidade ou não de se interceptar sistema de informática e telemática nos termos da Lei nº 9.296/1996. Em primeiro lugar, cumpre esclarecer que a lei veda a interceptação de sistema de informática e telemática, interpretando-se a legislação ordinária em consonância com a unidade do texto constitucional.

Se concebermos que o *e-mail* faz parte do sistema telemático, da mesma forma não se poderia fazer a interceptação. Daí pergunta-se: o *e-mail* é uma informação informática ou um novo tipo de correspondência? A questão pode ser respondida nos termos dos arts. 1º e 2º da Lei nº 9.296/1996 ao não mencionar o conceito de fluxo de comunicações em sistemas de informática e telemática, deixando a entender que se refere a todo conteúdo que possa fluir por esse instrumento, inserindo o *e-mail* (Góis Júnior, 2002)[43].

Examinando essa hipótese, o *e-mail* não poderá ser interceptado, porque será aferida como prova ilícita, tendo em vista que é vedado pela carta da república interceptar sistemas de informática e telemática. Se for considerado como correspondência, também não poderá ser interceptada, em face da proibição de violação de correspondência prevista na primeira parte do inciso XII do art. 5º da Constituição Federal e art. 151 do Código Penal.

Nesse caso, a correspondência não poderá ser violada, porque "correspondência é toda comunicação interpessoal realizada por meio capaz de transmitir o pensamento". Assim, engloba, além da carta, comunicação telefônica e telegráfica, rádio e outras formas de comunicação. O sigilo deve ser estendido ao inteiro conteúdo dos *e-mails* porque é uma espécie de correspondência que deve ser tutelada nos moldes do art. 151 do Código Penal brasileiro (Regis do Prado *apud* Silva, 2003, p. 111).

---

43 Em julgamento ao processo de n. 13.000613/2000, TRT da 10ª Região, o Juiz José Leone Cordeiro Leite da 3ª Vara do Trabalho proferiu o seguinte entendimento: "Não se diga que a correspondência eletrônica (e-mail) não está abrangida pelo termo "correspondência" de que trata o inciso XII do art. 5 da CF, pois a lei nesse caso não fez discriminação, não cabendo ao intérprete fazê-lo".

Dessa ideia não se poderá compactuar, porque o art. 10 da Lei nº 9.296/1996 é regra especial em relação ao art. 151 do Código Penal. Melhor é a solução apontada por Carla Rodrigues Araújo de Castro (2003, p. 22) que, sem maiores delongas, explica que "da análise das duas normas observa-se que a prevista no artigo 10 da Lei nº 9.296/1996 é especial em relação à do CP, uma vez que cuida das comunicações feitas através da informática".

Wendt e Jorge (2021) afirmam que é permitida a interceptação de *e-mails* e que a autoridade policial pode receber em tempo real na investigação o espelhamento das mensagens enviadas pelos criminosos, desde que haja autorização judicial. Esse espelhamento permite que o policial monitore todos os acessos e veja fotos, vídeos e textos que são trocadas pelos usuários.

Todavia, rebatendo a segunda parte do entendimento de Castro, perderia a finalidade de ter todo o trabalho de buscar e apreender o computador, nas vias legais, e não poder ter acesso ao conteúdo dos *e-mails*. Ademais, o Código de Processo Penal alinhava vários outros meios de prova que devem ser considerados pelo magistrado. Não se pode considerar como uma confissão um texto escrito via *e-mail* pelo acusado, sem que essa prova tenha sido analisada em conjunto no bojo probatório dos autos.

No posicionamento de Amaro Moraes e Silva Neto (2001), para que essa confissão eletrônica tenha valor probatório, deve ser submetida ao crivo de um perito para constatação da veracidade, já que se trata de crime *delicta facta permanentia* ou que deixam vestígios.

Por outro lado, é de se ponderar que o *e-mail* pode ser considerado como documento, porque, se contiver uma assinatura digital, essa assinatura poderá ser conferida no meio eletrônico, via certificado digital. Corroborando com esse raciocínio,

> Toda cópia do documento eletrônico terá sempre as mesmas características do original e, por isso, deve ser assim considerada. É o caso até de dizermos que não existe um original e não existem cópias nem vias do documento eletrônico, enquanto ele for mantido nesta forma. Se pensarmos, porém, que um documento eletrônico pode ser reproduzido em meio físico, e vice-versa, neste caso é possível falar-se em original e cópia. Se o documento for originalmente elaborado e assinado em meio eletrônico, é de se considerada original a mesma sequência de *bits*, qualquer que seja o meio em que esteja armazenada; mas podemos falar em cópia do documento eletrônico, quando esta sequência de *bits*, traduzida pelo programa de computador, for impressa sobre o papel. Neste caso, o papel é a cópia e o arquivo eletrônico com assinatura criptográfica é o original. Eventual alegação de desconformidade entre o original e a cópia demandará análise do documento eletrônico, com o uso de um computador e de *softwares* específicos que leiam este arquivo eletrônico e reconheçam a assinatura (Marcacini, 2005, s/p).

Para a conferência da assinatura, faz-se necessário o uso do Certificado Digital, documento eletrônico de identidade com validade jurídica e assinado digitalmente por uma Autoridade Certificadora (AC)[44]. O certificado digital contém informações sobre emissor e seu Titular, tais como: chave pública do titular; nome do titular; endereço de e-mail; nome da AC que emitiu o certificado, data de vencimento do certificado etc.[45]

44 No modelo ICP – Infraestrutura de chave pública, também conhecida como *PKI* (*Public Key Infrastructure).* Existem determinadas autoridades que possuem funções específicas com o objetivo de certificação de outras entidades, entre elas: Autoridade Certificadora Raiz, Autoridade Certificadora e Autoridade de Registro. Para melhor entender o assunto, o arcabouço legislativo pode ser conferido no sítio do ITI: http://www.iti.gov.br ou no sítio do ICP-Brasil: https://www.gov.br/iti/pt-br/assuntos/certificado-digital. Acesso em: 18 maio 2025.

45 A Certificação Digital é um conjunto de processos regidos pela Medida Provisória n. 2.200-2, de 24/8/2001, que instituiu a Infraestrutura de Chaves

São várias as funções do certificado digital, entre elas a verificação da identidade correspondente do correio eletrônico, acesso remoto aos sistemas de informação, verificação da identidade dos cidadãos ou outras entidades legais, proteção de identidade do *software*, proteção da identidade de documentos e garantia da segurança das transações eletrônicas, entre elas o *e-mail*.

O *e-mail* também pode ser transmitido e arquivado no disco rígido do computador, que poderá ser utilizado como prova, caso seja admitido como documento que possa ser apreendido e buscado (Avolio, 2003, p. 215).

A doutrina está dividida quanto à admissibilidade do *e-mail* como prova. No Brasil, temos duas correntes que admitem. Na primeira, de forma indireta, podem ser citados: Amaro Moraes e Silva Neto, Ângela Bittencourt Brasil, Leonardo Gurgel e Carlos Pires. A segunda, na forma direta: Maria da Conceição Barreto Gonzalez, Patrícia Regina Pinheiro Sampaio, Carlos Affonso Pereira de Souza, José Caldas Góis Júnior e Luiz Francisco Torquato Avolio. *In verbis*: [...] "para se provar a efetiva existência de um e-mail e de sua necessária integridade original, necessária se faz uma perícia no local onde ela se originou, qual seja, no computador remetente" (Silva Neto, 2001, s/p).

Comungando do mesmo posicionamento de Avolio (2015), Ângela Bittencourt (1996, p. 60) sinaliza que

> [...] A perícia judicial deve ser *prima facie* ser feita na máquina do remetente da mensagem e para isso é preciso que haja uma ordem judicial de busca e apreensão de natureza cautelar para averiguar-se se encontra em seus arquivos o objeto da investigação, ou seja, os *e-mails* arquivados e assim mesmo, se o investigado tiver sido apagado, será quase impossível a verificação de sua existência. Então, caso a mensagem tenha sido apagada, vai-se ao administrador com a ordem judicial para que este entregue o texto do *e-mail* enviado, desde que este seja nacional.

Observa-se do ensinamento da autora que, além da dificuldade de se interceptarem mensagens eletrônicas, o mundo cibernético não possui fronteiras. Nesse espaço sem limites, um juiz no Brasil dificilmente logrará êxito em pedido da acusação de obter informações de administradores de outros países, mesmo que o faça por meio de carta rogatória.

O *Hotmail*[46] é um dos provedores mais usados e conhecidos no mundo todo, e mesmo que se consiga ter acesso aos arquivos de administrador de outros países, uma terceira dificuldade tem sido motivo de ver fracassada a prova de crimes transnacionais em virtude dos *nicks*[47] utilizados no meio digital (Bitencourt, 2020).

Todavia, localizando os arquivos do usuário destinatário, o perito comprovará materialidade e autoria com a pesquisa no IPs[48] por onde ele tenha transitado.

Públicas Brasileira (ICP-Brasil) e que garantem as pessoas mais segurança durante a realização das transações eletrônicas. Com essa certificação, o cliente pode ficar sabendo quem é o autor de uma transação ou de uma mensagem, manter dados confidenciais protegidos e ainda armazenar documentos sem que ninguém possa ter acesso a eles.

46 *Hotmail* é uma administradora de provedores de serviços de *e-mail* da *Microsoft*.

47 *Nicks* ou *nicknames* são apelidos usados pelos internautas para não serem identificados e permanecerem no anonimato. Conforme já dito em outro capítulo, é um dos empecilhos que trava a descoberta a autoria de usuário na rede mundial de computadores.

48 IPs ou IP significa *Internet Protocol*.

O *e-mail* pode ser considerado como prova direta ou servir de suporte para outros meios probantes. Como prova direta, menciona a confissão por *e-mail* na esfera do direito comercial, que servirá como prova direta de negócios firmados na rede, e pode ser acatado como documento porque o conteúdo pode ser impresso e assinado pelo interessado. Admite que a prova testemunhal por *e-mail* pode ser considerada, uma vez que não existam outros meios de se provar determinado fato (Gurgel; Pires, 2002).

Nesse sentido, o Superior Tribunal de Justiça, apreciando pedido de trancamento de Inquérito Policial, negou recurso em *Habeas Corpus*, ao entender que a quebra do sigilo dos dados cadastrais do acusado junto à provedora de acesso à *Internet* não configura constrangimento ilegal porque havia sido precedida de autorização judicial ao ser feita a interceptação em conversa de *Chat* na *web*[49].

Entrementes, pode-se concordar com Pires quanto à prova apenas no aspecto cível, porque na esfera criminal admitir essa prova na via direta é retirar do acusado, muitas vezes, ainda indiciado, garantias mínimas, entre as quais de estar submetido ao devido processo legal.

Combatendo sua argumentação e reconhecendo a fragilidade dessa prova, Gurgel e Pires (2000, p. 48) arrematam que

> Questão problemática é a de se verificar que determinada pessoa mandou um *e-mail* a outra, sendo que o emissor apagou todos os rastros de seu ato, como poderia ser ele acusado pela emissão, pois uma inspeção em seu computador não encontraria nenhum vestígio? Basicamente a prova seria mais pericial e testemunhal, dá-se o exemplo de pessoa que presenciou o envio, no caso da prova testemunhal, ou o perito consegue rastrear através do provedor os acessos ou de programas específicos capazes de desfazer ações desse tipo deletar[50] ou formatar[51] em um determinado computador, a exemplo do *´unformat´* comando para restaurar dados formatados.

Na concepção de Wendt e Jorge (2021), o teor de um texto extraído de um *e-mail* pode ser considerado como uma modalidade de documento quando houver a ocorrência de dois requisitos, quais sejam a impossibilidade de alteração de seu conteúdo e a identificação fiel das partes, o qual sugere a implementação de uso da assinatura digitalizada[52] e da criptografia[53].

---

49 RHC n. 18116-SP (STJ-6a. Turma, RHC 18116-SP, rel. Min. Hélio Quaglia Barbosa, em notícias do site do STJ de 24.02.06).

50 Deletar significa excluir do texto ou arquivo, apagar.

51 Formatar, no conceito de Aurélio Buarque de Ferreira (1986, p. 800), é estabelecer a disposição dos dados em um arquivo ou registro indicando a ordem, o cumprimento ou a disposição destes.

52 A assinatura digital é defendida por outros autores como uma forma de se conferir autenticidade a um documento emitido na via eleita, a *Internet*, e de facilitar o comércio eletrônico já sendo realidade no Brasil. Cf. *site* do ICP-Brasil.

53 A criptografia pode ser entendida como uma ferramenta de codificação utilizada para envio de mensagens seguras em redes eletrônicas, no entender de Peck, 2002, p. 86. Como exemplos da legislação brasileira sobre certificadoras e criptografia temos: Instrução Normativa SRF n. 156, de 22 de dezembro de 1999, que instituiu os certificados eletrônicos da SRF; Decreto n. 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal; Decreto n. 3.585, de 5 de setembro de 2000, que institui regras para documentos que só serão recebidos pela Casa Civil da Presidência em formato eletrônico a partir de 1º. de janeiro de 2001; entre outros. (fonte extraída da obra de Peck, 2002, p. 87). "Da minha leitura, no inciso XII da Lei Fundamental, o que se protege, e de modo absoluto, até em relação ao Poder Judiciário, é a comunicação 'de dados' e não os 'dados', o que tornaria impossível qualquer investigação administrativa, fosse qual fosse." (MS 21.729, voto do Min. Sepúlveda Pertence, DJ 19/10/01).

A UNCITRAL (*United Nations Commission on International Trade Law)*, Resolução 51/162 da Assembleia Geral das Nações Unidas – ONU, de Nova York, de 16 de dezembro de 1996, tem diretriz regulamentadora do comércio eletrônico, reconhecendo o uso de tecnologias de encriptação para conferir ao documento eletrônico mesma validade e grau de segurança dos documentos escritos, tendo a mesma validade em relação ao valor probante.

Da segunda corrente, extrai-se que o *e-mail* pode ser considerado como prova condicionando-se a autenticidade de sua autoria, por força da fragilidade e da vulnerabilidade de sua integridade. Logo, pode ser usado como meio de prova, se existir uma assinatura digital ficando, portanto, protegido contra modificações no seu teor.

Wendt e Jorge (2021, p. 85-86) explicam que o *e-mail* geralmente é levado impresso pelas vítimas até a delegacia de polícia para que a autoridade policial possa investigar a autoria do fato e a infração penal cometida. Nesse caso, é preciso identificar a origem do *e-mail* que deve ser feita com o acesso ao código-fonte buscado na parte do cabeçalho do *e-mail* chamado "Received". É no "Received" que se "identifica o computador de onde partiu a mensagem". Os autores explicam que alguns provedores não facilitam essa identificação, a exemplo do Gmail, exigindo-se ordem judicial para que o Google informe os dados da conta, IPs do usuário de origem.

Analisando as duas correntes, depreende-se da majoritária que o *e-mail* pode ser admitido como meio de prova, desde que submetido à perícia judicial, por meio de autorização judicial de natureza cautelar de busca e apreensão dos equipamentos onde possa ser localizado. Já a corrente minoritária entende que o *e-mail* pode ser considerado como prova em ação criminal mediante simples constatação de certificação digital.

No STJ, em julgamento do REsp 1.381.603/MS, decidiu-se que o *e-mail* é capaz de ser aceito como prova desde que o magistrado se convença da verossimilhança das alegações e da idoneidade das declarações contidas nos autos. O ministro relator, Luiz Felipe Salomão, ponderou que o uso de certificação digital para a assinatura eletrônica confere maior credibilidade ao *e-mail* ao ser aceito como meio de prova[54].

5.5. Responsabilidade dos provedores

Da problemática apresentada, percebe-se a dificuldade da obtenção das informações contidas em arquivo de computador, de usuário que esteja sendo investigado e que as tenha apagado (deletado). Todavia, além do computador do remetente e do destinatário, as informações ficam gravadas no arquivo de seus respectivos provedores[55].

Provedor, ou mais comumente chamado de provedor de acesso, pode ser definido como

54. STJ/Resp: 1.381.603/MS 2013/0057876-1, Relator: ministro Luis Felipe Salomão, data de julgamento: 06/10/2016. Quarta Turma, publicado no DJE em 11/11/2016. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201300578761&dt_publicacao=11/11/2016 Acesso em: 9 jun. 2025.

55 Como exemplo de provedores temos vários: UOL,Vivo, Claro.

> [...] uma empresa prestadora de serviços de conexão à *Internet* e de serviços de valor adicionado como hospedagem, que detém ou utiliza uma determinada tecnologia, linhas de telefone e troncos de telecomunicação próprios ou de terceiros (Peck, 2002, p. 52).

As características jurídicas da dupla atuação dos provedores de acesso, (empresas prestadoras de serviços e aglutinadoras do mundo virtual), são duas: como prestadoras de serviços, são responsáveis pela transmissão de mensagens e conteúdos na rede e, como aglutinadoras do mundo virtual, são editores responsáveis pela hospedagem, publicação e produção do conteúdo na *Internet* (Peck, 2002).

Podem ser citadas como características dos serviços, no entender de Peck (2002): custo, competência técnica, confiabilidade no quesito segurança, capacidade e quantidade de linhas disponíveis proporcional ao número de usuários.

Estudando tais características, verifica-se que os provedores de acesso à *Internet* são espécies de empresas de telecomunicações, com peculiaridades que lhe são inerentes, como segmento misto nos serviços de telecomunicações, constituindo-se como serviço de valor adicionado. Peck (2002, p. 53) destaca que

> É importante ressaltar que a *Internet,* como qualquer rede, é acessada. Todo o conteúdo que está na *Internet* é acessado, ou seja, não existe uma materialização física dele para transportar seus direitos, como ocorre com livro, filme ou CD. Não existe o pedido de uma identificação (como a cédula de identidade) para que se entre em uma área pornográfica ou de acesso restrito a maiores de idade, como ocorre nas casas noturnas e discotecas. Mas existe a tecnologia. A *Internet* funciona como uma rede orgânica onde os responsáveis pelas portas de entrada e saída têm como autorizar o acesso, restringir o acesso, identificar o usuário em seu banco de dados, entre outras informações.

A questão que se coloca é a de responsabilidade direta dos provedores e a responsabilidade de informar dos provedores. A primeira hipótese ocorre quando o usuário insere, em uma *homepage,*[56] imagens de crianças contendo cenas pornográficas, sendo também o provedor responsável criminalmente pelo fato praticado por terceiro.

Ou seja, ainda não existe um meio eficaz de se fazer uma filtragem fiscalizadora do que se faz e se produz na *Internet*. Assim, não há de se falar em responsabilidade direta e imediata dos provedores de acesso à *Internet*.

Quanto à responsabilidade de informar dos provedores, é unânime o entendimento de que, mediante ordem judicial, os provedores de acesso têm obrigação de fornecer as informações armazenadas em seus arquivos. São informações importantes porque funcionam como meio de prova para demonstração de materialidade e autoria de ilícitos praticados na rede[57].

56 *Homepage* pode ser definida como a página de entrada ou página principal de um *website*. É nessa página que estão os *links* para as demais páginas do *website*.

57 Nesse sentido o Mandado de Segurança n. 1.0000.04.414635-5/000(1) impetrado em Minas Gerais, que teve a seguinte ementa: Mandado de Segurança - Crimes contra a honra praticados pela *Internet* – requisição de ordem judicial para que o provedor forneça a identificação de determinadas contas de *e-mails.* Rel. Paulo César Dias – 3ª. Câm. Crim. (TJ-MG).

Todavia, sem autorização judicial, os provedores não têm obrigação de entregar informações contidas em seus arquivos. Tais informações, muitas vezes, são de cunho privativo, confidencial, e estão protegidas constitucionalmente pelo princípio da inviolabilidade das correspondências.

Entretanto, a relação existente entre provedor de acesso à *Internet* e usuário é contratual e, geralmente, onerosa. Como já visto no Capítulo 2, os usuários pagam uma taxa mensal. Daí a necessidade de se regular essa relação, ou de, pelo menos, os provedores informarem (mesmo que seja via *e-mail*) os limites de sua atuação no meio virtual.

Os *disclaimers* revelam nova forma de se captar a vontade do usuário, de aderir às normas digitais capazes de controlar abusos cometidos e de aplicar penalidades ao infrator. No dizer de Peck (2002), *disclaimers* são declarações que as empresas provedoras de acesso à *Internet* utilizam para restringir o grau de responsabilidade delas em relação às informações lançadas no meio digital pelo usuário.

Para regular tais serviços, o ideal é que a regulamentação seja realizada, em âmbito internacional, por meio de um Código de Ética, Padrões e Procedimentos, e pela aplicação de um programa de computador (*software*) para bloquear conteúdos inaceitáveis no ambiente cibernético. Ao contratar uma empresa provedora de acesso à *Internet*, as cláusulas devem ser claras para informar quem é responsável pelo editorial do conteúdo a ser publicado na grande rede (Peck, 2002).

Na prática, quando alguém comete um delito utilizando a *Internet*, o juiz solicita ao provedor de acesso a identificação do IP do usuário para que se possa identificar o autor da infração penal. Essa identificação é uma forma de trazer aos autos a autoria de crimes difíceis de provar em face do meio cibernético em que é praticado.

No Brasil, a Associação Brasileira dos Provedores de Acesso, Serviços e Informações (ABRANET) firmou um Termo de Acordo com vinte e cinco provedores de Brasília, tendo os signatários se comprometido a incluir em sua *homepage* um ícone de acesso à página da Procuradoria da República do Distrito Federal, o que proporciona ao internauta denunciar, eletronicamente, ilícitos relacionados à pedofilia na rede.

Os provedores signatários se comprometeram ainda em se esforçarem no que se refere à identificação do usuário no momento de seu cadastramento e em registrar de forma detalhada toda e qualquer conexão realizada com os computadores de seus clientes, facilitando o trabalho da polícia judiciária quanto à identificação do usuário para comprovação da materialidade e autoria.

Outro ponto importante a ser debatido é a responsabilidade de informar dos provedores quando o assunto é o armazenamento das informações em seus arquivos. Os provedores guardam, em média, por 90 (noventa) dias, as informações que são preciosas em uma investigação criminal de crime cometido na *Internet.*

Essa questão é agravada quando os provedores têm sede em outros países e a Polícia Federal necessita de ordem judicial para ter acesso às informações das empresas provedoras. O procedimento é moroso, difícil e, na maioria das vezes, inexitoso.

A situação é fundamental porque, mesmo com a expedição de Carta Rogatória, os provedores do exterior não estão obrigados a cumprir ordem emanada do Brasil e, quando uma ordem chega a ser cumprida, a morosidade é tamanha que os dados já se perderam.

Pelo que se percebe, há preocupação de se regular os serviços oferecidos na rede com o fito de se estabelecer regras para facilitar o uso e permitir maior segurança ao usuário.

Até que se estabeleçam novas regras, as Companhias Telefônicas brasileiras devem atender a uma ordem judicial, e as provedoras de acesso à *Internet* devem informar o que determinar a ordem para coibir práticas abusivas e ilícitas ilimitadas na grande rede.

No Brasil, o Marco Civil da Internet, Lei nº 12.965/2014, trouxe delimitações aos provedores e estipulou responsabilidade dos provedores. Provedores de Conexão à Internet (ISPs) são empresas que fornecem o acesso à internet (como as operadoras de banda larga). A responsabilidade desses provedores é limitada. De acordo com o art. 18 do Marco Civil, eles não são responsabilizados civilmente por danos decorrentes de conteúdo gerado por terceiros. Isso significa que eles não são responsáveis pelo que os usuários publicam ou acessam na internet.

Provedores de Aplicações de Internet (Plataformas Digitais) são empresas que oferecem serviços online, como redes sociais, plataformas de vídeo, e-commerce, entre outros (exemplos: Facebook, Google, YouTube). A responsabilidade desses provedores é mais complexa e tem sido objeto de debates e decisões judiciais recentes, inclusive do Supremo Tribunal Federal (STF). Em geral, o Marco Civil da Internet (art. 19) estabelece que os provedores de aplicações de internet somente poderão ser responsabilizados civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomarem as providências para tornar indisponível o conteúdo que infringe as regras. No entanto, o STF (2025) tem definido parâmetros mais detalhados para essa responsabilização, como exposto a seguir.

a) Crimes contra a honra: nesses casos, os provedores só podem ser responsabilizados se descumprirem uma ordem judicial para a remoção do conteúdo. Contudo, as plataformas podem remover publicações com base em notificação extrajudicial. Se um conteúdo ofensivo já reconhecido judicialmente for replicado, os provedores devem remover as publicações idênticas com base em notificação judicial ou extrajudicial, sem a necessidade de novas decisões.

b) Crimes graves: para conteúdos que configuram crimes graves (como tentativa de golpe de Estado, terrorismo, instigação à mutilação ou suicídio, racismo, homofobia, crimes contra mulheres e crianças), a responsabilização pode ocorrer se houver falha sistêmica do provedor em adotar medidas adequadas de prevenção ou remoção, em violação do dever de atuar de forma responsável, transparente e cautelosa.

c) Conteúdo remunerado ou com interferência na distribuição: o STF também tem apontado que as plataformas podem ser responsabilizadas quando remuneradas por determinado conteúdo ou quando há nível relevante de interferência na distribuição desse conteúdo. Isso porque, nesses casos, a plataforma se torna, de alguma forma, "sócia" do conteúdo veiculado.

O Supremo Tribunal Federal (STF) concluiu o julgamento dos Recursos Extraordinários (RE) 1.037.396 (Tema 987) e RE 1.057.258 (Tema 533), que tratavam da constitucionalidade do art. 19 do Marco Civil da Internet (Lei nº 12.965/2014). A decisão principal foi a declaração de parcial inconstitucionalidade do art. 19, estabelecendo novos critérios para responsabilização dos provedores de aplicações de internet (plataformas digitais como redes sociais e serviços de vídeo) por conteúdos gerados por terceiros. Em resumo, o STF decidiu que:

a) para crimes contra a honra (calúnia, injúria, difamação), a remoção de conteúdo ainda exige ordem judicial, mas as plataformas podem remover publicações baseadas em notificação extrajudicial. Se um conteúdo já reconhecido judicialmente como ofensivo for replicado, a remoção pode ser feita por notificação judicial ou extrajudicial;

b) para crimes graves (ex.: terrorismo, racismo, crimes contra crianças, atos antidemocráticos), a responsabilização pode ocorrer mesmo sem ordem judicial prévia, se houver falha sistêmica da plataforma em adotar medidas preventivas ou de remoção. A notificação extrajudicial é suficiente para que as plataformas tenham o dever de agir;

c) em relação a conteúdos pagos ou impulsionados, as plataformas podem ser responsabilizadas quando remuneradas por um conteúdo ilícito ou quando há interferência relevante na sua distribuição (como impulsionamento), exigindo ação imediata para a remoção;

d) quanto aos deveres adicionais, as plataformas devem implementar autorregulação obrigatória, canais de atendimento acessíveis e ter representação jurídica no Brasil;

e) provedores de e-mail e mensageria pessoal continuam protegidos pela regra original do art. 19, dependendo de ordem judicial para remoção (STF, 2025).

5.6. Elaboração do laudo pericial tendo outros meios de provas como ponto de partida no crime virtual e/ou digital

De todos os meios de provas alinhavados, vê-se que alguns levam à produção de prova pericial porque os crimes praticados na *Internet*, como já dito, são daqueles que deixam vestígios, razão pela qual surge a necessidade de estar a acusação alicerçada em laudo pericial para demonstrar a materialidade do ilícito.

Assim, a necessidade de se estudar o termo perícia, que advém do vocábulo latino *peritia,* que quer dizer habilidade, saber, capacidade. O conceito de habilidade evoluiu com o tempo, significando ação de alguém com saber especializado (Aranha, 2006).

Diferentemente dos *delicta facta transeuntes*, crimes que não deixam vestígios, os *delicta facta permanentia* deixam vestígios e necessitam de exame pericial para se averiguarem todos os detalhes e se estabelecer a certeza da materialidade do delito. Pode-se exemplificar na primeira categoria os crimes de calúnia, difamação e injúria, na forma verbal previstos nos arts. 138, 139 e 140 do Código Penal Brasileiro. Na segunda categoria, todas as infrações que deixarem vestígios.

O art. 158 do Código de Processo Penal estabelece: "quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado".

O exame de corpo de delito direto se faz por meio de inspeção direta do perito, e o indireto, por meio de prova testemunhal, quando os vestígios tiverem desaparecido do universo fático probatório.

Se o acusado for processado, e nos autos não constar o laudo pericial, poderá se pleitear a nulidade processual em sede de preliminar, ante a ausência do exame, que o legislador a erigiu à categoria de nulidade insanável (Tourinho Filho, 2002).

É preciso que se diferencie o corpo de delito do exame de corpo de delito. Enquanto o corpo de delito "é o conjunto de vestígios materiais deixados pela infração penal, a materialidade do crime, aquilo que se vê, apalpa, sente, em suma, pode ser examinado através dos sentidos", o exame de corpo de delito "é um auto que se descrevem as observações dos peritos" (Mirabete, 2025, p. 271). Enquanto o corpo de delito se comprova via perícia, o laudo registra a existência do próprio delito.

Na verdade, o perito é um longa *manus* do magistrado. Em assuntos que envolvem matéria altamente especializada, o perito emite juízo de valor. Os crimes cometidos na rede mundial de computadores, por se tratar de matéria nova e envolverem infindáveis tipos de mídia, deixam vestígios, daí surge a necessidade de se colacionar aos autos o laudo pericial. A natureza jurídica da perícia é instrumental, técnico-opinativa e alicerça a sentença do juiz (Aranha, 2006).

A perícia fornece o diagnóstico e às vezes o prognóstico. Nos crimes virtuais, o perito verifica como o criminoso estava agindo (utilizou-se de mídia para praticar o crime) e pode sugerir como prognóstico medidas de segurança para a vítima (Camargo Aranha, 2006).

O Código de Processo Penal prevê necessidade de se resguardar em primeira mão todos os elementos que tiverem relação com o crime, devendo a autoridade policial tomar todos os cuidados nesse sentido.

Os incisos I, II, III e VII do art. 6º do Código de Processo Penal, com a redação dada pela Lei n. 8.862, de 28 de março de 1994, confirma a preocupação do legislador. Esse dispositivo está inserido no Título II, do Livro I, que trata do Inquérito Policial.

Na fase procedimental de investigação, em regra geral, quem toma conhecimento do fato é a autoridade policial. Assim, logo que tiver conhecimento da prática da infração penal, o Delegado de Polícia deve dirigir-se ao local do crime para diligenciar a manutenção do estado e conservação das coisas, até que os peritos criminais possam chegar ao local. Esse inciso tem aplicação imediata, por exemplo, em crimes de homicídio, furto e roubo em que houver arrombamento. *In verbis*:

> Tal providência é importante em vários delitos (homicídio, roubo, furto, etc.,), para que se possa efetuar o exame do lugar e outras diligências (colheita de impressões digitais, exame de manchas, etc.,) que podem revelar provas ou indícios úteis à elucidação do fato (Mirabete, 2025, p. 87).

O art. 6º é complementado pelo art. 169, ambos do Código de Processo Penal, ao tratar do exame do corpo de delito e das perícias em geral, previsto no Capítulo II, Título VII.

Segundo a redação do art. 169, a autoridade, que poderá ser policial ou judicial, deverá diligenciar imediatamente para que não se altere o estado das coisas até a chegada dos peritos no local do crime. Menciona, ainda, que os peritos poderão (faculdade) instruir os laudos com fotografias, desenhos ou esquemas elucidativos.

No inciso II, a redação surpreende: "apreender objetos que tiverem relação com o fato, após liberados pelos peritos criminais". Ora, *in casu*, os objetos não poderão ser descartados, porque, se houver necessidade de perícia complementar ou renovação de perícia, deverão estar à disposição do juízo. Tais objetos podem ser exemplificados como a arma que matou a vítima ou o pé de cabra que arrombou a porta da casa do ofendido.

O art. 91, inciso II, "a", do Código Penal reconhece a perda em favor da União dos instrumentos do crime, desde que consistam em coisas cuja fabricação, alienação, uso, porte ou detenção constituam fato ilícito.

O inciso III tem o cunho de acautelar todas as provas que servirem para o esclarecimento do fato e suas circunstâncias, uma vez que impõe a coleta. O legislador não especificou que provas seriam essas, deixando à escolha da autoridade policial. Todavia, o poder discricionário do Delegado não pode ofender as garantias previstas na Carta da República na ânsia de ver desbaratada organização criminosa ou de desvendar determinado fato. A autoridade pode, segundo o inciso III, colher declarações da vítima e do (suposto) autor da infração, ouvir testemunhas etc.

O inciso VII trata sobre o procedimento do exame de corpo de delito e quaisquer outras perícias para se fornecer ao órgão da acusação elementos suficientes para formação da *opinio delicti.* Porém, algumas ações penais têm sido propostas sem a presença do laudo pericial, uma vez que o art. 156 reconhece que pode ser juntado até a apresentação das alegações finais.

Daí se depreende que não existe um momento certo e específico para que se proceda à prova pericial. O art. 160, parágrafo único, do Código de Processo Penal, estipula o prazo de dez dias para que o laudo pericial seja elaborado, podendo, a requerimento dos peritos, e em casos excepcionais, ser prorrogado. Entretanto, a lei não estabeleceu qual o lapso temporal da prorrogação e não deixou claro quanto ao número de vezes que o prazo pode ser prorrogado.

O realce legal é que o laudo seja juntado atempadamente nos moldes do art. 156 do Código de Processo Penal e que sirva como base para demonstrar materialidade e autoria.

Todavia, nos crimes regidos pela Lei nº 9.609, de 19 de fevereiro de 1998, a denominada Lei do *Software*, o laudo pericial é condição de procedibilidade para o recebimento da queixa-crime. Trata-se de crime de ação penal de iniciativa privada, em que cabe à vítima, ou seu representante legal, providenciar a colheita da prova mediante a propositura de ação de produção antecipada de provas ou de ação de busca e apreensão dos *softwares* para que seja elaborado laudo pericial. Após a homologação do laudo, a vítima tem 30 dias para propor a ação penal, sob pena de preclusão, conforme redação dos

arts. 524 e seguintes do Código de Processo Penal, que tratam do processo e do julgamento dos crimes contra a propriedade imaterial.

A Lei nº 10.695, de 1º de julho de 2003, acrescentou ao art. 530 do Código de Processo Penal, mais nove artigos, sendo art. 530-A até o art. 530-I, disciplinando melhor a matéria, tendo em vista a dificuldade de outros meios de prova interferirem na elaboração do laudo pericial.

Em síntese, quando houver busca e apreensão, na hipótese do art. 184 do Código Penal, a autoridade policial procederá à apreensão dos bens ilicitamente produzidos ou reproduzidos em sua totalidade, juntamente com os equipamentos, suportes e materiais que possibilitarem a sua existência, desde que se destinem à prática de crime.

É uma evolução legislativa, em face da dificuldade, na prática, de se executar um mandado de busca e apreensão de um *software* pirata[58], em que os oficiais de justiça não sabem qual objeto deverão carrear aos autos.

Quanto aos crimes virtuais, as dificuldades se assemelham, uma vez que o atacante da rede utiliza tecnologia para cometer o ilícito, mas o ilícito praticado na *Internet* pode ser provado de diversas maneiras. A polícia, tomando conhecimento de uma *notitia criminis,* deve iniciar a investigação.

Se a *notitia criminis* for de natureza coercitiva, facilita as condições de se apreender coisas e de se prender, no ato do flagrante, a pessoa envolvida no ilícito. Prendendo o autor da infração em estado de flagrância e apreendendo coisas que tenham relação com o ilícito, fácil é enviá-las aos peritos para que possam elaborar o laudo pericial.

Diversamente, em face do anonimato a que pertence o modo de operar dos usuários da rede, o auto de prisão em flagrante é pouco lavrado, pois o lugar do ilícito é de difícil elucidação. Nesse caso, a autoridade policial deve, nos moldes do art. 6º do Código de Processo Penal, investigar o crime virtual com mais zelo e cuidado, objetivando apurar materialidade e autoria.

Assim, na sequência em que foram tratadas as providências acauteladoras de prova, verificou-se primeiramente que se deve requerer à autoridade judicial a autorização para se fazer a interceptação telefônica dos envolvidos, seguindo rigorosamente os requisitos já estudados neste Capítulo.

Tendo sido feita a transcrição das falas entre os envolvidos, e encontrados os endereços onde residem e/ou onde se encontram os computadores e periféricos, deve-se requerer mandado de busca e apreensão para se ter em mãos todos os equipamentos necessários à elaboração do competente laudo pericial. Além dos equipamentos, podem ser apreendidos documentos e outras coisas que tenham relação com a prática do ilícito.

Sem olvidar que, estando os peritos de posse dos equipamentos, *hardware* e de toda espécie de mídia, deverão fazer uma pesquisa minuciosa sobre as informações contidas em seus arquivos, o que demandará trabalho de perícia, como, por exemplo, análise dos *e-mails* enviados entre *crackers*, que

58 *Software* pirata ou pirateado é o programa de computador que é adquirido sem a devida licença do autor e sem o pagamento do valor de mercado com a respectiva expedição de nota fiscal. A maior parte dos computadores são vendidos e entregues aos clientes com a instalação de programas pirateados como por exemplo, o *Microsoft Word.*

serviriam para troca de programas com a função de capturar senhas de pessoas que fazem transações financeiras e comerciais pela *Internet.* Adiante, será visto, passo a passo, como o perito deve proceder estando de posse de computadores e periféricos.

Na oportunidade, as medidas cautelares de cunho pessoal, como a prisão preventiva e a prisão temporária, também são instrumentos eficazes para facilitar a instrução criminal e trazer novos elementos na elaboração do laudo pericial. Uma vez que, estando os envolvidos presos e confessam, trazem elementos de prova que servirão de base para a apuração do ilícito.

Para quem entende que a interceptação telemática pode ser utilizada, conforme visto no item 6.2, também pode ser considerada como um facilitador de demonstração de materialidade e autoria, o que é trabalho dos peritos.

5.7. Perícia nos ilícitos digitais

A realização de perícia originada de fatos considerados como ilícitos digitais deve ter atenção especial dos peritos. A começar pelo comando do art. 6º, inciso I, do Código de Processo Penal, ao dispor que: "logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá: dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos locais".

O art. 169 do Código de Processo Penal aduz:

> Para o efeito de exame do local onde houver sido praticada a infração, a autoridade providenciará imediatamente para que não se altere o estado das coisas até a chegada dos peritos, que poderão instruir seus laudos com fotografias, desenhos ou esquemas elucidativos (Brasil, 1940, s/p).

Depreende-se daí a importância que se deve dar ao estado de conservação do local e dos objetos que serão periciados, ainda mais quando se tratar de coisas relacionadas à prática de ilícitos digitais, que, como já dito alhures, são conhecidas como espécies de crimes que deixam rastros.

A autoridade policial, tendo conhecimento da prática de fatos dessa natureza, se for o caso de lavratura de auto de prisão em flagrante, poderá apreender computadores, aparelhos celulares e mídias equivalentes que tenham relevância para a apuração do fato.

Da mesma forma, estando munida de mandado judicial, a autoridade policial deve tomar alguns cuidados para que essa apreensão não seja feita de qualquer modo, acarretando perda da oportunidade de se levar o material coletado a exame. Daí a ressalva de que, além da autoridade policial, à equipe deve se somar a presença de pelo menos um perito.

Ao chegar em um local para proceder uma ordem de busca e apreensão, pode ocorrer que o computador esteja ligado, e a autoridade tenha de fazer o seu desligamento. Caso haja o desligamento com a interrupção da energia ou com o apertar do botão *power* (*on/off*) ou com a retirada do cabo de força da tomada, pode resultar em problemas sérios no sistema e obstacularizar inicialização[59] posterior (Costa, 2003).

59 Inicializar significa processar o acionamento da máquina computacional dando respectiva carga ao sistema operacional.

O correto é desligar os computadores e, no caso do *Windows*,

> A operação pode ser efetivada por meio do botão iniciar, situado no lado esquerdo da barra de tarefas. Clica-se em iniciar>desligar e seleciona-se a opção desligar na caixa de diálogo que aparece, ou ainda hibernar, opção que faz o *Windows* efetuar a gravação do conteúdo da memória no disco rígido de forma que, ao se religar o sistema, volta-se à condição anterior ao desligamento, o que pode dar pistas importantes aos peritos do laboratório de computação forense, se porventura não puderem acompanhar os trabalhos que resultarem na apreensão dos equipamentos (Costa, 2003, p. 12).

Corroborando com essa opinião, Caricatti (2004, p. 32) explica que

> Em tempos recentes a abordagem dos locais trazia a recomendação quase unânime de desligar as máquinas prontamente. Hoje, há que se levar em conta a possibilidade de um invasor ser bem preparado, cuidando para trabalhar apenas com a memória volátil, ou seja, sem gravar dados em áreas permanentes como arquivos em disco.

Assim, alguns elementos podem ser categorizados como sendo aqueles que têm maiores chances de permanecerem intactos mais tempo, como:

- registros de processador e memória cachê[60]
- memória principal
- estado das conexões de rede
- estado dos processos em execução
- conteúdo das mídias não removíveis
- conteúdo das mídias removíveis

O perito verificará, no caso em análise, qual elemento mais adequado e pertinente para que não se altere o estado das informações (dados) a serem periciados. Todavia, recomenda-se que ater apenas ao material que foi coletado é incipiente, porque a própria *Internet* é um meio de se coletar informações preciosas a respeito do fato a ser examinado.

De Lima (2020) adverte que a cadeia de custódia deve ser observada para garantir a autenticidade das evidências coletadas e examinadas para evitar qualquer tipo de adulteração. O autor explica que o marco inaugural da cadeia de custódia do vestígio ocorre em três modalidades: na preservação do local do crime; na identificação dos vestígios pelos policiais; e na realização da perícia pelos técnicos da área a fim de assegurar o cumprimento do art. 158-A, § 1º, do CPP (Brasil, 1940).

Quando se tratar de coleta e preservação de fato digital, Azevedo e Souza, Munhoz e Carvalho (2024, p. 55) explicam que a ABNT NBR ISSO/IEC 27037:2013 traz recomendações de procedimentos de padronização do tratamento das evidências digitais como "isolamento do fato original contra contaminação, coleta sistemática dos dados, identificação das origens/equipamentos, preservação correta e início do controle de acesso à evidência com a gestão da cadeia de custódia".

60 Memória cachê (*memory cache*) é a que tem alta resolução, de alta velocidade, reservada para armazenar dados necessários a acesso rápido.

Aliás, o trabalho dos peritos de pesquisa na rede pode ser feito antes mesmo de se proceder à busca e apreensão. Após a notícia chegar até a autoridade policial, pode-se, ao investigar, pesquisar na *Internet* para verificar a existência de sítio falso de instituição bancária, por exemplo, e, com o auxílio de um perito, checar as informações do endereço do IP para descobrir quem são os responsáveis pela infraestrutura em que funciona e quais os caminhos que têm seu fluxo de dados para, em caso de necessidade, buscar uma autorização judicial junto ao provedor para informar o nome do usuário.

De qualquer forma, frise-se que, na dúvida, deve-se requerer ao magistrado a realização de diligência que necessite violação de dados da pessoa investigada, com a fundamentação da necessidade da medida, que pode ser concedida nos limites legais.

Voltando ao local do fato em que a autoridade policial está fazendo o desligamento das máquinas, outro fato importante a ser ressaltado é o transporte delas bem como das mídias. No transporte, é recomendável que se evite a colocação do material coletado mal acondicionado, o que poderá acarretar danos, caso ocorra algum acidente de percurso. O ideal é que se faça o aprisionamento das máquinas e das mídias em caixas de papelão, envolvidas em isopor ou material plástico (Costa, 2003).

Após a chegada do material no local da perícia, geralmente denominado de Instituto de Criminalística[61], deve ser remetido à unidade responsável para que sejam iniciados os trabalhos. Em seguida, na fase de recebimento dos equipamentos, a identificação individual dos computadores é medida essencial para evitar confusão e perda de material apreendido. A identificação consiste no etiquetamento do material com as informações de "sua origem, ocorrência policial vinculada, autoridade solicitante dos exames, tipo de equipamento, data/hora do recebimento, propriedade, lote a que pertence, de quem recebeu/recolheu etc." (Costa, 2003, p. 105).

Antes do início dos exames, o perito, que, preferencialmente, deve estar acompanhado de outro perito, deve examinar o interior dos equipamentos recebidos e fotografá-los no ato da abertura, além de listar os componentes em formulário próprio (Costa, 2003).

Da mesma forma que não se pode desligar os computadores de forma abrupta, a ligação deve ser coordenada de modo a preservar os dados que se pretende analisar. Logo que as máquinas são montadas, recomenda-se que os peritos façam a duplicação da mídia para reforço do material e como medida de segurança. Sobre a duplicação, Costa (2003, p. 26) reflete:

> Mas por que os exames devem ser realizados em uma cópia e não na mídia original? Além da preservação da prova, decorre da necessidade de se estabelecer o que se chama de Computação Forense de *timeline* ou linha de tempo, que é uma cronologia de eventos relacionados ao caso de avaliação. Os arquivos possuem características que permitem identificar sua data de criação, última alteração e último acesso, conhecidos como metadados. O simples fato de abrirmos um arquivo de computador altera seu estado, que pode ser desde a data do último acesso, como informações relativas à máquina em que ele foi trabalhado

61 O Instituto Nacional de Criminalística que investiga crimes de atribuição da Polícia Federal está sediado em Brasília na SAIS Quadra 07, Lotes 09/10, e tem como estrutura duas divisões (Divisão de Perícias/DPER) e (Divisão de Pesquisa, Padrões e Dados Criminalísticos/DPCRIM) em que a primeira possui uma subdivisão especializada em Serviço de Perícias em Informática/SEPINF.

O importante é a preservação dos dados originais, bem como os duplicados que, em hipótese alguma, podem ser alterados. No caso das mídias removíveis, há acesso direto somente para leitura (*CDs*) ou proteção eletrônica contra escrita (*ZIP disks*) (Costa, 2003).

Existem casos em que os dados são apagados ou ocultados para dificultar o serviço de coleta de provas. Porém, para esses casos, o mercado tecnológico já disponibiliza de *softwares* específicos, como, por exemplo, o *Encase*[62], da *Guidance Software*, que serve para criar um arquivo com cópia perfeita da mídia de prova.

Outra forma conhecida é a pesquisa simples dos arquivos na lixeira do computador, chamada de pesquisa mídia a quente, porque é feita diretamente no local em que foi apagada (Costa, 2003).

Chegando ao local dos dados, Costa (2003) ensina que, dependendo do ilícito cometido, pode-se definir a estratégia de pesquisa na busca das evidências do usuário e do sistema. Nas evidências do usuário, a pesquisa é feita nos arquivos; na pasta com o nome do usuário (pessoa investigada), quando não houverem sido ocultados ou criptografados. Nesses casos, o perito fará a quebra da senha ou da chave criptográfica utilizada mediante um ataque dicionário ou força bruta[63].

Quanto às evidências no sistema informático, são maiores e podem ser capturadas em dois campos: evidências no sistema na máquina de origem e na máquina alvo. Nos primeiros, podem ser encontrados arquivos em que constarão os últimos documentos utilizados no computador. A memória *cache* noticia quais foram os arquivos de imagens e elementos de composição das páginas visitadas por um determinado período, que, configurada a pasta, determinará o modo de atualização e visualização dos arquivos, bem como dos *sites* visitados. Além disso, uma navegação básica no *browser* do usuário permitirá ter ciência dos endereços eletrônicos que foram diretamente acessados (Costa, 2003).

Já nos sistemas da máquina alvo, caso seja endereçada à perícia, são abertos os arquivos *log*, que têm a função de registrar todas as transações como, por exemplo, *softwares* antivírus, servidores *WEB*, cliente etc. (Costa, 2003).

O importante é que haja, previamente, um encadeamento de ações a serem desenvolvidas pelos peritos de forma a obter otimização nos resultados (laudo pericial). Para que isso ocorra, além dos cuidados recomendados anteriormente, a metodologia adotada é fundamental para a elucidação do fato investigado e para resposta de possíveis quesitos apresentados pela defesa. O arquivamento da documentação (que pode ser feita em arquivos de computador) e a metodologia adotada são que garantem uma provável repetição do exame pericial em caso de questionamento judicial (Costa, 2003).

Na elaboração do laudo pericial, após se fazer um introito do caso, o perito deve abordar o objetivo dos exames tomando como base a solicitação da autoridade requisitante. No que se refere à metodologia, o perito deve indicar qual o *hardware* e o *software* que se aplicou ao caso, não se olvidando que o último (*software*) não pode ser pirateado. Dando sequência, será feita a exposição dos exames e ao final apresentada a conclusão da perícia.

62 O *Encase* permite visualização do arquivo e sua condição.

63 O ataque dicionário e da força-bruta tem o condão de descodificar o arquivo permitindo-se a consulta e a análise dos arquivos de dados mediante testes individuais de senha baseados em análise combinatória de caracteres (alfabéticos, numéricos e outros especiais).

Furlaneto Neto e Santos (2020) discriminam as fases da perícia, sendo a primeira de se identificar quais dispositivos e fontes de dados são relevantes para a investigação. Isso pode incluir: computadores (desktops, notebooks); Smartphones e tablets; dispositivos de armazenamento externo (pen drives, HDs externos, cartões de memória); sistemas em nuvem (e-mails, redes sociais, serviços de armazenamento online).

Em seguida, caminha-se para a preservação dos dados, sendo a etapa mais crítica, pois a integridade da prova digital é fundamental para sua validade em juízo. O objetivo é garantir que as evidências não sejam alteradas, corrompidas ou adulteradas. As ações incluem: a) isolamento do dispositivo: desconectar o dispositivo da internet e de outras redes para evitar alterações remotas; b) criação de imagens forenses: fazer cópias exatas (bit a bit) de discos rígidos, dispositivos de armazenamento e até mesmo da memória RAM. Essas cópias são chamadas de "imagens forenses" e são trabalhadas durante a análise, enquanto o original é preservado; c) obedecer à cadeia de custódia: manter um registro detalhado de todas as pessoas que tiveram contato com a evidência, desde a sua coleta até a apresentação em tribunal para garantir autenticidade e integridade da prova (Furlaneto Neto; Santos, 2020).

O próximo passo é a coleta dos dados. Com as imagens forenses criadas, o perito começa a extrair informações relevantes. Essa coleta pode envolver: a) recuperação de arquivos deletados: muitas vezes, dados deletados não são realmente apagados do disco, apenas seu espaço é marcado como disponível. Ferramentas especializadas podem recuperá-los; b) análise de logs de sistema com os registros de atividades do sistema operacional, aplicativos e redes podem revelar horários de acesso, ações realizadas e tentativas de acesso; c) extração de e-mails, mensagens e históricos: conteúdo de e-mails, mensagens de texto, chats (*WhatsApp*, Telegram) e históricos de navegação são coletados; d) análise de metadados mediante a análise das informações sobre os arquivos, como data de criação, última modificação, autor, e até mesmo dados de geolocalização de fotos e vídeos (Costa, 2003; Wendt; Jorge, 2021).

Em seguida, o perito fará análise dos dados examinando detalhadamente os dados coletados em busca de evidências que comprovem ou refutem uma hipótese investigativa. São usadas diversas metodologias e ferramentas especializadas, tanto proprietárias quanto de código aberto. Algumas técnicas e ferramentas incluem: a) análise de sistemas de arquivos para identificar padrões de uso, arquivos ocultos e alterações no sistema; b) análise de memória volátil (RAM) para investigar dados que estavam na memória do dispositivo no momento do crime, o que pode revelar processos em execução, dados de rede e senhas temporárias. Ferramentas como *Volatility* são usadas para isso; c) análise de rede: rastrear o tráfego de dados para identificar a origem de ataques, padrões de comunicação e vazamento de informações. O *Wireshark* é uma ferramenta popular para análise de pacotes de rede; d) análise de *malware*: identificar e entender a funcionalidade de softwares maliciosos; e) criação de linhas do tempo (*timelines*): reconstruir a sequência de eventos com base nos metadados e logs, facilitando a compreensão cronológica dos fatos; f) recuperação de dados ocultos: utilizar técnicas como esteganografia reversa para expor informações que foram intencionalmente escondidas; g) busca por palavras-chave: deve procurar termos específicos que possam estar relacionados ao crime (Furlaneto Neto; Santos, 2020).

Por último, far-se-á a elaboração do laudo pericial detalhado e fundamentado, isto é, a perícia feita nos equipamentos utilizados pelos suspeitos ou acusados de prática de ilícitos digitais deve ser programada, obedecendo a uma ritualística própria, para que se possam capturar as informações solicitadas e responder de forma adequada ao juízo se o computador e as mídias apreendidas foram meios utilizados para ataques na rede mundial de computadores.

CONCLUSÃO

Constata-se que dentre as inovações tecnológicas a *Internet* é uma modalidade de alcance global e que pode, dependendo de seu uso, acarretar sérios prejuízos aos internautas. Daí a necessidade de adoção dos meios de prevenção para que os usuários não se tornem vítimas em potencial dos agressores da rede.

As técnicas mais utilizadas pelos atacantes virtuais são mensagens eletrônicas com o objetivo de capturar dados de natureza pessoal da vítima, envio de programas *trojans* e criação de páginas clonadas àquelas acessadas pelo usuário, todas tendo em comum a finalidade de "pescar" as senhas bancárias dos clientes, quando se tratar de ilícitos praticados em desfavor de clientes de instituições bancárias.

Por outro lado, as medidas de prevenção podem minimizar tais condutas, ainda mais, se houver uma conscientização do usuário da internet pelas empresas que oferecem estes serviços. A Cartilha virtual do Comitê Gestor da *Internet* já é uma iniciativa positiva que ensina o internauta a guardar seus dados com mais acuidade. O uso da certificação digital também é uma tendência que assegura ao cliente de uma instituição comercial fazer transações na rede com mais segurança, uma vez que detém o código da chave de sua assinatura digital.

Todavia, caso o usuário tenha se tornado uma vítima de um atacante virtual e advinda a conduta, e sendo ela tipificada na norma, cabe ao investigador perquirir a busca da materialidade e da autoria do ilícito para que o órgão acusatório possa ter elementos suficientes para a propositura da ação penal. Sendo a *Internet* um ambiente virtual, e o ilícito um fato, necessária é a adequação do investigador e do magistrado no cuidado da coleta dessa prova em face da legislação em vigor.

Todos os meios de provas previstos no atual Código de Processo Penal podem ser utilizados pelas autoridades envolvidas, desde que produzidos sob o manto da licitude, calcados na ordem dos princípios constitucionais. Tanto as provas nominadas, típicas ou ordinárias, quanto inominadas, atípicas ou extraordinárias, podem ser colhidas no inquérito policial e na fase judicial, desde que compatíveis com o ordenamento jurídico brasileiro.

As medidas acauteladoras, seja a busca e apreensão sejam as prisões de natureza processual, em geral, têm o objetivo de arregimentar provas do fato. E nem se diga que uma prisão preventiva não teria, entre outras, tal finalidade, uma vez que, estando o acusado preso, impede que coaja testemunhas, facilitando, portanto, a produção da prova testemunhal.

Quanto à interceptação telefônica, é um dos meios de prova mais usados pela polícia em várias modalidades de ilícitos, entre eles, os digitais. Estando preenchidos os requisitos do art. 2º da Lei nº 9.196/1996, a ordem para a interceptação deve ser admitida após autorização judicial fundamentada. A observação que se faz é quanto à restrição de não se obter a interceptação telefônica de pessoas que estejam praticando ilícitos na *Internet* em crimes punidos com pena de detenção, o que é vedado no inciso III do art. 2º da lei citada, o que dificulta, em alguns casos, a apuração do fato.

A interpretação em termos e limites constitucionais pode ser realizada como princípio de interpretação e como técnica de controle de constitucionalidade. Quanto ao primeiro, outros dois princípios derivam – o da supremacia constitucional e o da presunção da constitucionalidade; e, quanto ao segundo, a não aplicação da norma por afrontar a Constituição Federal. O que deve prevalecer é que a interceptação é a exceção, enquanto o sigilo é a regra. A Constituição Federal apenas autoriza a interceptação das comunicações telefônicas, excluindo-se a de dados e as telegráficas.

O intérprete deve vislumbrar que a ressalva existente no inciso XII do art. 5º do texto constitucional refere-se apenas ao último caso, que, na hipótese, refere-se às interceptações telefônicas. Na dúvida, o que deve prevalecer é a proteção às garantias e aos direitos fundamentais, que devem ser respeitados pelo magistrado.

Quanto à possibilidade de se coletar provas em ilícitos virtuais ou digitais é plenamente possível, desde que haja um trabalho efetivo da polícia. A autoridade policial pode representar pela busca e apreensão dos objetos que tiverem relação com os fatos objeto de investigação. Ou seja, computadores e periféricos podem, sim, ser apreendidos via ordem judicial para que sejam enviados ao departamento pericial. Esses objetos podem conter informações preciosas que poderão servir como meio de prova, como, por exemplo, o conteúdo de *e-mails*, que poderão ser revelados, desde que haja prévia autorização judicial. Outro objeto importante é a apreensão de aparelhos celulares que objetiva a leitura das mensagens trocadas pelos acusados para a descoberta de fatos importantes que tenham ligação direta com o crime praticado.

Ao contrário do entendimento de alguns doutrinadores, os dados contidos e estanques em arquivos de computador, como conteúdo de *e-mails*, após a chegada a seu destinatário, podem ter os equipamentos apreendidos (ou em situação de flagrância ou por meio de autorização judicial), e endereçados à perícia para a elaboração do laudo pericial. Outro fator relevante diz respeito às informações que os provedores de internet podem revelar, desde que requisitados por intermédio de ordem judicial.

Por fim, a elaboração do laudo pericial pode ser realizada tendo como ponto de partida outros meios de provas nos ilícitos virtuais ou digitais, tais como: fotografias, desenhos, degravação das conversas telefônicas e objetos que se relacionam com o ilícito (computadores e todas as espécies de mídias).

O laudo pericial a ser elaborado deve ter o zelo por parte dos peritos para que não se percam os vestígios do ilícito e se corra o risco de não obter a materialidade que poderá levar a um julgamento justo, sendo indispensável à elucidação da verdade. Não é concebível que em ilícito dessa natureza,

em que tenham sido apreendidas as mídias e outros instrumentos do crime, por falta de estrutura do Estado, o Juiz não tenha condições de proferir uma decisão justa e compatível com as provas obtidas na instrução processual.

Todavia, conclui-se que todos os meios de prova previstos no Código de Processo Penal são aplicáveis na investigação dos ilícitos virtuais, desde que sua produção seja realizada nos limites constitucionais e da legislação em vigor. Além desses, os meios de provas atípicos existentes em leis esparsas também podem ser efetivados nos ilícitos virtuais, ressalvada a realização da interceptação de sistemas de informática e telemática em obediência ao inciso XII do art. 5º da Constituição Federal.

REFERÊNCIAS

AGUIAR, Marcelo (colab. Murilo Ramos). Internet. Lanterninha. **Revista Época**. São Paulo: Editora Globo, n. 395, p. 71, 12 dez. 2005.

ALVES, Roque de Brito. **Criminologia**. Rio de Janeiro: Forense, 1986.

AMORIM, Ricardo. COMPORTAMENTO. De ladrões de cartão de crédito a simples pichadores de páginas, adolescentes se divertem invadindo sites na Internet. A gangue do mouse. **Revista Época**, n. 348, 17 de jan. de 2005, p. 52/59.

ARANHA, Adalberto José Q. T. de. **Da prova no processo penal**. São Paulo: Saraiva, 2004.

ARAS, Vladimir. Crimes de informática: uma nova criminalidade. **Jus Navigandi**, Teresina, ano 5, n. 51, out. 2001. Disponível em: http://jus.uol.com.br/revista/texto/2250/crimes-de-informatica Acesso em: 15 ago. 2025.

ARAÚJO, José Osterno Campos de. **Verdade processual penal**. 1. ed. (a.2005), 2. tir. Curitiba: Juruá, 2006.

ASSOCIAÇÃO BRASILEIRA DE DIREITO DE INFORMÁTICA (ABDI). Seminário internacional. São Paulo, 1991.

ATHENIENSE, Alexandre. **Internet e o direito**. Belo Horizonte: Inédita, 2000.

AVENA, Norberto. **Processo penal**: esquematizado. 4. ed. Rio de Janeiro: Forense; São Paulo: Método, 2012.

AVOLIO, Luiz Francisco Torquato. **Provas ilícitas***:* interceptações telefônicas, ambientais e gravações clandestinas. 3. ed. rev. e atual. São Paulo: Editora Revista dos Tribunais, 2003.

AVOLIO, Luiz Francisco Torquato. **Provas ilícitas***:* interceptações telefônicas, ambientais e gravações clandestinas. 6. ed. rev. e atual. São Paulo: Editora Revista dos Tribunais, 2015.

BARROS, Marco Antônio de. **A busca da verdade no processo penal**. São Paulo: Editora Revista dos Tribunais, 2002.

BARROS, Romeu Pires de Campos. **Sistema do processo penal brasileiro**. v.1, Rio de Janeiro: Forense, 1987.

BARROS, Romeu Pires de Campos. **Sistema do processo penal brasileiro**. v.2, Rio de Janeiro: Forense, 1987.

BARROS, Romeu Pires de Campos. **Processo penal cautelar**. Rio de Janeiro: Forense, 1987.

BARROSO, Luís Roberto. **O direito constitucional e a efetividade de suas normas**. Limites e possibilidades da Constituição Brasileira. 7. ed. Rio de Janeiro: Renovar, 2003.

BECCARIA, Cesare. **Dos delitos e das penas**. trad. José Roberto Malta. São Paulo: WVC, 2002.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**. Parte geral. v. 1. 26. ed. São Paulo: Saraiva, 2020.

BRASIL, Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília. Senado: Saraiva, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 20 dez. 2024.

BRASIL, **Lei n. 9.296 de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º. da Constituição Federal. Diário Oficial da União. Brasília, 25 de julho de 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm#art10A Acesso em: 9 jun. 2025.

BRASIL, **Decreto-lei n. 3.689, de 3 de outubro de 1941**.Código de Processo Penal. Diário Oficial da União. Publicado no dia 13 e retificado em 24 de outubro de 1941.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União, Brasília, DF, 16 jul. 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 2 jun. 2025.

BRASIL**. Lei n. 9.807, de 13 de julho de 1999**. Estabelece normas para a organização e a manutenção de programas especiais de proteção a vítimas e a testemunhas ameaçadas, institui o Programa Federal de Assistência a Vítimas a Testemunhas ameaçadas e dispõe sobre a proteção de acusados ou condenados que tenham voluntariamente prestado efetiva colaboração à investigação policial e ao processo criminal. Disponível em:<http://www.planalto.gov.br/ccivil_03/leis/L9807.htm >. Acesso em: 01 jun. 2025.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Diário Oficial da União, Brasília, DF, 28 maio 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm Acesso em: 4 jun. 2025.

BRASIL. **Lei 14.132, de 31 de março de 2021**. Acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm. Acesso em: 7 jun. 2025.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário 1.037.396/SP**. Tema 987 – Limites da responsabilidade civil de provedores de aplicações de internet por conteúdos gerados por terceiros. Relator: Ministro Dias Toffoli. Brasília, DF, julgado em 22 maio 2024. **Diário de Justiça Eletrônico**, Brasília, DF, [data da publicação do acórdão no DJe]. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5177063. Acesso em: 5 jul. 2025.

BROLESI SILVA, Carlos Magno. A criptografia e o mundo jurídico. **Boletim IBCCRIM**. São Paulo, n. 54, p. 16. maio de 1994.

CAMARÃO, Paulo César Bhering. **Glossário de Informática**. 2. ed. rev. e ampl. Rio de Janeiro: LTC – Livros Técnicos e Científicos, 1994.

CAPEZ, Fernando. **Curso de processo penal**. 12. ed. rev. e atual. São Paulo: Saraiva, 2005.

CARNELUTTI, Francesco. **As misérias do processo penal**. São Paulo: Edicamp, 2001.

CARNELUTTI, Francesco. **Das provas no processo penal**. 1. ed. trad. de Vera Lúcia Bison. Campinas: Impactus, 2005.

CARRARA, Francesco. **Programa do curso de direito criminal**. Turim, 1841.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Tradução de Maria Luiza X. de A. Borges. Revisão Paulo Vaz. Rio de Janeiro: Zahar, 2003.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus aspectos processuais**. 2. ed. ampl. e atual. Rio de Janeiro: Lumen Juris, 2003.

CINTRA, Antonio Carlos de Araújo Cintra; GRINOVER, Ada Pellegrini; DINAMARCO, Cândido Rangel. **Teoria Geral do Processo**. 21. ed. rev. atual. de acordo com a EC 45, de 8.12.2004, São Paulo: Malheiros Editores, 2005.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da Internet**. São Paulo: Saraiva, 2000.

COSTA, Marcelo Antônio Sampaio Lemos. **Computação forense**. 2. ed. São Paulo: Millenium, 2003.

COMER, Douglas. **Internetworking with TCP/IP**. 3rd. ed. New Jersey: Prentice Hall, 1995.

COSTA, Paula Bajer Fernandes da. **Igualdade no direito processual penal brasileiro**. São Paulo: Editora Revista dos Tribunais, 2001.

CRESPO, Marcelo Xavier de F. **Crimes digitais**. Disponível em: Minha Biblioteca, SRV Editora LTDA, 2011.

CUNHA, Rogério Sanches. **Pacote Anticrime – Lei 13.964/2019: comentários no CP, CPP e LEP. Salvador:** Editora JusPodivm, 2020.

DELMANTO, Celso; DELMANTO, Roberto; DELMANTO JÚNIOR, Roberto. **Código Penal Comentado.** 4. ed. Rio de Janeiro: Renovar, 1998.

DELMANTO, Roberto. A permissão constitucional e a nova lei de interceptação telefônica. **Boletim IBCCRIM**. São Paulo, n. 47, p. 02, out. 1996.

DE LIMA, Renato Brasileiro. **Manual de processo penal**. Atualizado com o Pacote AntiCrime. 8. ed. rev. atual. ampl. Salvador: Editora JusPodivm, 2020.

DRUMMOND, Victor. **Internet, privacidade e dados pessoais**. Rio de Janeiro: Lumen Juris, 2003.

EISENBERG, Marco Cepick, (organizadores). **Internet e Política**: teoria e prática da democracia eletrônica. Belo Horizonte: Editora UFMG, 2002.

FALCÃO, Joaquim. Internet estável e segura. **Prática Jurídica**, Brasília, a. IV, n. 43, 31 de outubro de 2005.

FEBRABAM. 82% das transações bancárias dos brasileiros são feitas pelos canais digitais, revela pesquisa. Disponível em: https://portal.febraban.org.br/noticia/4310/pt-br/ Acesso em: 15 ago. 2025.

FERNANDES, Antonio Scarance. Interceptações telefônicas: aspectos processuais da nova lei. **Boletim IBCCRIM**. São Paulo, n. 45, p. 15-16, ago. 1996.

FERRAJOLI, Luigi. **Direito e Razão**: teoria do garantismo penal. prefácio da 1ª. edição italiana. 3. ed. São Paulo: Revista dos Tribunais, 2010.

FERREIRA, Aurélio Buarque de Holanda. **Novo dicionário da língua portuguesa**. 2. ed. rev. aum. 34. imp. Rio de Janeiro: Nova Fronteira, 1986.

FILHO, Élio Wanderley de Siqueira. Sigilo das comunicações telefônicas, telegráficas e de dados: aspectos relevantes da escuta telefônica. **Revista CEJ**, Brasília, v. 2, n. 5, p. 40-46, maio/ago. 1998.

FILHO, Vicente Greco. **Interceptação telefônica**: (considerações sobre a lei n. 9.296, de 24 de julho de 1996) 2. ed. rev., atual. e ampl. (com a colaboração de João Daniel Rassi). São Paulo: Saraiva, 2005.

FILHO, Vicente Greco. Algumas observações sobre o direito penal e a Internet. **Boletim IBCCRIM.** São Paulo, v. 8, n. 95, esp., p. 3, out. 2000.

FIORILLO, Celso Antônio, Pacheco; Christiany Pegorari Conte. **Crimes no meio ambiente digital**. SRV Editora LTDA, 2016.

FRAGOSO, Heleno Cláudio. **Lições de direito penal***:* a nova parte geral. 8. ed. Rio de Janeiro: Forense, 1985.

GOIS JÚNIOR, José Caldas. **O direito na era das redes**: a liberdade e o direito no ciberespaço. São Paulo: Edipro, 2002.

GOMES, Luiz Flávio; MACIEL, Silvio. **Interceptação telefônica e telemática (Lei 9.296/96)**. 2. ed. São Paulo: Revista dos Tribunais, 2011.

GOMES, Olavo José Anchiechi. **Segurança total – protegendo-se contra os hackers**: leis e projetos de leis envolvendo crimes digitais no Brasil e em outros países. São Paulo: Makron, 2000.

GOMES FILHO, Antonio Magalhães. A violação do princípio da proporcionalidade pela Lei 9.296/96. **Boletim IBCCRIM**. São Paulo, n. 45, p. 14, ago. 1996.

GRECO FILHO, Vicente. *Interceptação telefônica*: (considerações sobre a lei n. 9.296, de 24 de julho de 1996) 2. ed. rev., atual. e ampl. (com a colaboração de João Daniel Rassi). São Paulo: Saraiva, 2005.

GRINOVER, Ada Pellegrini; FERNANDES, Antonio Scarance; GOMES FILHO, Antônio Magalhães. **As nulidades no processo penal**. 8. ed. rev. e atual. São Paulo: Editora Revista dos Tribunais, 2004.

GURGEL, André; PIRES, Paulo. **Crimes de informática e seus reflexos jurídicos**. São Paulo: Malheiros, 2000.

HARBELE, Peter. **Hermenêutica constitucional – a sociedade aberta dos intérpretes da constituição:** Contribuição para a interpretação pluralista e "procedimental" da Constituição. Trad. Gilmar Ferreira Mendes; Sergio Antonio Fabris editor. Porto Alegre, RS,1997.

INAF (Indicador de analfabetismo funcional). **Analfabetismo no Brasil**. Disponível em: https://alfabetismofuncional.org.br/ Acesso em: 8 jul. 2025.

JESUS, Damásio E. de. **Direito penal. Parte especial**. v. 3, 23. ed. rev. e atual. São Paulo: 2000.

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

KOLBE JÚNIOR, Armando. **Investigação de crimes digitais**. Curitiba: Contentus, 2020.

KAMINSKI, Omar. (organizador). **Internet legal***:* o direito na tecnologia da informação. Curitiba: Juruá, 2003.

LEITÃO JÚNIOR, José. **Internet e Direito:** Prova e Responsabilidade Civil. Campinas: Millennium, 2002.

LOPES Júnior, Aury. **Direito processual penal e sua conformidade constitucional**. v. 1. 7. ed. Rio de Janeiro: Lumen Juris, 2011.

LOPES Júnior, Aury. **Direito Processual Penal**. 13. ed. São Paulo: Saraiva, 2016.

LIMA NETO, José Henrique Barbosa Moreira. Da inviolabilidade de dados: inconstitucionalidade da Lei n. 9.296/96 (Lei de interceptação de comunicações telefônicas). **Boletim IBCCRIM**. São Paulo, n. 56, p. 03-04, jul. 1997.

MALATESTA, Nicola Framarino Dei. **A lógica das provas em matéria criminal**. Trad. de Paolo Capitanio. Campinas: Bookseller, 2004.

MARCÃO, Renato. **Curso de Processo Penal**. São Paulo: 2020.

MARQUES, José Frederico. **Elementos de Direito Processual Penal**. v. I, II, III e IV, 2. ed. Campinas: Millennium, 2003.

MARTINS, José de Sousa. **Exclusão social e a nova desigualdade**. São Paulo: 1997.

MEIRELLES, Fernando de Souza. **Informática**: novas aplicações com microcomputadores. 2. ed. atual. e ampl. São Paulo: Makron Books, 1994.

MIRABETE, Julio Fabbrini.; FABBRINI, Renato N. **Manual de direito penal:** parte especial - arts. 121 a 234-B do CP. 38. ed. Cotia, SP: Foco, 2025. *E-book*. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 02 jun. 2025.

MIRABETE, Julio Fabbrini; FABBRINI, Renato Nalini. **Código penal interpretado**. 12. ed. Indaiatuba, SP: Editora Foco, 2025.

MIRABETE, Julio Fabbrini. **Processo Penal**. 18. ed. rev. e atual. até 31 de dezembro de 2005. São Paulo: Atlas, 2006.

MITNICK, Kevin D. **A arte de enganar**. Trad. Kátia Aparecida Roque.São Paulo: Perason Makron Books, 2003.

MITTERMAIER, C. J. A. **Tratado da Prova em matéria criminal**. 4. ed. trad. de Herbert Wuntzel Heinrichi. Campinas: Bookseller, 2004.

MOLINA, Antonio Garcia-Pablos de Molina, GOMES, Luiz Flávio Gomes. **Criminologia: introdução a seus fundamentos teóricos:** introdução às bases criminológicas da Lei n. 9.099/95, leis dos juizados especiais criminais. 4. ed. rev. atual, ampl. São Paulo: Editora Revista dos Tribunais, 2002.

MORAES, Alexandre de. A constitucionalidade do parágrafo único do art. 1º. da lei n. 9.296/96: interceptações do fluxo de comunicações em sistemas de informática e telemática. **Boletim IBCCRIM**. São Paulo, n. 54, p. 05, maio 1997.

MUSTARO, Pollyana Notargiacomo. **Hackers:** um estudo sobre linguagens, identidades e educações no ciberespaço.Tese de Doutorado. São Paulo: Faculdade de Educação da Universidade de São Paulo, 2003, 273 p.

NETO, Mário Furlaneto; SANTOS, José Eduardo Lourenço dos. APONTAMENTOS SOBRE A CADEIA DE CUSTÓDIA DA PROVA DIGITAL NO BRASIL. **Revista Em Tempo**, [S.l.], v. 20, n. 1, nov. 2020. ISSN 1984-7858. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3130. Acesso em: 08 jul. 2025.

NETO, Ameleto Masini. **Crimes cibernéticos**. Indaiatuba, SP: Editora Foco, 2025.

NUCCI, Guilherme de Souza. **Manual de processo penal e execução penal**. 5. ed. e rev. atual. e ampl. São Paulo: Revista dos Tribunais, 2008.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**.16. ed. Rio de Janeiro: Forense, 2020.

OLIVEIRA, Ana Sofia Schmidt de. **A vítima e o direito penal**. São Paulo: Editora Revista dos Tribunais, 1999.

OLIVEIRA, Edmundo. **Vitimologia e Direito Penal**: o crime precipitado pela vítima. Rio de Janeiro: Forense, 2005.

OLIVEIRA, Eugênio Pacelli de. **Curso de processo penal**. 19. ed. rev. atual. São Paulo: Atlas, 2015.

PAESANI, Liliana Mainardi. **Direito de informática**: comercialização e desenvolvimento internacional do Software. 3. ed. São Paulo: Atlas, 2001.

PECK, Patrícia. **Direito Digital**. São Paulo: Saraiva, 2002.

PIMENTEL, Alexandre Freire. **O direito cibernético**: um enfoque teórico e lógico-explicativo. Rio de Janeiro: Renovar, 2000.

PINHEIRO, Reginaldo César. Os crimes virtuais na esfera jurídica brasileira. **Boletim IBCCRIM.** São Paulo, v. 8, n. 101, p. 18-19, abril de 2001.

POLÍCIA FEDERAL. PF deflagra a operação Face Off contra fraudadores de contas vinculadas à Plataforma GOV.BR. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2025/05/pf-deflagra-a--operacao-face-off-contra-fraudadores-de-contas-vinculadas-a-plataforma-gov.br Acesso em: 16 ago. 2025.

PLANTULO, Vicente Lentini. **Estelionato eletrônico**. Curitiba: Juruá. 2003.

PRADO, Geraldo. A interceptação das comunicações telefônicas e o sigilo constitucional de dados operados em sistemas informáticos e telemáticos. **Boletim IBCCIM**. São Paulo, n. 55, p.13-14, jun. 1997.

PRADO, Luiz Regis. **Curso de direito penal brasileiro**. v. 1: parte geral. 11. ed. rev. atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2011.

QUEIJO, Maria Elizabeth. **O direito de não produzir prova contra si mesmo**. (o princípio nemo tenegere e suas decorrências no processo penal). São Paulo: Saraiva, 2003.

RANGEL, Paulo. **Direito Processual Penal**. 23. ed. São Paulo: Atlas, 2015.

REIS, Maria Helena Junqueira. **Computer crimes**: a criminalidade na era dos computadores. Belo Horizonte: Del Rey, 1996.Rio de Janeiro: Forense, 1987.

RIBEIRO, Neide Aparecida. ***Cyberbullying*: práticas e consequências da violência virtual na escola**. Salvador: Editora JusPodivm, 2019.

ROCHA, Fernando Antonio Nogueira Galvão da. Criminalidade do computador. **Revista Jurídica do Ministério Público**, Belo Horizonte, a 27, p. 75-98, 1996.

ROSA, Fabrício. **Crimes de informática**. Campinas: Bookseller, 2002.

RYDLEWSKI, Carlos. O velho novo golpe. **Revista Veja**. n. 17 de nov. de 2004, p. 168/171.

SANDEBERG, Jared. Falta de Segurança da internet. O Estado de São Paulo. São Paulo, 14 jul. 1997. **Caderno de Informática**. p. 3.

SENISE, Ivete. **Os crimes de informática**. In: Barra, Rubens Prestes; ANDREUCCI, Ricardo Antunes. Estudos Jurídicos em Homenagem a Manoel Pedro Pimentel. São Paulo: RT, 1992.

SENADO FEDERAL. Golpes digitais atingem 24% da população brasileira, revela DataSenado. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado Acesso em: 15 ago. 2025.

SHECAIRA, Sérgio Salomão. **Criminologia**. São Paulo: Editora Revista dos Tribunais, 2004.

SILVA, Mauro Marcelo de Lima e. Polícia revela o perfil do criminoso na Internet. In. Omar KaminsKi. **Internet Legal**: O direito na Tecnologia da Informação. Doutrina e Jurisprudência. Curitiba: Juruá, 2003.

SILVA NETO, Amaro Moraes. **Privacidade na Internet**. São Paulo: Juarez de Oliveira, 2001.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. São Paulo: RT, 1989.

SILVA, Rita de Cássia Lopes. **Direito penal e sistema informático**. Luiz Regis do Prado (Coord.). São Paulo: RT, 2003.

SILVEIRA, Sergio Amadeu. **Ambivalências, liberdade e controle dos ciberviventes**. (in) SILVEIRA, Sergio Amadeu (org). Cidadania e Redes Digitais. Citizenship and digital networks. 1. ed. 1. imp. São Paulo: Comitê Gestor da Internet no Brasil: Maracá – Edcuação e Tecnologias, 2010.

SOARES, Luiz Fernando Gomes. **Redes de Computadores**. 9. ed. rev. ampl. Rio de Janeiro: Campus, 1995.

SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Roumullo. **Manual prático de provas digitais**. 2. ed. rev. atual. e ampl. São Paulo: Thompson Reuters, 2024.

SOUZA, Guilherme de. **Pacote Anticrime comentado:** Lei n. 13.964, de 24.12.2019. 1.ed. Rio de Janeiro: Forense, 2020.

TELES, Ney Moura. **Direito penal**: parte geral. 2. ed. São Paulo: Atlas, 2006.

TONINI, Paolo. **A prova no processo penal italiano**. Trad. de Alexandra Martins Mirós. São Paulo: Editora Revista dos Tribunais, 2002.

TOURINHO FILHO, Fernando da Costa. **Manual de processo penal**. 4. ed. rev., atual. e aum. São Paulo: Saraiva, 2002.

UOL. Brasil é o segundo país com mais ataques cibernéticos no mundo. Disponível em: https://cultura.uol.com.br/noticias/69028_brasil-e-o-segundo-pais-com-mais-ataques-ciberneticos-no-mundo-diz-estudo.html Acesso em: 8 jul. 2025.

VIANA, Túlio Lima. **Fundamentos de direito penal informático***:* do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003.

WILHELM, Anthony e CEPICK Marco (organiz.). **Internet e política**. Teoria e prática da democracia eletrônica. Belo Horizonte: Editora UFMG, 2002.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**. 3. ed. Rio de Janeiro: Brasport, 2021.

WOLTON, Dominique. **Internet, e depois**? Uma teoria crítica das novas mídias. trad. Isabel Crosseti, 3. ed. Porto Alegre: Sulina, 2012.

GLOSSÁRIO

Ábaco – instrumento utilizado pelos povos primitivos para se fazer contagem, cálculos, operações algébricas.

ADSL - do Inglês *Asymmetric Digital Subscriber Line*. Sistema que permite a utilização das linhas telefônicas para transmissão de dados em velocidades maiores que as permitidas por um modem convencional.

Adware - do Inglês *Advertising Software*. *Software* especificamente projetado para apresentar propagandas. Constitui uma forma de retorno financeiro para aqueles que desenvolvem *software* livre ou prestam serviços gratuitos. Pode ser considerado um tipo de *spyware*, caso monitore os hábitos do usuário, por exemplo, durante a navegação na Internet para direcionar as propagandas que serão apresentadas.

Antivírus - programa ou *software* especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de código malicioso.

ARPANET - rede de compartilhamento de computadores da ARPA - *Advanced Research Projects Agency*, que mais tarde evoluiu para a *Internet*.

Atacante - pessoa responsável pela realização de um ataque. Veja também Ataque.

Ataque - tentativa, bem ou mal sucedida, de acesso ou uso não autorizado a um programa ou computador. Também são considerados ataques às tentativas de negação de serviço.

Autenticação - técnica pela qual a *Internet* requer a identificação do internauta através da digitação do seu *username* e *password*.

***Backbone* -** infraestrutura formada pelas linhas de comunicação e o hardware de transmissão e de recepção para acesso à *Internet* mundial vendido aos provedores brasileiros pela Embratel, Global One, RNP e Intelig.

Backdoor - programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.

Backup - copiar arquivos para um segundo dispositivo (um outro *drive* ou disquete) como medida de precaução no caso de haver algum problema com o dispositivo original onde os arquivos se encontram. Uma das mais importantes regras no uso de computadores é "faça o *backup* de seus arquivos regularmente".

Banda Larga – canal de comunicação que tem a largura da banda maior que o canal de voz, sendo capaz de transmitir dados em alta velocidade.

Boato - *email* que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente ou aponta como autora da mensagem alguma instituição, empresa importante ou órgão governamental. Através de uma leitura minuciosa deste tipo de *e-mail*, normalmente, é possível identificar em seu conteúdo mensagens absurdas e muitas vezes sem sentido.

Bot - programa que, além de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o *bot*, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar *spam*, etc.

Botão *Power (on/off)* – botão parte integrante do computador que permite o ligamento e o desligamento da máquina computacional.

Botnets - redes formadas por diversos computadores infectados com *bots.* Podem ser usadas em atividades de negação de serviço, esquemas de fraude, envio de *spam*, etc.

***Bridge* -** equipamento que conecta duas redes locais (*LANs)* ou dois segmentos de uma mesma *LAN*. Diferentemente dos roteadores ou *routers*, *bridges* são protocolo-independente, enviando pacotes sem a capacidade de otimizar rotas. Isso lhes dá velocidade, mas menos versatilidade.

Browser - são programas de computador usados para localizar e visualizar documentos em HTML. São esses programas que permitem a navegação no ambiente *WWW* e a visualização de *websites*. Os *browsers* mais utilizados são o *Netscape* e o *Microsoft Explorer*.

Buttons - são botões ou selos ilustrativos que fazem parte da programação visual do *website.*

Byte - a medida de armazenamento em espaço em disco igual a 8 *bits*.

Cable modem - *modem* projetado para operar sobre linhas de TV a cabo.

Cavalo de troia - programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

CGI - significa *Common Gateway Interface*. São *scripts* que permite a inclusão de formulários em páginas *Web.*

***Chats* –** salas de bate papo da *Internet*.

Chips – unidade semicondutora microscópica composta de transistores interconectados e outros componentes eletrônicos prensados num único bloco, formando um circuito completo ou quase completo. Circuito integrado.

Clicar – teclar, digitar.

Código malicioso - termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os *vírus*, *worms*, *bots*, cavalos de tróia, *rootkits*, etc.

Comércio eletrônico - também chamado de *e-commerce*, é qualquer forma de transação comercial onde as partes interagem eletronicamente. Conjunto de técnicas e tecnologias computacionais utilizadas para facilitar e executar transações comerciais de bens e serviços através da *Internet*. É a venda de produtos e serviços através da *Internet*.

Computador - equipamento eletrônico capaz de ordenar, calcular, testar, pesquisar e editar informações de acordo com instruções estabelecidas e segundo uma representação binária, obedecendo a um conjunto de operações aritméticas e lógicas.

Conexão segura - conexão que utiliza um protocolo de criptografia para a transmissão de dados, como por exemplo, HTTPS ou SSH.

Conta - permissão para acesso à *Internet*, normalmente simbolizada por um *login* e uma senha. A conta é aberta e mantida num provedor de acesso mediante o pagamento de mensalidades pelo internauta.

Cookies - são arquivos contendo informações como nome e preferências dos visitantes de um *website*. Esta informação é fornecida por cada internauta em sua primeira visita ao site. O servidor do *site* visitado registra a informação num arquivo e armazena este arquivo no disco rígido do internauta. Quando o internauta retorna ao site, o servidor procura e acha o *cookie* e se autoconfigura de acordo com a preferências indicadas por cada internauta.

Core – núcleo da Rede.

Correio eletrônico ou ***e-mail*** - sistema de comunicação baseado no envio e no recebimento de mensagens eletrônicas via *Internet.* Indica tanto o ambiente da Internet onde você envia mensagens eletrônicas como a própria mensagem eletrônica em si.

CPU - *Central Processing Unit* ou Unidade Central de Processamento. É a unidade que leva e traz instruções da memória do computador e as decodifica para controlar todas as outras partes do computador.

Cracker - pessoa que usa os serviços da Internet para lesar outras pessoas.

Criptografia - ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.

Cybercafés – estabelecimentos comerciais, como bares, restaurantes e lanchonetes que disponibilizam ao usuário um serviço de *Internet,* além de outros, tais como: digitação de texto, consultas virtuais, etc.

Cyberpunks – pessoas que são especialistas em quebra de senhas e entrada não autorizada em sistemas de informática.

Cyberspace - há um limite para a quantidade de dados que qualquer tipo de fio/cabo/canal pode transportar num determinado momento, mesmo no caso de fibras óticas; a capacidade de armazenamento de um sistema. É o espaço eletrônico e onde ocorrem as transações na *Internet.*

DARPA ou *Defense Advanced Research Projects Agency* - organização central de pesquisa e desenvolvimento do Departamento de Defesa norte-americano.

DDoS - do Inglês *Distributed Denial of Service*. Ataque de negação de serviço distribuído, ou seja,

um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à *Internet.* Veja Negação de serviço.

***DHTML* -** sigla para *Dynamic Hipertext Markup Language*. É um tipo de linguagem utilizada para construir as páginas da *Web* e os *websites* com recursos de acesso dinâmico.

***Disclaimers* -** informações disponibilizadas pelo provedor para restringir ou limitar responsabilidades de informações ou de ações lançadas pelos usuários na rede.

Disco rígido - é o disco interno ao computador onde os dados são armazenados.

DNS - do Inglês *Domain Name System*. Serviço que traduz nomes de domínios para endereços IP e vice-versa. DNS significa *Domain Name Server*. É um sistema hierárquico de bases de dados distribuídas que converte um nome de domínio em um endereço IP do computador/servidor *Internet* de um provedor de acesso e hospedagem de *websites*.

Domain Names - nomes de domínio.

Domínio - nome de uma área reservada num servidor *Internet* que corresponde ao endereço numerico de um *website* (endereço IP). No Brasil, os domínios sempre terminam com .br (sigla do Brasil na *Internet*) e podem apresentar vários tipos (.com para empresas comerciais, .org para empresas não comerciais, etc.). Ex: aisa.com.br é um domínio brasileiro do tipo comercial (o mais comumente usado).

DoS - do Inglês *Denial of Service*. Veja Negação de serviço.

Download - ato de copiar um arquivo de um *website* qualquer disponível na *Internet* para o seu computador pessoal.

E-commerce ou **comércio eletrônico** - realização de negócios através da *Internet.*

E-mail - Significa correio eletrônico e indica tanto o ambiente da Internet onde você envia mensagens eletrônicas como a própria mensagem eletrônica em si.

Endereço *IP* - este endereço é um número único para cada computador conectado à *Internet*, composto por uma sequência de 4 números que variam de 0 até 255, separados por «.». Por exemplo: 192.168.34.25. É o endereço de cada servidor conectado à *Internet*, de acordo com o *Internet Protocol*.

Engenharia social - método de ataque onde uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

***Excel* –** programa de computador.

Exploit - programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um software de computador.

Falsa identidade - ato onde o falsificador atribui-se identidade ilegítima, podendo se fazer passar por outra pessoa, com objetivo de obter vantagens indevidas, como por exemplo, obter crédito, furtar dinheiro de contas bancárias das vítimas, utilizar cartões de crédito de terceiros, entre outras.

Filtro *anti-spam* - programa que permite separar os *e-mails* conforme regras pré-definidas. Originalmente era utilizado para o gerenciamento das caixas postais. No entanto, com o crescimento do volume de *spams* na rede, tornou-se um importante recurso técnico para a seleção de e-mails válidos, dentre os diversos *spams* recebidos.

Filtros - são formas de diminuir o escopo de consultas pela definição de áreas ou tipos de dados a serem incluídos ou excluídos.

***Firefox* –** navegação livre e multiplataforma desenvolvido pela *Mozilla Foundation* com ajuda de centenas de colaboradores.

Firewall - dispositivo constituído pela combinação de *software* e *hardware,* utilizado para dividir e controlar o acesso entre redes de computadores.

***Firewall* pessoal** - *software* ou programa utilizado para proteger um computador contra acessos não autorizados vindos da *Internet*. É um tipo específico de *firewall.*

Flogs – *p*áginas construídas na *Internet* com conteúdo de ordem pessoal.

Formulários - são páginas HTML usadas para coletar informações dos internautas. São também, chamadas *"scripts".*

Fowarding – trecho de passagem entre o roteador e a mensagem.

Freeware - são programas de computador de domínio público, ou seja, são gratuitos e podem ser usados à vontade pelos internautas.

FTP ou ***File Transfer Protocol*** - significa protocolo de transferência de arquivos pela Internet. É o método padrão de enviar arquivos entre computadores pela Internet.

Gateway - porta de entrada de cada rede individual ligada à Internet.

Hackers - são especialistas em violar sistemas de computação.

Hard Disk - disco rígido.

Hardware - estrutura e as peças eletrônicas, magnéticas e mecânicas de um computador.

Hipermídia - mídia que inclui gráficos, sons e vídeos.

Hipertexto - texto em formato de cruzamentos. O hipertexto permite os saltos de um assunto para outro ou de uma página para a outra através de *hiperlinks* ou *links*.

Hoax - boato.

Homepage - página de entrada ou página principal de um *website*. É nesta página que estão os *links* para as demais páginas do *website.*

Hop – salto.

Hospedagem - ato de armazenar *websites* de clientes por parte de um provedor de acesso.

Host - é um computador numa rede de computadores.

HTML - do Inglês *HyperText Markup Language*. Linguagem universal utilizada na elaboração de páginas na *Internet.*

HTTP - *Hyper Text Transfer Protocol* é o protocolo padrão que permite a transferência de dados na Web entre os servidores e os *browsers.* É este protocolo que permite os saltos de uma página para a outra através dos *links* do hipertexto.

HTTPS - quando utilizado como parte de uma URL, especifica a utilização de HTTP com algum mecanismo de segurança, normalmente o SSL.

Internauta - gíria usada para identificar o usuário da Internet, a pessoa que usa a Internet para comunicação, pesquisa, trabalho e/ou lazer.

Internet **-** rede mundial de computadores interconectados. É o sistema de informação global que: a) é logicamente ligado por um endereço único global baseado no *Internet Protocol* (IP) ou suas subsequentes extensões; b) é capaz de suportar comunicações usando o *Transmission Control Protocol/ Internet Protocol* (TCP/IP) ou suas subsequentes extensões e/ou outros protocolos compatíveis ao IP; e c) provê, usa ou torna acessível, tanto publicamente como privadamente, serviços de mais alto nível produzidos na infra-estrutura descrita.

Internet Banking – serviço virtual disponibilizado pelas instituições bancárias para que o cliente para fazer pagamentos, emitir extratos, transferências, aplicações financeiras, etc.

Internet Society – comunidade da *Internet.*

Intranet - rede baseada em protocolos TCP/IP (uma *internet*) que pertence a uma empresa e que é acessada apenas pelos membros e funcionários da empresa (e, eventualmente, também por outras pessoas que tenham autorização para tal). Como a *Internet, intranets* são usadas para compartilhar informações.

Invasão - ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações em um computador.

Invasor - pessoa responsável pela realização de uma invasão (comprometimento). Veja também Invasão.

IP – veja Endereço *IP*.

IP**,** ou ***Internet Protocol*** – Protocolo da *Internet*. É este protocolo que identifica, localiza e estabelece conexão entre computadores ligados à *Internet*.

IRC – significa *Internet Relay Chat*. Também conhecido como "bate-papo", é um ambiente que permite comunicação escrita *online* entre usuários da *Internet.*

ISP – significa *Internet Service Provider* ou provedor de acesso à *Internet*. ***Keylogger*** - Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um site de comércio eletrônico ou *Internet Banking*, para a captura de senhas bancárias ou números de cartões de crédito.

LAN – significa *Local Area Network*. É uma rede local de computadores localizados em uma área relativamente pequena.

***Laptop* –** computador pequeno e portátil que você pode colocar no seu colo (*top*=em cima e *lap*=-colo em inglês). Também conhecido como *notebook*.

Largura de banda – quantidade de dados que podem ser transmitidos em um canal de comunicação, em um determinado intervalo de tempo.

***Links* –** são palavras ou ilustrações pré-estabelecidas como pontos de saltos. Quando clicadas, provocam a transferência para outro assunto ou página *Web*.

***Log* –** arquivo criado por um servidor *web* que contém todas as informações de acessos à *Internet* considerando a atividade do servidor.

***Login* –** pode significar: a) o ato de acessar a *Internet*; b) o seu nome de usuário para o acesso à *Internet* (cadastrado em um provedor em conjunto com uma senha) ou para o acesso a um *website* que porventura exija um cadastramento prévio do internauta (neste caso, o cadastramento do *login* é feito no *website*).

***Mail-Bomb* –** mensagem virtual que contém um explosivo, conhecido com arquivo maligno capaz de causar danos ao usuário.

Malware – do Inglês *Malicious software* (*software* malicioso). Veja Código malicioso.

MB – significa *MegaByte*. É uma medida de armazenamento em espaço em disco igual a 1.024 KB ou 1.048.576 bits.

***Megabytes* –** unidade de medida que corresponde a 1.048.576 *bytes*.

Microcomputador - é um computador de pequeno porte. É também chamado PC, sigla para *Personal Computer* (computador pessoal).

Modem – dispositivo que permite o envio e recebimento de dados utilizando as linhas telefônicas. É a sigla para *MOdulator/DEModulator*. É um equipamento que transforma os sinais digitais de seu microcomputador em sinais analógicos que podem viajar através de uma linha telefônica. O som que você ouve quando faz a discagem para o seu provedor de acesso informa que a ligação foi feita e que os sinais analógicos enviados do seu micro chegaram em um dos *modens* de recepção do provedor. A partir daí, os sinais analógicos são convertidos novamente em informação digital, tornando possível o seu acesso à Internet.

Navegação – é o processo de se mover de um *website* para outro seguindo *links.*

***NCP* -** significa *Network Control Protocol*, ou protocolo de controle de redes.

Negação de serviço – atividade maliciosa onde o atacante utiliza um computador para tirar de operação um serviço ou computador conectado à *Internet*.

Newsgroups – são grupos de notícias sobre assuntos diversos enviadas a internautas pré-cadastrados.

***Nicks* –** apelido, pseudônimo utilizado pelos *hackers* na *Internet*.

Notebook – é um computador pessoal pequeno leve e portátil. *Notebook* significa caderno em inglês.

Número IP – veja Endereço IP.

Online – significa ligado e conectado. Usuários estão *on-line* quando estão conectados com a Internet através de um modem.

Opt-in – regra de envio de mensagens que define que é proibido mandar *e-mails* comerciais/spam, a menos que exista uma concordância prévia por parte do destinatário. Veja também *Soft opt-in*.

Opt-out – regra de envio de mensagens que define que é permitido mandar *e-mails* comerciais/*spam*, mas deve-se prover um mecanismo para que o destinatário possa parar de receber as mensagens.

Orkut – comunidades Virtuais, agrupamentos de pessoas que se reúnem na rede para abordar diversos assuntos em comum. Ex: Comunidade virtual dos alunos que discute a respeito dos professores de uma universidade.

***Outlook Express* –** programa que permite a conexão via *e-mail.*

Page view – é o número de *hits* exclusivamente para páginas HTML. É também chamado "*page impression*".

Página – É o conjunto de textos e ilustrações que são mostrados em uma mesma tela.

Password – quer dizer palavra-chave ou senha. Normalmente é associada a um *login* por questão de segurança.

Phishing – também conhecido como *phishing scam* ou *phishing/scam*. Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na *Internet*.

***Phreackers* –** espécie de *hacker* que é especialista em burlar sistema de comunicações, como por exemplo, fazer ligações internacionais sem efetuar o pagamento.

Pirata da rede – pessoa que utiliza a *Internet* com fins maliciosos. Também conhecido como *Cracker*.

Plataforma – É o sistema operacional utilizado pelo internauta (*Windows 95, NT, Unix*, etc.).

POP – significa *Point of Presence*. São os pontos de presença dos *backbones Internet* em cada cidade onde o *backbone* oferece serviço aos provedores de acesso.

Porta dos fundos – Veja *Backdoor*.

Portal – é uma página ou *website* que agrega vários *links* e serviços, servindo como porta de entrada ou ponto de partida para a navegação de internautas.

Protocolo – é um formato estabelecido para a transmissão de dados entre dois dispositivos de

computadores (*drives*, impressoras e *modens*, por exemplo). Protocolos definem o tipo de consistência e checagem de erros, o método de compressão de dados, a forma como o dispositivo de envio indicará que a mensagem está terminada e a forma como o dispositivo de recebimento indicará que recebeu a mensagem.

Provedor de acesso – é uma empresa que provê acesso à *Internet* aos seus clientes através da manutenção de uma central de linhas telefônicas exclusivas ligadas aos seus servidores de serviços *Internet*.

Provedor de informação – é uma empresa que provê informações variadas em seu *website.*

***Proxi* –** gerador de programas aplicativos. Produz um código fonte legível e consistente que facilita as tarefas de manutenção.

Proxy – servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar a performance de acesso a determinados serviços ou permitir que mais de uma máquina se conecte à *Internet*.

***Proxy* Aberto** – *proxy* mal configurado que pode ser abusado por atacantes e utilizado como uma forma de tornar anônimas algumas ações na *Internet*, como atacar outras redes ou enviar *spam.*

***Real Time* –** em tempo real.

Roteador ou **router** – é um equipamento que conecta qualquer número de *LANs* e otimiza o roteamento das conexões *Internet*.

Scam – esquemas ou ações enganosas e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras.

Scan – técnica normalmente implementada por um tipo de programa, projetado para efetuar varreduras em redes de computadores. Veja *Scanner.*

Scanner – programa utilizado para efetuar varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

Screenlogger – forma avançada de *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado. Veja também *Keylogger.*

Senha - conjunto de caracteres, de conhecimento único do usuário, utilizado no processo de verificação de sua identidade, assegurando que ele é realmente quem diz ser. É uma palavra qualquer escolhida pelo usuário que, em conjunto com o *login*, serve para liberar o acesso do usuário à *Internet* ou a *websites* que porventura exijam senha para entrada.

Servidor – computador que administra e fornece programas e informações para os computadores conectados em sua rede.

SET – sigla para *Secure Eletronic Transaction*. É um padrão de segurança utilizado em *websites* de comércio eletrônico.

Site – local na *Internet* identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações multimídia.

Sítio – página da *Internet*.

Soft opt-in – regra semelhante ao *opt-in*, mas neste caso prevê uma exceção quando já existe uma relação comercial entre remetente e destinatário. Dessa forma, não é necessária a permissão explícita por parte do destinatário para receber *e-mails* desse remetente. Veja *Spam* - Termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem também é referenciada como UCE (do Inglês *Unsolicited Commercial E-mail*).

Software – são os programas, dados e rotinas desenvolvidos para computadores. Os programas de software precisam ser instalados nos computadores para que eles passem a desempenhar determinadas funções.

Spam – envio de *e-mails* comerciais não solicitados - um grave erro e fonte de problemas na *Internet*.

Spammer – pessoa que envia *spam*.

Spider – é um programa automatizado que faz buscas pela *Internet*.

Spyware – termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

SSH – do Inglês *Secure Shell*. Protocolo que utiliza criptografia para acesso a um computador remoto, permitindo a execução de comandos, transferência de arquivos, entre outros.

SSL – do Inglês *Secure Sockets Layer*. Protocolo que fornece confidencialidade e integridade na comunicação entre um cliente e um servidor, através do uso de criptografia. Veja também HTTPS.

TCP/IP – *Transmission Control Protocol/Internet Protocol* (ou protocolo de controle de transmissão/protocolo *Internet*). É o protocolo que satisfaz as necessidades de um ambiente de redes de arquitetura aberta como a *Internet*.

Telnet – é uma aplicação onde o internauta acessa um servidor remoto pela *Internet.*

Trojan horse – veja Cavalo de troia.

UNIX - é um sistema operacional de alta performance escrito em C (linguagem de alto nível).

URL – do *Inglês Universal Resource Locator*. Seqüência de caracteres que indica a localização de um recurso na Internet, como por exemplo, http://cartilha.cert.br/.

URL – significa *Uniform Resouce Locator*. Uma URL é um endereço virtual que indica exatamente onde as informações da empresa ou da pessoa se encontram. A primeira parte do endereço indica que protocolo está sendo usado e a segunda parte do endereço especifica o domínio onde o recurso está localizado, no formato http://www.domínio.tipododominio.sigladopaís.

Vírus – programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O *vírus* depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

VRML ou ***Virtual Reality Modeling Language*** – é um padrão de programação que permite modelagem e navegação em terceira dimensão na *Web.*

WAN ou ***Wide Area Network*** – é um sistema de *LANs* interconectadas através de linhas telefônicas ou ondas de rádio.

WAP ou ***Wireless Application Protocol*** - é uma especificação segura que permite aos usuários acessar informações e a *Internet* através de equipamentos portáveis, móveis e *wireless* como celulares e *pagers*.

Warez – pessoas que copiam programas de computador de forma ilegal e distribuem gratuitamente na *Internet.*

Web – é o ambiente multimídia *Internet*, também conhecido como *WWW*. *Web,* especialmente HTTP, HTML e XML. O W3C foi fundado em 1994 por Tim Berners-Lee, considerado o inventor da *Web.* W3C significa *World Wide Web Consortium* e é a organização oficial para os padrões

Webcan – equipamento que permite a filmagem e visualização no endereço de destino do que está sendo filmado se o usuário se conecta ao outro usuário na *Internet* e o destinatário aceita o programa para que possa ter as imagens em tempo real.

Webmaster – é o profissional responsável por um ou mais *websites*.

Website – é um conjunto de páginas ou lugar no ambiente *Web* da *Internet* que é ocupado com informações (texto, fotos, animações gráficas, sons e até vídeos) de uma empresa ou de uma pessoa.

Word – programa de computador.

Worm – programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do *vírus*, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores.

WWW – significa *World Wide Web* e é o ambiente multimídia da *Internet,* a reunião de texto, imagem, som, vídeo e movimento na *Internet.*

ZIP – *a*rquivo compactado.

Sobre a autora

Neide Aparecida Ribeiro

Doutora em Educação (UCB). Mestre em Direito Público (UFG). Especialista em Direito Processual Penal e Direito Constitucional (UFG). Especializanda em Direito à Saúde (Verbo Jurídico). Bacharel em Direito (UFG). Professora efetiva do Curso de Direito da UNITINS no Câmpus de Palmas/TO. Integra como membro do Comitê Técnico-Científico Institucional (CTCI) da UNITINS. Membro do Conselho Penitenciário do Estado do Tocantins. Pesquisadora. Advogada. Email: neide.ar@unitins.br


EDITORA
UNITINS