UNIVERSIDADE DO ESTADO DE SANTA CATARINA - UDESC
CENTRO DE CIÊNCIAS TECNOLÓGICAS - CCT
MESTRADO EM COMPUTAÇÃO APLICADA

JULIANA DE PAULA SANTOS

HACKING LEGAL E *FISHING EXPEDITION*: UMA ANÁLISE DAS PRÁTICAS SOB PERSPECTIVAS DAS LEGISLAÇÕES DO BRASIL E EUROPA

JOINVILLE

2025

JULIANA DE PAULA SANTOS

HACKING LEGAL E *FISHING EXPEDITION*: UMA ANÁLISE DAS PRÁTICAS SOB PERSPECTIVAS DAS LEGISLAÇÕES DO BRASIL E EUROPA

Dissertação submetida ao Programa de Pós-Graduação em Computação Aplicada do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina, para a obtenção do grau de Mestre em Computação Aplicada.

Orientador: Dr. Charles Christian Miers

JOINVILLE

2025

Ficha catalográfica elaborada pelo programa de geração automática da

Biblioteca Universitária Udesc,

com os dados fornecidos pelo(a) autor(a)

Paula Santos, Juliana de
Hacking Legal e Fishing Expedition: uma análise das práticas sob perspectivas das legislações do Brasil e Europa / Juliana de Paula Santos. -- 2025.
103 p.

Orientador: Charles Christian Miers
Dissertação (mestrado) -- Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação em Computação Aplicada, Joinville, 2025.

1. Hacking Legal. 2. Fishing Expedition. 3. LGPD. 4. GDPR. 5. Cadeia de custódia. I. Christian Miers, Charles. II. Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação em Computação Aplicada. III. Título.

Juliana de Paula Santos

***Hacking Legal* e *Fishing Expedition*: uma análise das práticas sob perspectivas das legislações do Brasil e Europa**

Esta dissertação foi julgada adequada para a obtenção do título de **Mestre em Computação Aplicada** área de concentração em "Sistemas de Computação", e aprovada em sua forma final pelo Curso de Mestrado em Computação Aplicada do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina.

Banca Examinadora:

Dr. Charles Christian Miers - UDESC
Orientador

Dr. Guilherme Piêgas Koslovski - UDESC

Dr. Mehran Misaghi - IFC

Joinville, 27 de agosto de 2025

Dedicado ao desenvolvimento tecno-científico de Santa Catarina e do Brasil.

AGRADECIMENTOS

Agradeço ao meu orientador, Prof. Charles Christian Mirs pelos valiosos ensinamentos. Também desejo de agradecer a Universidade do Estado de Santa Catarina (UDESC), aos professores do Programa de Pós-Graduação em Computação Aplicada (PPGCAP) e ao Laboratório de Processamento Paralelo Distribuído (LabP2D).

"Feliz aquele que transfere o que sabe e aprende o que ensina."
Cora Coralina

RESUMO

Os governos vêm intensificando a prática de coletar dispositivos portáteis e computadores na busca de informações úteis em investigações criminais e de segurança nacional. Diversos destes dispositivos empregam serviços executados em nuvens e provedores remotos que acabam sendo envolvidos neste procedimento. Depara-se, então, com uso da tecnologia para combater uma criminalidade cada vez mais cibernética. Duas práticas investigativas são o *Hacking Legal* e *Fishing Expedition*. A imprescindibilidade de regramento que harmonize o uso destas práticas de forma a se alcançar o equilíbrio entre a persecução penal, a segurança nacional, a proteção dos dados pessoais e a cadeia de custódia de vestígios digitais, em consonância com a legislação vigente como o General Data Protection Regulation (GDPR) e a Lei Geral de Proteção de Dados Pessoais (LGPD), constitui a problemática desta pesquisa. Este trabalho apresenta uma revisão e uma proposta de análise da viabilidade e as implicações das práticas de *Hacking Legal* e *Fishing Expedition* para lidar com a necessidade das agências policiais e de inteligência, abordando as ferramentas de extração de dados e a observância ao instituto da cadeia de custódia digital. Esta proposta transita entre os aspectos legais do ordenamento jurídico brasileiro e junto os tribunais internacionais, tendo como principal contribuição a consolidação do *Hacking Legal*, *Fishing Expedition*, frente a LGPD e GDPR, levando em consideração a cadeia de custódia digital, usando bases acadêmicas e do judiciário federal brasileiro. Por fim, adiciona-se os aspectos técnicos e a tecnologia de forma a proporcionar uma ligação entre profissionais da segurança da informação e agentes do direito e do governo.

Palavras-chaves: Investigação Criminal, Segurança Nacional, Práticas Investigativas, *Hacking Legal*, *Fishing Expedition*, Cadeia de Custódia, Proteção das Dados Pessoais, GDPR, LGPD.

ABSTRACT

Governments have been intensifying the practice of collecting portable devices and computers in search of helpful information in criminal and national security investigations. Several of these devices employ cloud-based services and remote providers that end up being involved in this process. Then, technology is being used to combat increasing cybercrime. Two investigative practices are Legal Hacking and Fishing Expedition. The essential need for regulations that harmonize the use of these practices in order to achieve a balance between criminal prosecution, national security, personal data protection, and the chain of custody of digital traces, in line with current legislation such as the GDPR and LGPD, constitutes the focus of this research. This master's thesis presents a review and a proposal for analyzing the feasibility and implications of Legal Hacking and Fishing Expedition practices to address the needs of law enforcement and intelligence agencies, observing data extraction tools and the digital chain of custody. This proposal addresses the legal aspects of the Brazilian legal system and international courts, with its main contribution being the consolidation of Hacking Legal and Fishing Expedition, in the face of LGPD and GDPR, taking into account the digital chain of custody, using academic bases and the Brazilian federal judiciary. Finally, it incorporates technical aspects and technology to provide a link between information security professionals, law enforcement, and government officials.

Key-words: Criminal Investigation, National Security, Investigative Practices, Legal Hacking, Fishing Expedition, Chain of Custody, Personal Data Protection, GDPR, LGPD.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ANPD Autoridade Nacional de Proteção de Dados

APL Anteprojeto de Lei de Proteção de Dados Pessoais para Segurança Pública e Persecução Penal

CRFB/88 Constituição da República Federativa do Brasil de 1988

CEDH Convenção Europeia dos Direitos Humanos

CE Conselho da Europa

CDC Código de Defesa do Consumidor

CIA *Central Intelligence Agency*

CP Código Penal

CPP Código Processo Penal

CNJ Conselho Nacional de Justiça

DECCC Diretoria Estadual de Combate a Crimes Cibernéticos

EDL *Emergency Download Mode*

FBI *Federal Bureau of Investigation*

FE *Fishing Expedition*

GDPR General Data Protection Regulation

HL *Hacking Legal*

ISO *International Organization for Standardization*

LGPD Lei Geral de Proteção de Dados Pessoais

MDFT Mobile Device Forensic Tools

NSA *National Security Agency*

OCDE Organização para Cooperação e Desenvolvimento Econômico

PGR Procuradoria Geral da República

RSL *Revisão Sistemática da Literatura*

SENASP Secretaria Nacional de Segurança Pública

SGPI Sistema de Gestão da Privacidade da Informação

STJ Superior Tribunal de Justiça

STF Supremo Tribunal Federal

UE União Europeia

UFED Universal Forensic Extraction Device

USA *United States of America*

LabP2D Laboratório de Processamento Paralelo Distribuído

PPGCAP Programa de Pós-Graduação em Computação Aplicada

UDESC Universidade do Estado de Santa Catarina

SUMÁRIO

1 INTRODUÇÃO

As inovações recentes em dispositivos portáteis mudaram o comportamento dos consumidores e sua forma de acessar serviços e redes. Esses acessos também cresceram em variedade e complexidade. Um reflexo dessa mudança está na transformação dos serviços de comunicação, passando de um relacionamento direto cliente-provedor para um ambiente complexo, sendo possível a utilização de vários métodos de acesso para manter interações simultâneas com múltiplos provedores (BELLOVIN et al., 2014). Noutro vértice, surge a preocupação das agências policiais e de inteligência de "ficarem no escuro" (*Going Dark*) quanto ao teor de comunicação e armazenamento em dispositivos eletrônicos, à medida em que as comunicações digitais ficam inacessíveis à autoridade policial, favorecendo o cometimento de ilícitos (PEREIRA; RODRIGUES; VIEIRA, 2021).

Em síntese, a dinamicidade do mundo digital aponta desafios adicionais à atividade estatal de persecução penal. A globalização, a virtualização da economia e o surgimento contínuo de novas tecnologias passaram a exigir a atualização das técnicas de investigação na busca de uma tutela penal mais eficiente ao mesmo tempo em que os limites formais e materiais da atuação penal dos Estados devem se adequar ao contexto do direito fundamental à proteção dos dados pessoais. Nesse cenário, este trabalho expõe a viabilidade e as implicações das práticas investigativas do *Hacking Legal* e do *Fishing Expedition* à luz da necessidade das agências de investigação, da preservação da cadeia de custódia de meios da prova digital e do direito fundamental à proteção dos dados, a partir do contexto brasileiro e internacional.

Com vistas a fundamentar o trabalho é feita uma contextualização da regulamentação da proteção de dados na Europa e no Brasil, até a entrada em vigor das legislações específicas do General Data Protection Regulation (GDPR) e da Lei Geral de Proteção de Dados Pessoais (LGPD), respectivamente. Posteriormente, é apresentada uma explanação das práticas investigativas, cadeia de custódia, ferramentas de acesso remoto e de extração de dados digitais e definições pertinentes a estas práticas na persecução penal. Neste ponto, é dado destaque a dois temas. Primeiro, a cadeia de custódia (cuja preservação objetiva tutelar a identidade, integridade e autenticidade dos elementos de prova) uma vez que a produção da prova no processo penal, em especial nos crimes praticados por meio da Internet, seja por agentes virtualmente infiltrados ou em face de quebra de dados ou mesmo interceptação do fluxo das comunicações de informática, necessita respeitar a cadeia de custódia e adequar-se às exigências legais, de forma a garantir a privacidade dos dados pessoais e os direitos individuais da pessoa humana. Depois, o uso da ferramenta de extração de dados

Cellebrite, com utilização no Brasil pelas polícias científicas estaduais e federal, além de outros órgãos relacionados à segurança pública.

O problema principal deste trabalho exige uma solução no sentido de se buscar um equilíbrio que promova uma tutela penal eficiente e a proteção dos dados pessoais dos investigados. O objetivo é realizar uma análise comparativa apresentando uma visão geral do estado atual das práticas do *Hacking Legal* (HL) e do *Fishing Expedition* (FE) e os desafios à tecnologia e às regras de interceptação legal com vistas a explorar a flexibilização dos métodos de colheita de provas.

Através de uma *Revisão Sistemática da Literatura* (RSL) identificou-se os trabalhos relacionados/estado da arte das práticas abordadas e legislações aplicadas no âmbito nacional e internacional visando correlacionar aspectos legais e técnicos.

A execução do trabalho se dá por meio de uma composição de pesquisa referenciada e revisão bibliográfica aliada a pesquisa exploratória[1] junto a Polícia Científica do Estado de Santa Catarina, envolvendo estudo de caso. Desta forma, o trabalho sintetiza os conceitos obtidos na fundamentação com problema proposto envolvendo pesquisa bibliográfica somada a pesquisa exploratória, de forma a proporcionar a construção das contribuições. Importante pontuar que as literaturas referentes às práticas do *Hacking Legal* (HL) e do *Fishing Expedition* (FE) estão dispostas separadamente ou só na parte do Direito, muitas vezes em *blogs* e sítio jurídicos ou, então, na área de cibersegurança. Assim, a relevância deste trabalho é fazer a junção destas áreas, pois tal intersecção não é identificada e explorada conforme demonstra a revisão bibliográfica, visto que a formação acadêmica desta orientada é tanto bacharel em Engenharia Elétrica como em Direito, atuando profissionalmente na Justiça Federal.

Como principais contribuições desta pesquisa, pode-se citar:

1. Sistematização da Lei Geral de Proteção de Dados Pessoais (LGPD) e do General Data Protection Regulation (GDPR) com viés de direito e cibersegurança, fazendo uma análise da evolução história da normatização da proteção de dados no cenário brasileiro e europeu e sua aplicação na persecução penal relacionando as práticas do HL e FE.

2. Consolidação acerca do instituto da cadeia de custódia com viés no direito e cibersegurança, auxiliada por entrevista com a equipe técnica da Polícia Científica de Santa Catarina em Joinville.

[1] (GIL, 2002) define pesquisa exploratória como uma metodologia que tem como objetivo proporcionar maior familiaridade com o problema de pesquisa, envolvendo entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado e análise de exemplos que auxiliam a compreensão. Caracteriza-se por metodologias flexíveis, sem uso de questionários, observação e informações amplas, proximidade com o objeto de pesquisa.

3. Consolidação da aplicação das HL e FE, suas ferramentas, usando tanto bases acadêmicas como do judiciário federal brasileiro.
4. Comparativo de HL vs FE levando em consideração aspectos da cadeia de custódia frente a LGPD e GDPR.
5. Estudo de caso acerca da ferramenta Cellebrite Universal Forensic Extraction Device (UFED) com ênfase nas técnicas de acesso e extração de dados em dispositivos móveis.

O texto está organizado em cinco capítulos, incluída esta introdução. O Capítulo 2 apresenta a fundamentação, mostrando, primeiramente, o contexto histórico das legislações que envolvem a proteção de dados na Europa e no Brasil, as práticas investigativas na persecução penal e a cadeia de custódia da prova digital. Depois do levantamento conceitual-teórico, é apresentada a definição do problema. No Capítulo 3, os aspectos relevantes das práticas investigativas do HL e do FE são abordados. Além disto, estão detalhados os passos da RSL, bem como as questões e processo de pesquisa. Também estão identificados os trabalhos relacionados. O Capítulo 4 dedica-se à apresentação e análise das ferramentas de *hacking*, tanto para acesso remoto de dados armazenados ou em trânsito, quanto para extração de dados digitais via acesso físico a dispositivo de armazenamento. Deu-se ênfase à ferramenta da empresa Cellebrite (estudo de caso). O Capítulo 5 apresenta as considerações finais e as produções decorrentes desta pesquisa.

2 FUNDAMENTAÇÃO

A partir da década de 1970, com a disseminação do uso de tecnologias de informação e o advento das mídias sociais, novas interrelações surgiram entre a vida privada e econômica dos indivíduos (FERREIRA; PINHEIRO; MARQUES, 2021). As pessoas passaram a ser vistas como um dado estatístico sendo seus dados pessoais considerados insumos para diversas áreas como saúde, educação, comércio virtual, redes sociais, governança, dentre outras. Entretanto, as possibilidades de uso da tecnologia, por meio da busca de provas, dados e informações, armazenados ou em trânsito, têm alterado as formas tradicionais de investigação criminal (SAAD, 2021). Noutro vértice, surgem questões relativas a proteção do sigilo das comunicações e privacidade, bem como ao uso de dados pessoais no âmbito da segurança pública e em investigações criminais. A preocupação com a segurança e a proteção dos dados pessoais vem exigindo reflexão e esforços a fim de identificar problemas prementes, desenhar limites, verificar a suficiência da regulação normativa/legislação e sua excepcionalidade, bem como a expansão do uso das tecnologias de vigilância, especialmente em meio digital, na investigação criminal.

Este capítulo apresenta uma fundamentação das práticas, regulamentos, normas e leis relacionadas às necessidades de segurança cibernética. Além disto, este capítulo discorre acerca da legislação europeia - General Data Protection Regulation (GDPR) - e brasileira - Lei Geral de Proteção de Dados Pessoais (LGPD) - apresentando breve comparação e, ainda, introduz os conceitos de práticas institucionais para obtenção de dados investigativos. Por fim, apresenta a definição do problema. Na Seção 2.1, realiza-se um estudo para identificar as legislações relacionadas a segurança dos dados pessoais com vistas a apresentar um histórico no cenário europeu e brasileiro. A Seção 2.2 mostra uma visão geral das legislações GDPR e LGPD, apresentando os mapas mentais elaborados para definição dos critérios comparativos e a evolução de cada uma sintetizada em uma linha do tempo. A Seção 2.3 apresenta uma breve comparação entre as legislações GDPR e LGPD destacando correlações, exceções e atualizações. As legislações são comparadas de acordo com os critérios apresentados na seção anterior. Na Seção 2.4 são conceituadas as principais práticas institucionais para obtenção de dados investigativos. São discutidos aspectos gerais de segurança e proteção dos dados na cadeia investigativa. A partir dos conceitos e do cenário levantado, esta seção faz uma definição do problema circundado por este trabalho na Seção 2.6. Também são levantados quais os atores envolvidos no problema, as consequências e as limitações relacionadas à aplicação das práticas do *Hacking Legal* (HL) e *Fishing Expedition* (FE) no âmbito das investigações criminais.

2.1 CONTEXTO E EVOLUÇÃO HISTÓRICA

Ao longo do tempo, vários documentos de direito internacional foram criados com a finalidade de proteger o direito à intimidade e à vida privada do indivíduo. Um dos primeiros instrumentos internacionais a tratar do direito à intimidade e à vida privada do indivíduo foi a Declaração Americana dos Direitos e Deveres do Homem, criada em 1948, em Bogotá, durante a IX Conferência Internacional Americana (FERREIRA; PINHEIRO; MARQUES, 2021). No mesmo ano, a Assembleia das Nações Unidas aprovou a Declaração Universal dos Direitos Humanos com vistas a promover o respeito aos direitos e liberdades, tanto nacional, quanto internacionalmente, entre os povos dos Estados-Membros. Reconheceu valores de proteção da privacidade individual e familiar e a liberdade de informação, opinião e de expressão, deixando claro que nenhum direito é absoluto - mesmo a privacidade pode ser limitada diante do que for estabelecido em lei - objetivando a preservação de direito e liberdades de terceiros, a moralidade, a ordem pública e o bem-estar social (ONU, 1948).

Na sequência, em 1950, a Convenção Europeia dos Direitos Humanos (CEDH) fez referência ao direito à privacidade e consagrou o direito de qualquer pessoa ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência e estabeleceu as condições em que são permitidas restrições a este direito (UE, 2023). A partir dessa base e com o progresso da tecnologia e a invenção da internet, a União Europeia (UE) reconheceu a necessidade de proteção mais moderna, por meio de legislação, para garantir o direito à privacidade. Nos anos de 1973 e 1974, o Conselho da Europa (CE) editou as Resoluções 22 e 29, respectivamente, para estabelecer princípios para a proteção de informações pessoais em bancos de dados automatizados, tanto no setor público, como no privado (NEVES, 2021). Mais tarde, em 1980, foram criadas as Diretrizes da Organização para Cooperação e Desenvolvimento Econômico (OCDE) sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais, que apesar de serem recomendações, constituíram um importante passo no sentido de harmonizar as legislações dos Estados-Membros e dos países interessados em ingressar na organização (EU, 2018).

Em 1981, o CE criou a Convenção 108, primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados. Essa convenção teve uma perspectiva universal, não sendo criada apenas para os países europeus, mas vinculando os Estados que a ratificaram. Conforme (EU, 2018), a Convenção 108 aplica-se a todo o tratamento de dados realizado tanto pelo setor público como pelo privado, incluindo o tratamento de dados pelas autoridades judiciárias e policiais. Com o passar do tempo, observou-se que a Convenção 108 não compreendia todos os aspectos necessários para uma ampla e densa disciplina de proteção da privacidade, o que levou a Comissão Europeia, provocada pelo seu Parlamento Europeu, a editar

um novo documento (MALDONADO; BLUM, 2021).

Surge, então, em 1995, a Diretiva 95/46/CE, estabelecendo uma definição básica de dados pessoais e outras delimitações importantes para a discussão do tema, além do incentivo ao comércio (EU, 2018). Resultou da necessidade de assegurar um elevado nível de proteção e a livre circulação de dados pessoais entre os diferentes Estados-Membros. Essa diretiva foi, por mais de 20 anos, o principal documento internacional sobre o assunto.

Em 2016, o GDPR assumiu o lugar da Diretiva 95/46/CE, sendo diretamente aplicado a todos os países-membros da UE (ERICKSON, 2019). Sua aprovação modernizou a legislação sobre proteção de dados na Europa, tornando-a apta para proteger os direitos fundamentais no contexto dos desafios econômicos e sociais da era digital e estabelecendo um ambiente de segurança jurídica, de que podem se beneficiar os operadores econômicos e os indivíduos, enquanto titulares dos dados (EU, 2018). Nesse mesmo ano de 2016, foi aprovada, em paralelo ao GDPR, a Diretiva (UE) 2016/680 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados (UE, 2016). Nessa linha do tempo, até 2018, no cenário brasileiro, não existia regulamentação que abordasse especificamente a problemática da proteção de dados. O assunto era indiretamente tratado em legislações esparsas (MALDONADO; BLUM, 2021).

A Constituição da República Federativa do Brasil de 1988 (CRFB/88), em seu Art. 5º, inciso XII, assegurou o direito à privacidade das informações pessoais ao dispor que "*é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal*". Importante destacar que os dados pessoais passaram a ser objeto de proteção constitucional por força da Emenda Constitucional nº 115/2022 que acrescentou o inciso LXXIX ao Art. 5º da CRFB/88, assegurando, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Além disso, outras leis desenharam de alguma forma a segurança dos dados pessoais no âmbito nacional (FERREIRA; PINHEIRO; MARQUES, 2021), como:

- Código de Defesa do Consumidor (CDC) (Lei nº 8.078/1990) - que prevê, em seu Art. 43, o direito à proteção dos dados pessoais assegurando ao consumidor o acesso às suas informações pessoais e de consumo, constante em cadastros, fichas, registros, bem como sobre suas respectivas fontes (BRASIL, 1990);

- Lei de Interceptação Telefônica e Telemática (Lei nº 9.296/1996) - que regulamentou o inciso XII, parte final, do Art. 5° da CRFB/88, cujo texto garante, como regra, o sigilo das correspondências e telecomunicações. O inciso constitucional permite, excepcionalmente, a quebra do sigilo, mediante o preenchimento de dois requisitos: que atenda as hipóteses e a forma prevista em lei; e que a finalidade seja investigação criminal ou produção de prova em processo penal. Atendendo ao comando constitucional, a mencionada lei descreve as hipóteses e as formalidades necessárias para a concessão judicial da quebra de sigilo (BRASIL, 1996);

- Lei do Sigilo Bancário (Lei Complementar nº 105/2001) - que dispõe sobre o sigilo das operações de instituições financeiras (BRASIL, 2001), estabelecendo que as operações ativas e passivas e serviços prestados entre uma instituição financeira e seu cliente estão protegidos por sigilo bancário, sendo uma garantia constitucional vinculada à intimidade e à vida privada do cidadão;

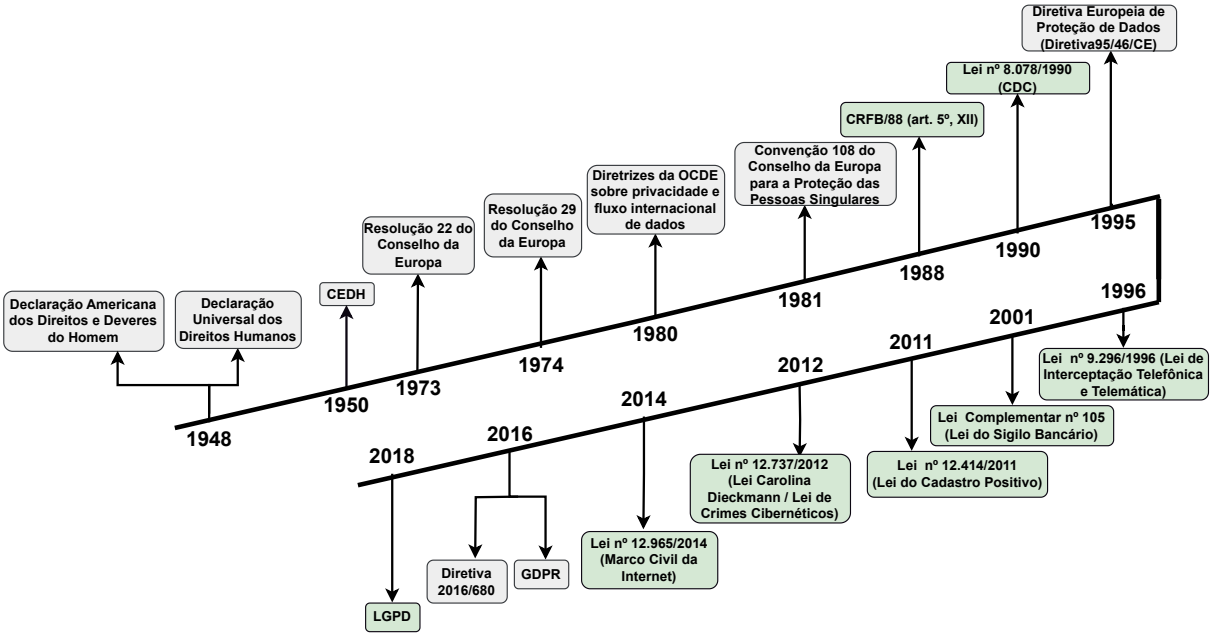
- Lei do Cadastro Positivo (Lei nº 12.414/2011) - que disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, bem como reconhece os direitos do titular dos dados, atrelando o tratamento à finalidade pretendida (BRASIL, 2011);

- Lei de Crimes Cibernéticos ou Lei Carolina Dieckmann (Lei nº 12.737/2012) - que alterou o Código Penal (CP) Brasileiro para tipificar os crimes cibernéticos com foco nas invasões a dispositivos, sem permissão do proprietário. Sua redação prevê crimes que decorrem do uso indevido de informações e materiais pessoais relativos à privacidade pessoal na internet (e.g., fotos e vídeos) (BRASIL, 2012); e

- Marco Civil da Internet (Lei nº 12.965/2014) - que disciplina os princípios, garantias, direitos e deveres para o uso na internet no Brasil, fundamentada no respeito à liberdade de expressão. A privacidade e a proteção dos dados foram abordados nos capítulos I e II, mais precisamente nos Art. 3º, 7º e 8º (BRASIL, 2014a).

Outrossim, as movimentações internacionais e a influência gerada pelo GDPR, destacaram a importância de se ter, no Brasil, uma legislação específica sobre proteção de dados, o que culminou na assinatura, em 2018, da LGPD. A Figura 1 retrata a evolução histórica das legislações na Europa e no Brasil, referentes a proteção de dados pessoais.

Figura 1 – Linha do tempo até GDPR e LGPD.



Fonte: A autora.

Neste contexto, pode-se dizer que as regulamentações sobre proteção de dados passaram por diversas fases até chegar ao momento atual quando o direito à proteção de dados adquire o enfoque de direito fundamental e passa a ter legislações específicas como GDPR e LGPD.

2.2 GDPR E LGPD

Em razão da extensão da presença da tecnologia na vida das pessoas, os dados pessoais estão sendo captados a todo o tempo, não só pelo que se digita nos aplicativos, redes sociais e sítios da Internet, mas também pelo que se fala (SILVA, 2018), resultado de uma sociedade cada vez mais conectada e produtora de informações. Esse volume de informações impõe um intenso tratamento de dados pessoais em diversas esferas, servindo, e.g., aos propósitos mercadológicos, i.e., marketing direcionado, com a oferta de produtos ou serviços mais adequados ao consumidor; à promoção da saúde com a adoção de tecnologias para maior assertividade em diagnósticos e tratamentos; às identidades digitais; à segurança pública; às atividades de investigação e prevenção de crime e, ainda, à prestação jurisdicional.

Nessa perspectiva, mostra-se necessário haver clara regulamentação da dimensão da invasão legal da intimidade e vida privada, i.e., quais devem ser os limites das autorizações judiciais para coletar e analisar estes dados. Como consequência dessa realidade, percebeu-se a relevância de leis que tutelassem o direito de privacidade e de proteção de dados dos cidadãos.

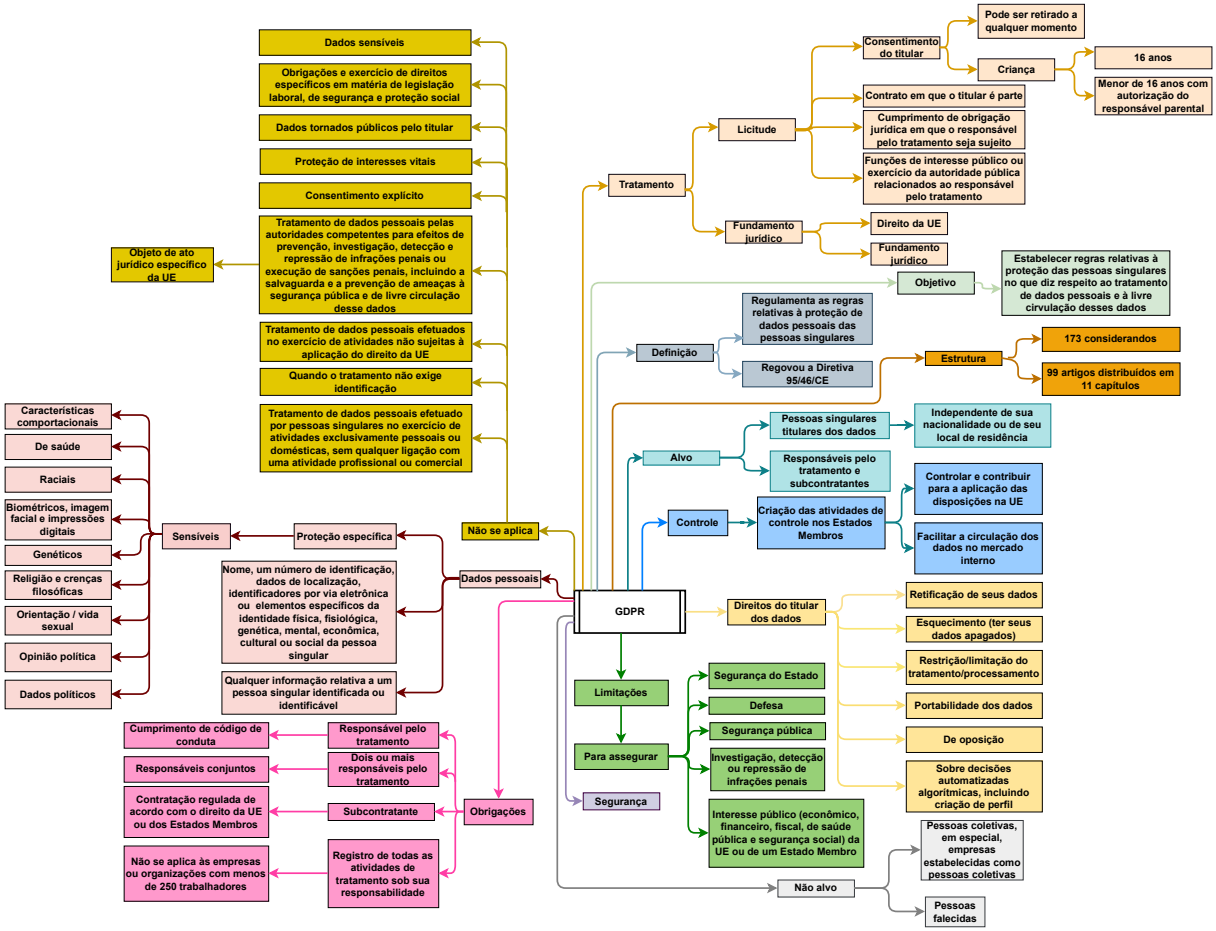
2.2.1 GDPR

À medida que a tecnologia avançava e a internet se tornava cada vez mais pervasiva, a UE reconheceu a necessidade de uma abordagem abrangente sobre a proteção de dados pessoais, que culminou na aprovação do GDPR.

O GDPR é a lei de proteção de dados europeia, aprovada pelo Conselho Europeu em 2016 e que entrou em vigor em maio de 2018, com o objetivo de unificar a proteção dos dados pessoais na UE. Consiste em 173 *recitals* (considerandos) e 99 artigos, com vistas a garantir a proteção dos dados pessoais utilizados por empresas em qualquer lugar, desde que tenham como alvo ou coletem dados relacionados a pessoas na UE (EU, 2016).

Este regulamento padroniza a lei de privacidade de dados da UE criando uma estrutura para uso entre os Estados Membros (ERICKSON, 2019). Contudo, os Estados Membros deverão atualizar as leis nacionais vigentes em matéria de proteção de dados de forma a obter o seu alinhamento total com o regulamento. A Figura 2 fornece uma visão geral deste marco regulatório.

Figura 2 – Principais aspectos organizacionais GDPR.



Fonte: A autora.

O GDPR contém regras detalhadas sobre o âmbito de aplicação territorial.

Aplica-se às empresas estabelecidas na UE, e também aos responsáveis pelo tratamento e aos subcontratantes não estabelecidos na UE que oferecem bens ou serviços a titulares dos dados na UE ou que controlam o seu comportamento (EU, 2016).

Nos termos do (EU, 2018), o GDPR preserva e desenvolve os princípios e direitos fundamentais do titular dos dados, além de introduzir novas obrigações que impõem às organizações a aplicação da proteção de dados, a designação de um encarregado da proteção de dados em determinadas circunstâncias, a observância de um novo direito de portabilidade dos dados e a observância do princípio da responsabilidade. Para tanto, em seu Art. 5º (EU, 2016) estabelece os princípios norteadores do tratamento dos dados pessoais na comunidade europeia, ilustrados na Figura 3.

Figura 3 – Princípios da proteção de dados GDPR.

Fonte: Adaptado de (EU, 2016).

Uma breve descrição dos princípios da GDPR (Figura 3):

- Licitude, lealdade e transparência - os titulares dos dados devem ser informados dos principais elementos de tratamento de seus dados pessoais de forma clara, acessível, concisa, transparente e inteligível;
- Limitação das finalidades - os dados devem ser tratados para uma finalidade específica;
- Minimização de dados - os dados pessoais devem ser adequados, pertinentes e limitados em relação aos fins para os quais processados. O objetivo é diminuir a quantidade de dados, coletando apenas aqueles que são essenciais ao produto ou serviço ofertado;
- Exatidão - os dados devem ser exatos e atualizados sempre que necessário;

- Limitação de armazenamento - os dados devem ser conservados de forma a permitir a identificação de seus titulares e apenas durante o período necessário para as finalidades para que são tratados;
- Integridade e confidencialidade - tratamento de forma a garantir a segurança dos dados; e
- Responsabilidade - exige que as organizações implementem medidas técnicas e organizacionais apropriadas, e sejam capazes de prestar contas e demonstrar eficácia, quando solicitadas.

A proteção de tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detenção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, e de livre circulação desses dados, é objeto de ato jurídico específico da UE. Tal matéria foi regulamentada pela Diretiva 2016/680 aprovada pelo Parlamento Europeu em 27/04/2016, tendo como objetivo promover a harmonização da legislação processual penal dos países membros da UE, estipulando instruções e orientações para a adaptação da atividade policial aos padrões tecnológicos atuais (UE, 2016).

Enquanto o GDPR estabelece regras gerais para proteger os indivíduos em relação ao tratamento dos seus dados pessoais e para garantir a livre circulação dos referidos dados na UE, a diretiva estabelece regras específicas relativas à proteção de dados nos domínios da cooperação judiciária em matéria penal e da cooperação policial (EU, 2018). Assim, quando uma autoridade competente trata dados pessoais para efeitos de prevenção, investigação, detecção ou repressão de infrações penais, é aplicável a Diretiva (UE) 2016/680. Por outro lado, quando trata dados pessoais para fins diferentes dos referidos, é aplicável o GDPR.

2.2.2 LGPD

A LGPD é a Lei nº 13.709/18 assinada em agosto de 2018 e com vigência a partir de 28/12/2018 quanto aos Arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; de 01/08/2021, quanto aos arts. 52, 53 e 54 e 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos (BRASIL, 2018).

A LGPD representa um marco histórico na regulamentação sobre o tratamento de dados pessoais no Brasil, tanto em meios físicos quanto em plataforma digitais, como para instituições públicas e privadas. A lei visa promover a proteção dos dados pessoais, relacionados à pessoa (brasileira ou não) que esteja no Brasil, no momento

da coleta; dados tratados dentro do território nacional, independentemente do meio aplicado, do país-sede do operador ou do país onde se localizam os dados; dados usados para fornecimento de bens ou serviços (SERPRO, 2023). Inspirada na regulação europeia sobre o tema enuncia, entre suas finalidades, “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (Art. 1º, LGPD). Tem como princípios norteadores, elencados em seu Art. 6º, a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização e prestação de contas.

Para (PINHEIRO, 2018) é um marco legal de impacto expressivo, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica.

Apesar de ter grande âmbito de aplicação, a LGPD, também como o GDPR, excetuou de seu escopo de aplicação as operações de tratamento de dados pessoais realizadas para fins exclusivos de segurança pública, defesa nacional, segurança de Estado e persecução penal, nos termos de seu Art. 4º, Inciso III. Previu, para a matéria, normatização por legislação específica, a ser aprovada pelo Congresso Nacional, e estabeleceu diretrizes para sua elaboração - a lei futura deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular já previstos na LGPD (Art. 4º, §1º, LGPD).

Com vistas a suprir esta lacuna legislativa, duas propostas de texto legal foram apresentadas sobre o tema: o Anteprojeto de Lei de Proteção de Dados Pessoais para Segurança Pública e Persecução Penal (APL) elaborado por uma comissão de juristas indicada pela Câmara dos Deputados, de novembro de 2020, informalmente denominada "LGPD Penal"e o Projeto de Lei nº 1515/2022 de autoria do deputado Coronel Armando, do Partido Liberal de Santa Catarina/SC (AZEVEDO, 2022).

O objeto do APL é proporcionar maior segurança jurídica para que os órgãos de investigação e repressão criminais pudessem exercer suas funções com maior eficiência e eficácia, sem perder de vista as garantias processuais penais e os direitos fundamentais dos titulares de dados envolvidos (BRASIL, 2020). Busca-se, nesta proposta, regular as atividades de tratamento dos dados na esfera penal de acordo com o grau de risco, delimitando-se a esfera de atuação das autoridades competentes e garantindo os princípios gerais de proteção e os direitos do titular (AZEVEDO, 2022).

O APL designa o Conselho Nacional de Justiça (CNJ) como autoridade de su-

pervisão do cumprimento da futura lei, opção distinta da adotada pela LGPD, que instituiu a Autoridade Nacional de Proteção de Dados (ANPD) para realizar a mesma função supervisora para tratamentos gerais. Atualmente, o APL se encontra na Câmara dos Deputados à espera de um parlamentar que o apresente formalmente, tornando-o assim um Projeto de Lei.

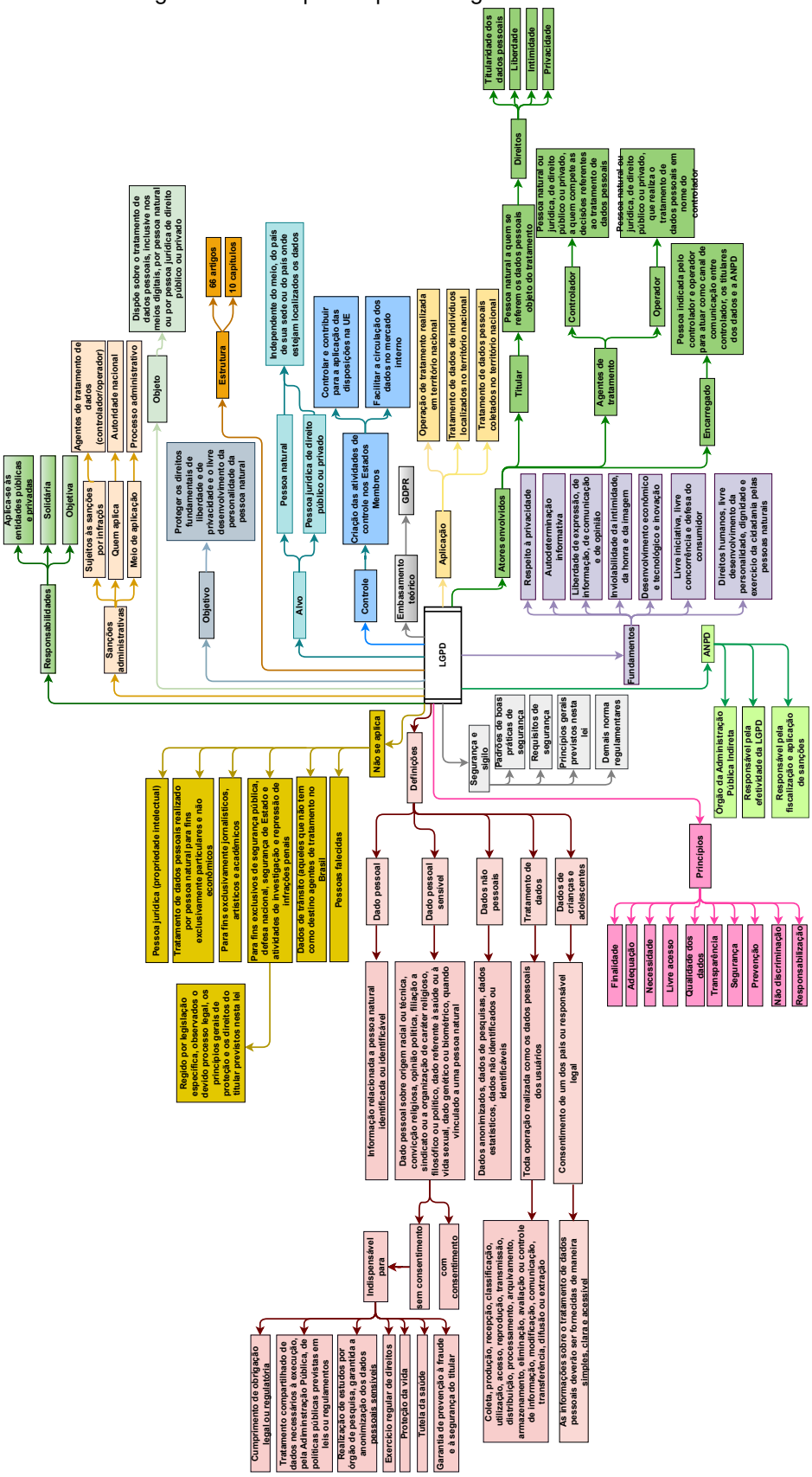
Nessa linha, visando suprir a mesma lacuna legal, em junho de 2022, o deputado Coronel Armando propôs o Projeto de Lei nº 1515/2022, em tramitação na Câmara dos Deputados, aguardando criação de Comissão Temporária pela Mesa Diretora. Tal projeto também abrange a aplicação da LGPD para fins de segurança do Estado, de defesa nacional, de segurança pública e de investigação e repressão de infrações penais. A proposta tem o objetivo de regular o Art. 4º, §1º, LGPD, que prevê regra específica para o tratamento de dados pessoais nestes casos. O projeto baseia-se em três pilares - proteção dos direitos fundamentais de segurança, liberdade e privacidade; eficiência da atuação dos órgãos responsáveis; e intercâmbio de dados pessoais entre autoridades competentes-, cabendo à ANPD supervisionar a proteção dos dados pessoais nas circunstâncias abrangidas (BRASIL, 2022).

Uma diferenciação importante entre os textos do APL e do Projeto de Lei nº 1515/2022 diz respeito ao escopo regulado. O APL se propõe a regular duas das exceções tratadas pela LGPD sobre o tema, quais sejam: o tratamento de dados pessoais para fins de segurança e persecução penal nos termos de seus Art. 3º e 4º (BRASIL, 2020). O Projeto de Lei nº 1515/2022 (BRASIL, 2022), por sua vez, enquadra em seu escopo de aplicação os tratamentos de dados para fins de segurança pública e persecução penal, além de defesa nacional, segurança de Estado e atividades de investigação e inteligência (Art. 1º, *caput* e § 2º).

Importante destacar, também, a norma ABNT NBR ISO/IEC 27701:2019, que estabelece requisitos para um Sistema de Gestão da Privacidade da Informação (SGPI), fornecendo diretrizes para as organizaçãoes (e.g. controladoras e operadoras de dados pessoais) para o estabelecimento, implementação, manutenção e melhoria contínua de um SGPI, com vistas a se adequarem à LGPD ((PPSI), 2024).

A Figura 4 resume os pontos abordados pela LGPD no âmbito do tratamento dos dados pessoais.

Figura 4 – Principais aspectos organizacionais LGPD.



Fonte: A autora.

2.3 COMPARAÇÃO ENTRE GDPR E LGPD

Considerando a proteção dos dados pessoais um direito fundamental das pessoais singulares, o GDPR determina que estes dados devem ser processados de forma legal, justa e transparente; coletados para fins explicitamente especificados e limitados; adequado, relevante e apenas minimizado ao necessário e, ainda, preciso e atualizado.

O GDPR define dados pessoais como qualquer informação relativa a uma pessoa singular identificada ou identificável (titular dos dados), elencando num rol exemplificativo quais são estes dados como: nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular (Art. 4º, GDPR). No mesmo viés, a LGPD conceitua, em seu Art. 5º, I, dados pessoais como "*informação relacionada a pessoa natural identificada ou identificável*". Quanto à aplicação, a legislação europeia se aplica ao tratamento de dados realizado por empresa nos termos de seu Art. 2º. Noutro vértice, a lei brasileira se dedica à proteção de dados de pessoas naturais, independentemente de quem realize o tratamento de dados, podendo ser uma pessoa natural ou jurídica, ressalvadas as exceções descritas de forma taxativa e restritiva no seu Art. 4º.

No que tange a abrangência territorial, o GDPR usa o critério da organização que possui estabelecimento na UE, enquanto a LGPD adota o critério de aplicação às operações de tratamento de dados realizadas no território brasileiro. Enquanto a LGPD se refere a dados relacionados à pessoa (brasileira ou não) que esteja no Brasil, no momento da coleta; dados tratados dentro do território nacional, independentemente do meio aplicado, do país-sede do operador ou do país onde se localizam os dados e; dados usados para fornecimento de bens ou serviços (WEISS, 2020); para o GDPR independe se o tratamento de dados acontece dentro ou fora do UE, pois adota o critério de localização física territorial do estabelecimento. Ou seja, o GDPR se aplica às empresas sediadas na UE, mesmo que não armazenem os dados em seu território (ERICKSON, 2019). Aplica-se, também, às empresas que, apesar de não estarem localizadas na UE, ofertam bens ou serviços a quem se encontra no território da UE, sendo irrelevante a cidadania do titular dos dados ou o país de sua residência (MALDONADO; BLUM, 2021). Na Tabela 1 estão relacionados os principais critérios comparativos entre as legislações de proteção de dados Europeia e Brasileira.

Tabela 1 – Critérios comparativos GDPR e LGPD.

Critério	GDPR	LGPD
Objeto	Estabelece regras relativas à proteção do tratamento de dados pessoais e à livre circulação desses dados	Dispõe sobre o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural
Objetivo	Proteção de dados pessoais das pessoas singulares	Proteção de dados pessoais das pessoas naturais
Estrutura	173 *Recitals* (Considerandos) e 99 Artigos distribuídos em 11 Capítulos	66 Artigos distribuídos em 10 Capítulos
Dados pessoais	Qualquer informação relativa a uma pessoa singular identificada ou identificável (titular de dados): nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular	Informação relacionada a pessoa natural identificada ou identificável
Aplicação material	Tratamento de dados pessoais efetuado por empresa por meios total ou parcialmente automatizados e por meios não automatizados	Tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado
Aplicação territorial	Tratamento de dados pessoais efetuados por: -empresa situada no território da União Europeia, independente do tratamento de dados ocorrer dentro ou fora dela; - empresa não estabelecida na União Europeia, de titulares residentes no território da União Europeia; - empresa não estabelecida na União Europeia, mas em local onde é aplicado o direito de um Estado-Membro	Tratamento de dados pessoais desde que: - operação de tratamento realizada em território nacional; - a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; - os dados pessoais do tratamento tenham sido coletados no território nacional
Não se aplica	- Dados de pessoas falecidas; - dados pessoais efetuados no exercício de atividades não sujeitas à aplicação do direito da UE; -quando o tratamento não exige identificação; - tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relacionadas com a política externa e de segurança comum da UE; - tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas e, portanto, sem qualquer ligação com uma atividade profissional ou comercial; - tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, e de livre circulação desses dados	- tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos; -para fins exclusivamente jornalísticos e não econômicos e acadêmicos; - para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais; - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado
Atores envolvidos	Titular dos dados: pessoa singular identificada ou identificável a quem se referem os dados. Agentes de tratamento: - Responsável pelo tratamento: a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; - Subcontratante: uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes; -Encarregado (DPO): coopera com a autoridade de controle e atua como ponto de contato entre responsável pelo tratamento, subcontratante e autoridade de controle	Titular dos dados: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (pessoa física a que se referem os dados) Agentes de tratamento: -Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; -Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.
Tratamento de dados pessoais sensíveis	Proíbe o tratamento, estabelecendo algumas exceções. Dados genéticos: relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde e que resulta de uma análise de amostra biológica; Dados biométricos: resultantes de tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem sua identificação única (imagens faciais ou dados dactiloscópicos); Dados relativos à saúde: relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Somente poderá ocorrer: com consentimento de forma específica e destacada, para finalidades específicas e sem consentimento nas hipóteses descritas no Art. 11, II, desta lei
Consentimento dos usuários	O tratamento dos dados pessoais só é lícito com o consentimento de seu titular para uma ou mais finalidades específicas	O tratamento de dados pessoais somente poderá ser realizado mediante consentimento pelo titular

Fonte: A autora.

É importante destacar que, tanto o GDPR quanto a LGPD estabeleceram um novo cenário de segurança jurídica, com a padronização de normas e práticas, para promoverem a proteção dos dados pessoais.

2.4 PRÁTICAS INVESTIGATIVAS

A sociedade atual encontra-se imersa em um ambiente de diferentes tecnologias e em constante desenvolvimento, em que as pessoas, para terem acesso a

espaços e serviços digitais, disponibilizam, continuamente, seus dados pessoais deixando rastros no mundo *online*. Como consequência disto, os crimes cibernéticos estão cada vez mais frequentes e usuais, exigindo do Estado o aprimoramento de seus meios de coletar evidências, artefatos e provas de dispositivos eletrônicos e serviços computacionais.

A atividade de investigação criminal é de extrema importância para a efetividade do sistema judicial e para a concretização dos direitos fundamentais. Os governos, por meio de seus órgãos e instituições, vem intensificando a prática de coletar celulares, *tablets* e computadores - dispositivos que dependem de serviços executados em nuvens e provedores remotos - na busca de informações úteis e evidências para auxiliar e viabilizar as investigações digitais no âmbito da persecução penal e segurança cibernética. A produção de prova que viola direito fundamental nem sempre será considerada lícita, havendo que se equilibrar os valores fundamentais contrastantes. Para (VILARES, 2010), a análise acerca da flexibilização de direitos fundamentais, para fins de cooperação com a persecução penal, deve levar em consideração a adequação da medida para atingir o resultado; a necessidade de ser aplicada, i.e., ser o menos onerosa possível; e proporcionalidade em sentido estrito, devendo haver uma equivalência entre os danos que serão causados e o benefício que será extraído.

Nos termos do parágrafo único, da Resolução CNJ nº 362/2020, é de interesse do Estado e da sociedade a investigação das condutas ilícitas que danifiquem ou exponham a segurança das redes e sistemas computacionais ou que possam comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (BRASIL, 2020). Com o avanço da complexidade dos delitos, a expansão da criminalidade, principalmente a cibernética e o surgimento de novos mecanismos e procedimentos ilícitos, advindos do avanço da tecnologia digital, o estudo e o desenvolvimento de métodos e estratégias investigativas tornaram-se essenciais de modo a incrementar a eficiência da atuação estatal (PAULINO et al., 2021).

As técnicas de investigação tradicionais têm se mostrando ineficazes na apuração das complexas engrenagens criminosas que fazem uso da tecnologia para ocultar as evidências dos delitos e assegurar o proveito econômico das atividades criminosas. Em determinados casos, faz-se necessário colocar de lado a investigação tradicional e considerar novas práticas investigativas na seara do crime cibernético. Enquanto no local de um crime tradicional se encontram informações essenciais para a investigação como testemunhas, vestígios e indícios; o crime cibernético abriga suas principais evidências em inúmeros dispositivos como computadores, telefones celulares, *pen drives*, máquinas fotográficas, provedores de Internet, registros de equipamentos de infraestrutura de rede (e.g., roteadores, *firewalls*, *web servers*, servidores de *e-mails*) (SHIMABUKURO, 2017).

Nesse cenário atual, os desafios da investigação são enormes considerando que a transmissão de dados digitais é dotada de sofisticada criptografia, dificultando o acesso ao conteúdo de dados digitais trocados entre criminosos, de forma a inviabilizar a persecução penal de graves delitos. Assim, o Estado não pode permanecer inerte diante da evolução da criminalidade. Os meios de obtenção de prova utilizados na persecução penal, principalmente nos casos de criminalidade organizada, também devem sofisticar-se, possibilitando o uso da tecnologia - por meio da busca de rastros, dados e informações, armazenados ou em trânsito - alterando significativamente as formas tradicionais de investigação criminal (SAAD, 2021).

Considerando este contexto, os órgãos responsáveis pelas investigações criminais têm adotado procedimentos e aplicado tecnologias para obtenção de provas nos quais são realizadas a exploração excepcional de dispositivos, a remoção de proteção eletrônica e a infiltração policial.

2.4.1 Exploração Excepcional de Dispositivos

Trata-se de interceptação pontual de sinais e acesso autorizado judicialmente ao conteúdo de comunicações protegidas por criptografia. Para (PEREIRA; RODRIGUES; VIEIRA, 2021), o acesso remoto é uma técnica policial autorizada judicialmente, que visa o acesso excepcional a dispositivo eletrônico, aplicativo ou sistema informático ou rede de dados, utilizado pelo investigado, com o objetivo de coletar prova digital e proceder o seu armazenamento com integralidade, com vistas à sua utilização no processo penal. Elenca como alternativas possíveis para o acesso excepcional de dados, sem violação da criptografia, e.g., a apreensão e desbloqueio dos dispositivos das pessoais investigadas, *hacking* governamental desses dispositivos, análise de metadados, *client side-scanning*, inserção de usuário fantasma e acesso a dados armazenados em nuvem. Descreve que a referida técnica investigativa é recepcionada por diferentes jurisdições podendo ser também chamada de *hacking* policial, ocorrer de três maneiras: acesso físico ao computador do investigado, instalando um *malware*, um *keylogger*; acesso remoto ao dispositivo do investigado, e.g., um envio de e-mail ao investigado contendo um anexo ou link que conduziria a instalação de um *malware*, que pode eventualmente copiar arquivos, acionar a *webcam*, ativar o microfone; ou acessar o computador do suspeito utilizando login e senha.

Importante destacar, aqui, o posicionamento do Supremo Tribunal Federal (STF) sobre a matéria, quando o Ministro Edson Fachin, no julgamento da ação de Arguição de Descumprimento de Preceito Fundamental 403 (STF, 2020), assinalou que, embora haja o risco de que criminosos se utilizem de mensagens criptografadas para acobertar suas ações, o risco causado pelo uso da ferramenta ainda não justifica a imposição de soluções que envolvam acesso excepcional ou que diminuam

a proteção garantida por uma criptografia. Porém, apontou que os órgãos de segurança pública e a Procuradoria Geral da República (PGR) defendem que o acesso excepcional garante aos agentes de investigação um mecanismo indispensável para a consecução de suas atividades de investigação em casos graves.

2.4.2 Remoção de Proteção Eletrônica

Ao passo que a criptografia e outros métodos de segurança da informação tornaram-se uma proteção indispensável na sociedade da informação, as instituições de segurança pública ao redor do mundo, em contrapartida, têm alegado que a técnica se tornou um obstáculo para o cumprimento de suas funções (HENNESSEY, 2016). A criptografia, para essas instituições, impede que a polícia tenha acesso a informações necessárias para investigações criminais.

Se por um lado a demanda por criptografia torna o cidadão comum mais blindado contra *hackers* e espiões, por outro pode acabar reforçando as defesas de grupos terroristas e facções criminosas, que acabam operando com mais facilidade sob os radares governamentais (PEREIRA; RODRIGUES; VIEIRA, 2021).

Já outros métodos de segurança podem impossibilitar o acesso de agentes legais (e.g., biometria). A criação de brechas nos sistemas operacionais (e.g., *backdoors*) pode proporcionar debilidades na segurança e sujeição ao ataque de *crackers*/*hackers* e, consequentemente, danos à garantia de proteção da privacidade e dos dados pessoais (SILVA; SILVA; ROSA, 2022).

2.4.3 Infiltração policial

A infiltração policial consiste em um meio especial de obtenção da prova pelo qual o agente de polícia, judicialmente autorizado, ingressa, ainda que virtualmente, em determinada organização criminosa, forjando a condição de integrante, com o escopo de alcançar informações a respeito de seu funcionamento e de seus membros. Apresenta como características básicas a dissimulação -a ocultação da condição de agente oficial e de suas verdadeiras intenções; o engano - que permite ao agente obter a confiança do suspeito; e a interação - relação direta entre agente e investigado; que servem para nortear a ação do Estado (FERREIRA, 2021). Na sequência são introduzidas definições elementares quando se trata de práticas relacionadas a obtenção de provas investigativas de crimes cibernéticos.

2.4.4 Definições pertinentes às práticas investigativas

Esta seção apresenta definições relevantes referentes às práticas investigativas na persecução penal:

- **prova digital**: As provas digitais podem ser produzidas em registros nos sistemas de dados de empresas, ferramentas de geoprocessamento, dados publicados em redes sociais e até encontrados por meio de biometria. Os dados produzidos podem ser encontrados em fontes abertas - de livre acesso como e.g., pesquisas no Google, sites de transparência, redes sociais - ou fontes fechadas - de acesso restrito, por meio de solicitação judicial - em titularidade de pessoas físicas e empresas públicas e privadas (TST, 2021).

  A prova digital pode permanecer disponível para acesso por curto período de tempo, podendo ser, ao mesmo tempo, de fácil dispersão e armazenamento. Pode, ainda, ser facilmente modificada e/ou dificilmente acessada, dependendo do meio em que foi produzida.

  (NETO; SANTOS, 2020) elenca como características das provas digitais:

  – Imaterialidade: ausência de representação física facilitando a transmissão e contribuindo para o grande armazenamento de conteúdos nos sistemas informáticos;
  – Volatilidade: apresenta-se frágil, podendo sofrer alterações ou mesmo desaparecimento;
  – Suscetibilidade de clonagem e facilidade de dispersão: em decorrência da imaterialidade, torna-se suscetível ao processo de clonagem, podendo ser facilmente copiada e transmitida a outros dispositivos eletrônicos, oferecendo risco à preservação da originalidade do arquivo utilizado como meio de prova; e
  – Necessidade de dispositivo de transmissão: necessita de dispositivos físicos para o processamento e exteriorização.

  Segundo (TAMMAY; MAURíCIO, 2020), a utilidade da prova digital passa necessariamente pela observância de três fatores principais:

  – autenticidade: o vestígio deve ser autêntico, guardando a sua identidade desde o momento da sua coleta até a análise pelo Juiz;
  – integridade: os vestígios e provas digitais devem estar livres de qualquer corrupção, adulteração ou interação que modifique suas características originais e, com isso, possa fragilizar as conclusões extraídas da sua análise; e
  – cadeia de custódia: constitui-se em procedimento de preservação da autenticidade, idoneidade e integridade da atividade probatória ao longo da persecução penal.

- **Vestígio digital**: O vestígio digital pode ser um dispositivo móvel, nas comunicações, principalmente através de aplicativos e redes sociais, tais como WhattsApp, Telegram, X (antigo Twitter), Instagram. Também há dispositivos com software embarcado, e.g., um *drone*, um *smartwatch*, um *notebook*, um assistente de voz (e.g., Alexa) ou qualquer outro que possa, por meio digital, oferecer elemento de informação ao agente da lei, na missão de coletar o maior número possível de dados sobre o crime, seu local, suas circunstâncias e seu autor. Em suma, tudo que de um modo ou de outro está conectado à rede deixa rastros digitais.

- **Encontro fortuito de provas**: Também conhecido como serendipidade ou encontro casual de provas é a descoberta inesperada, no decorrer de uma investigação legalmente autorizada, de provas sobre crime que a princípio não estava sendo investigado (STJ, 2023b). No cumprimento de uma diligência relativa a um delito, a autoridade policial casualmente encontra provas pertinentes à outra infração penal, que não estavam na linha de desdobramento normal da investigação.] Em dizer simples, é mirar em algo e acertar coisa diversa, porém valiosa.

  Segundo o magistrado Alexandre Morais da Rosa (SILVA; SILVA; ROSA, 2022), a serendipicidade - ou encontro fortuito de provas - pode ser classificada como de primeiro ou segundo grau. O que diferencia uma da outra é a existência de conexão ou continência, i.e., quando a prova obtida guardar relação com o objeto inicial da investigação ou com pessoa envolvida, será de primeiro grau. Se não houver esse vínculo será de segundo grau e será utilizada como *notícia do crime*. Em julgados recentes, tanto o Superior Tribunal de Justiça (STJ) quanto o STF têm admitido a colheita acidental de provas mesmo quando não há conexão entre os crimes. A orientação dos ministros destes tribunais tem sido em admitir a prova para pessoas ou crimes diversos daquele originalmente perseguido, ainda que não conexos ou continentes, desde que o procedimento investigativo seja legal (STJ, 2015).

- ***Geo-fencing***: Conhecido como cercamento geográfico, diz respeito a uma técnica de identificação dos usuários de aplicações de internet que se encontram em uma dada região dentro de um intervalo temporal determina. A partir da autorização judicial de acesso a dados digitais, permiti-se identificar as pessoas que estavam em um espaço geográfico em determinado período, afunilando as investigações sobre possíveis suspeitos (ARABI, 2022).

  Esses dados coletados devem ter uma fiel documentação de sua cadeia de custódia de forma a garantir a autenticidade e a integridade dos elementos informativos colhidos. E, ainda, necessária a estrita observância ao sigilo no tratamento

dos dados coletados, inclusive com o descarte daqueles que não apresentem relevância para a atividade investigativa.

Como técnica especial de investigação, o *geo-fencing* é um mapeamento de presença digital, numa determinada área, com vistas a identificar potenciais suspeitos de um crime. No Brasil, referida técnica encontra respaldo legal no Art. 22 da Lei 12.965/2014 (BRASIL, 2014a).

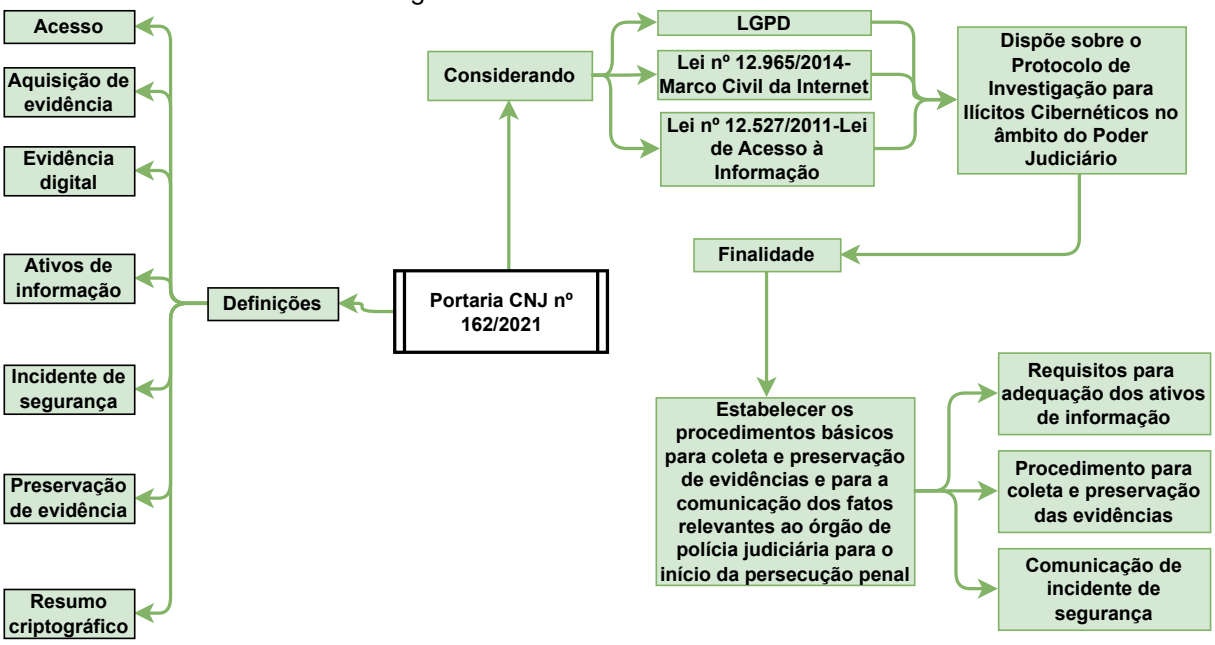
- ***Phishing***: Trata-se de um ataque cibernético que envolve o envio de e-mails, mensagens de texto ou sites fraudulentos, que parecem ser de fontes confiáveis e legítimas, com vistas a enganar indivíduos para que forneçam dados confidenciais (e.g. detalhes de cartão de crédito, credenciais de login ou números de segurança social). Os ataques de *phishing* podem ser altamente sofisticados e difíceis de detectar, pois podem surgir de uma fonte confiável, como um banco ou agência governamental (MAHMOOD, 2023).

- **HL**: Também conhecido como “*Hacking* Governamental”, "*Hacking* Policial", e ainda, "técnicas investigativas de rede", consiste na implantação, por autoridades investigativas, de ferramentas que permitem a invasão de sistemas de computadores, possibilitando o acesso ao seu conteúdo, concentrando-se em observar e explorar falhas de segurança preexistentes e, muitas vezes, não intencionais (LIGUORI, 2020). Pode ser conhecido como um procedimento em que os operadores de rede ou provedores de serviços de comunicação permitem que as forças da lei ou agências de inteligência fiscalizem as comunicações de indivíduos ou organizações.

- ***Fishing Expedition***: Traduzido como pescaria probatória, é a apropriação de meios legais para, sem objetivo traçado, pescar qualquer espécie de evidência, tendo ou não relação com o caso concreto (SILVA; SILVA; ROSA, 2022). Trata-se de uma investigação especulativa indiscriminada, sem objetivo certo e declarado, que, de forma ampla e genérica, lança suas redes com a esperança de pescar qualquer prova, para subsidiar uma futura acusação ou para tentar justificar uma ação já iniciada.

Ademais, a Portaria CNJ nº 162/2021 (BRASIL, 2021) que, em seu Anexo III, dispõe sobre o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário, traz mais algumas definições importantes sobre o tema, conforme mostrado na Figura 5. Referida portaria ressalta o interesse do Estado e da sociedade na investigação de condutas ilícitas que danifiquem ou exponham a segurança das redes e sistemas computacionais ou que possam comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Figura 5 – Portaria CNJ nº 162/2021.



Fonte: A autora.

Uma breve explanação das definições apresentadas na Figura 5:

- acesso: ato de ingressar, transitar, conhecer ou consultar a informação e usar os ativos de informação de um órgão ou entidade;
- aquisição de evidência: processo de coleta e cópia de evidências;
- evidência digital: informação ou dado, armazenado ou transmitido eletronicamente, em modo binário, que pode ser reconhecida como parte de um evento;
- ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos e sistemas necessários, locais e recursos humanos;
- incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
- preservação de evidência: processo de salvaguarda das evidências e dos dispositivos preservando a integridade e confidencialidade das informações; e
- resumo criptográfico: método criptográfico que quando aplicado sobre uma informação, independente de seu tamanho, gera resultado único e de tamanho fixo (*hash*).

Assim, esse novo cenário de segurança jurídica estabelecido com a introdução do GDPR e da LGPD, para promoção da proteção dos dados pessoais, tornou a

investigação digital essencial, sendo necessário entender os possíveis riscos de segurança e privacidade na implementação das práticas de HL e FE como mecanismos de obtenção de provas relacionados a crimes cibernéticos. Em que pese a existência das diversas técnicas abordadas nesta seção, esta pesquisa será direcionada ao HL e FE que serão abordados com maior nível de detalhes no Capítulo 3.

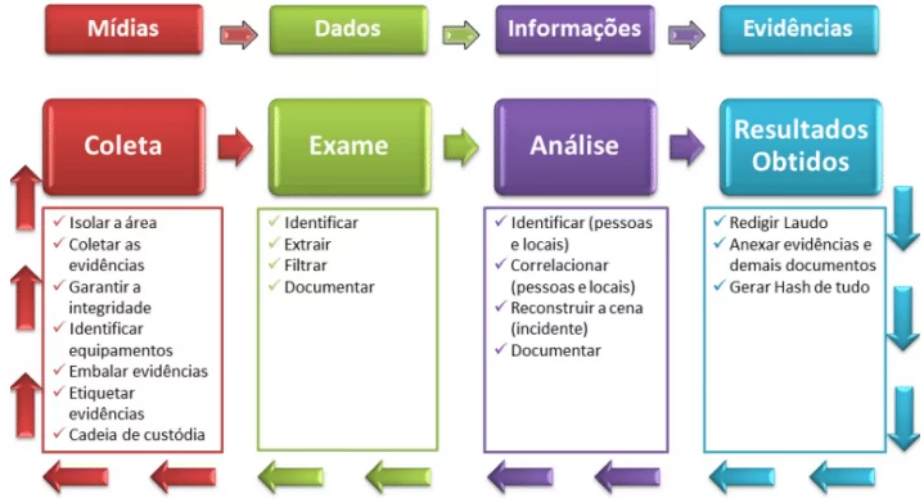
2.5 CADEIA DE CUSTÓDIA

A cadeia de custódia da prova corresponde, na linguagem jurídica, ao conjunto de procedimentos exigidos à preservação e rastreabilidade desses elementos de convencimento, caracterizando requisito de validade do resultado da atividade probatória primária, após a sua admissibilidade e valoração (PASTORE; FONSECA, 2022).

Não é diferente quando a análise envolve as chamadas provas digitais. A importância da cadeia de custódia se dá pelo grau de dificuldade da tarefa de preservar a integridade do elemento probatório digital e verificar sua autenticidade, além de determinar o cuidado que se deve ter, tendo em vista os riscos concretos de manipulação e alteração dos dados. Mostra-se essencial na utilidade da prova digital, sendo um dos principais fatores a serem observados em uma investigação criminal. Deste modo, a cadeia de custódia constitui-se em procedimento de preservação da autenticidade, idoneidade e integridade da atividade probatória ao longo da persecução penal (TAMMAY; MAURíCIO, 2020).

Importante destacar que a abordagem neste trabalho, quanto a cadeia de custódia, é a prevista no ordenamento jurídico brasileiro. Embora não exista um padrão único internacional para a cadeia de custódia, podendo variar em outros países, a *International Organization for Standardization* (ISO) tem publicações que visam contribuir com a padronização para identificação, coleta, aquisição e preservação de evidências forenses digitais em todas as etapas no processo de investigação, que fazem parte da família ISO 27000 - Gestão da Segurança da Informação. Para tanto, no Brasil, a norma ABNT NBR ISO/IEC 27037:2013 padroniza o tratamento de evidências digitais, contribuindo para a aceitação, força probatória e relevância do conteúdo gerado, minimizando os riscos de violação, implantação e parcialidade na construção dos relatórios técnicos confeccionados para relatar as evidências digitais pertinentes ao caso em epígrafe (OLIVEIRA, 2021). Apesar de não se tratar de norma obrigatória, serviu de alicerce e referencial teórico, adotado pela Secretaria Nacional de Segurança Pública (SENASP), conforme Portaria SENASP nº 82, de 16 de julho de 2014 (BRASIL, 2014b). Na Figura 6, observa-se o fluxo das atividades de tratamento de evidências digitais conforme norma ABNT NBR ISO/IEC 27037:2013.

Figura 6 – Fluxo do tratamento da prova digital.



Fonte: (OLIVEIRA, 2021).

Uma breve explicação das fases listadas na Figura 6:

- **coleta**: consiste em recolher o dispositivo questionado de sua localização original para um laboratório ou outro ambiente controlado para posterior aquisição e análise;
- **exame**: após a coleta, consiste no recebimento dos equipamentos pelo setor competente para fins de manutenção da cadeia de custódia, com os registros e cautelas de sigilo, com vistas a realização de extração;
- **análise**: a análise das informações consiste no ato de identificar e documentar todo e qualquer conteúdo que possua relação direta ou indireta com o objeto da investigação, bem como encontrar indícios que corroborem a identificação dos agentes envolvidos no ato ilícito; e
- **resultados obtidos**: partindo do princípio que todo resultado obtido deve ser auditável, nesta etapa ocorre a geração de código *hash*, com o intuito de garantir a integridade dos documentos eletrônicos.

O processo de tratamento das evidências digitais, apesar de possuir diferentes etapas, pode ser entendido como uno, haja vista que essas etapas são interligadas e dependentes, podendo comprometer um dado extremamente sensível e volátil caso sejam desprezadas as cautelas citadas.

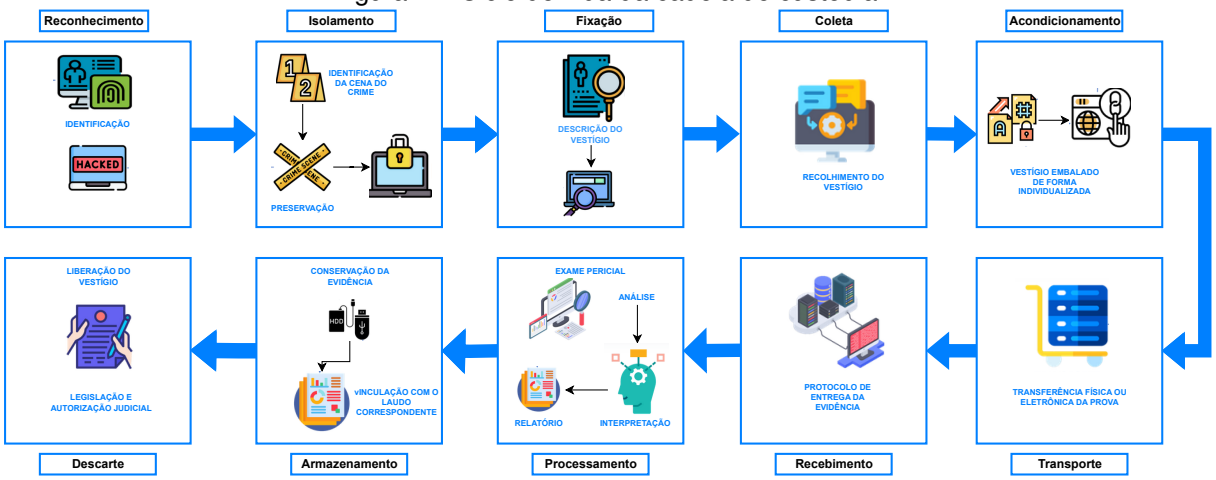
Finalmente, com o advento da Lei nº 13.964/2019 (BRASIL, 2019), também conhecida como Pacote Anticrime, surgiu a definição legal da cadeia de custódia e o reconhecimento de sua relevância. Este diploma alterou o Código Processo Penal (CPP) introduzindo no ordenamento jurídico pátrio menção expressa à cadeia de

custódia, com sua respectiva disciplina (Art. 158 do A ao F), tratando a coleta de vestígios no local do crime de forma mais específica.

O Art. 158A do CPP (BRASIL, 2019) define a cadeia de custódia como "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".

A Figura 7 ilustra as etapas do rastreamento de vestígios na cadeia de custódia, prevista no código processual brasileiro.

Figura 7 – Ciclo de vida da cadeia de custódia.



Fonte: A autora.

As etapas da cadeia de custódia quanto ao rastreamento do vestígio estão dispostas no Art. 158B do mesmo diploma legal. De acordo com a mencionada lei (BRASIL, 2019), o rastreamento de vestígios na cadeia de custódia compreende as etapas:

- reconhecimento: primeira etapa, no qual o agente responsável tem a função de identificar e distinguir determinado elemento como de potencial interesse para a produção da prova pericial;
- isolamento: nesta etapa é realizado o isolamento e a preservação do material e do ambiente imediato, mediato e relacionado aos vestígios e local de crime, de forma a evitar que se altere o estado das coisas, conservando, assim, todo o ambiente ao redor para que não haja interferências de terceiros;
- fixação: é a descrição detalhada do vestígio conforme se encontra no local de crime ou no corpo de delito, mencionando sua posição na área de exames, podendo ser ilustrada por fotografias, filmagens ou croqui, sendo indispensável a sua descrição no laudo pericial produzido por perito responsável;

- coleta: é o recolhimento do vestígio que será submetido à análise pericial, respeitando suas características e natureza;
- acondicionamento: trata-se de procedimento por meio do qual cada vestígio coletado é embalado de forma individualizada, de acordo com suas características físicas, químicas e biológicas, para posterior análise, com anotação da data, hora e nome de quem realizou a coleta e o acondicionamento;
- transporte: esta etapa consiste na transferência do vestígio de um local para o outro, utilizando as condições adequadas (embalagens, veículos, temperatura, entre outras), de modo a garantir a manutenção de suas características originais, bem como o controle de sua posse;
- recebimento: nessa etapa é necessário documentar com a maior quantidade de informações possíveis. O recebimento é o ato formal de transferência da posse do vestígio, que deve ser documentado com, no mínimo, informações referentes ao número de procedimento e unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu. Esses dados são importantes para identificar eventuais erros no procedimento da cadeia de custódia, inclusive o responsável de cada etapa;
- processamento: é o exame pericial em si. Nessa fase o perito realiza a manipulação do vestígio de acordo com a metodologia adequada às suas características biológicas, físicas e químicas, a fim de se obter o resultado desejado, que deverá ser formalizado em laudo oficial;
- armazenamento: refere-se a guarda em condições adequadas, do material a ser processado, guardado para realização de contra-perícia, descartado ou transportado, com vinculação ao número do laudo correspondente; e
- descarte: é o procedimento referente à liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial.

A preservação da cadeia de custódia é fundamental para estabelecer a integridade e autoria das provas digitais. Este processo meticuloso envolve a documentação cronológica do manuseio da evidência, desde sua coleta até sua apresentação em tribunal. Em relação aos crimes digitais, a integridade da cadeia de custódia é assegurada por *hashes*, algoritmos, que funcionam como a impressão digital de um arquivo. Se os *hashes* forem idênticos, entre a busca e uso posterior, reforça-se a ideia de preservação da cadeia de custódia (CATARINA/SC, 2024). Por outro lado, se apontada a divergência entre os *hashes* da coleta com os de um uso posterior no curso da

investigação ou mesmo no processo judicial, há indícios de quebra dessa cadeia de custódia (PRADO, 2021).

Por meio da cadeia de custódia das provas digitais são tutelados os direitos fundamentais à confidencialidade e garantia da integridade dos sistemas de tecnologia da informação, à proteção da identidade digital, do domicílio digital e, por óbvio, da privacidade associada ao direito de decidir o que tornar público ou não relativamente a essa esfera da vida. Nesse viés, para que a prova digital seja admitida no processo penal como fonte probatória confiável é necessária a preservação da cadeia de custódia por meio da adoção de procedimentos rigorosos capazes de preservar a evidência e garantir os requisitos necessários à sua admissão.

Segundo jurisprudência do STJ (STJ, 2023a), "*a principal finalidade da cadeia de custódia é garantir que os vestígios deixados no mundo material por uma infração penal correspondem exatamente àqueles arrecadados pela polícia, examinados e apresentados em juízo*". Portanto, percorrer este caminho com integridade fará com que os dados se transformem em elementos de informação e posteriormente em provas admitidas em tribunal, culminando com a culpa ou absolvição dos envolvidos ao final do processo.

2.6 DEFINIÇÃO DO PROBLEMA

As inovações recentes em dispositivos portáteis mudaram a forma como os consumidores acessam redes e serviços baseados em rede. Os métodos de acesso às redes de comunicação também cresceram em variedade e complexidade. Um resultado dessa mudança é a transformação dos serviços de comunicação passando de um relacionamento direto entre um cliente e um provedor para um ambiente complexo no qual um cliente pode usar vários métodos de acesso para manter interações simultâneas com vários provedores (BELLOVIN et al., 2014).

O cenário apresentado neste trabalho é o de uma sociedade com profundas mudanças nas relações sociais, que ocorrem notadamente em ambientes virtuais, iniciado com a criação da internet/Internet e em progresso acelerado com uso intenso de *smartphones* nas comunicações sociais - principalmente através de aplicativos e redes sociais, tais como WhatsApp, Telegram, X (antigo Twitter), Instagram, bem como o acesso os serviços *online* como os bancários, *e-commerce* e *delivery*.

Nesta senda, surgem demandas sociais relacionadas à privacidade das comunicações e por consequência, cada vez mais, tem-se investido em criptografia na transmissão, armazenamento e proteção dos dados, de modo a inviabilizar o acesso e o conhecimento por terceiros. Em outro vértice, a criminalidade também se aproveita desta alta tecnologia disponível no mercado.

Assim, a regulamentação do tratamento de dados pessoais no contexto exposto constitui uma tentativa de atribuir maior legalidade às medidas adotadas em matéria de persecução e repressão penal, no sentido de balizar a atuação do Estado, contribuir com o devido processo legal e assegurar direitos dos jurisdicionados. Considerando o cenário de necessidade de regulamentação, tanto nacional quanto estrangeira, que se apoie na ideia maior de segurança nacional, concomitante com a segurança individual e coletiva dos usuários da Internet, este trabalho busca explorar a viabilidade e as implicações das práticas investigativas de HL e *Fishing Expedition* no processo de persecução penal. Contudo, face as novas leis (e.g., LGPD) e regulamentações (e.g., GDPR), há de se verificar como estas práticas investigativas podem ser impactadas e quais os principais recursos técnicos disponíveis (i.e., softwares, hardwares, ...).

Os critérios de avaliação para verificar se existem, na literatura, soluções a esse problema, devem ser pautados, basicamente, em três questões motivadoras:

- Q1: Apresenta aspectos legais e técnicos acerca da utilização do HL e FE como práticas no processo de persecução penal?
- Q2: Apresenta aplicação das práticas HL e FE (ou similares/correlatos) no ordenamento brasileiro e/ou nos tribunais internacionais?
- Q3: Faz referência a legislação em vigor LGPD e GDPR, quanto a utilização de dados pessoais, no âmbito da investigação criminal?

Partindo-se desses critérios e métricas, pode-se avaliar se o problema é resolvido ou não, os quais servirão de base para compararem-se os trabalhos relacionados identificados na revisão bibliográfica.

2.7 CONSIDERAÇÕES DO CAPÍTULO

Neste capítulo, primeiramente, foi apresentada a evolução histórica das legislações referentes à proteção de dados no cenário europeu e brasileiro, discorrendo acerca da abrangência e escopo material e territorial do GDPR e da LGPD, de forma a ressaltar seus propósitos e principais pontos de comparação. Tal abordagem mostra-se fundamental ao entendimento do arcabouço legal que envolve a proteção de dados pessoais na qual se encontra a problemática que este trabalho pretende apresentar.

Trouxe, também, conceitos elementares no conhecimento e compreensão de práticas investigativas para apuração de infrações penais e execução das funções de polícia judiciária na persecução penal. De maneira mais específica apresentou o con-

ceito de prova digital e cadeia de custódia, com detalhamento de seu procedimento, conforme estabelecido na Lei Anti-Crime (BRASIL, 2019).

Diante deste contexto e com os conceitos apresentados neste capítulo, possível relacioná-los a problemática aqui apresentada. A abordagem detalhada das práticas de HL e FE podem ser encontradas no Capítulo 3.

3 *Hacking Legal* (HL) E *Fishing Expedition* (FE)

A principal abordagem deste capítulo é discorrer e detalhar os aspectos relevantes das práticas investigativas do HL e FE, descrevendo suas aplicações e etapas técnicas. Ao final são apresentados os trabalhos relacionados.

3.1 *Hacking Legal* (HL)

As provas relativas, não somente a crimes cibernéticos, mas também a qualquer outro delito, estão sendo cada vez mais disponíveis em formato eletrônico, em sistemas de computador ou dispositivos de armazenamento podendo apresentar recursos que facilitam o trabalho da polícia e outros órgãos responsáveis pela aplicação da lei (ŠKORVáNEK et al., 2019). Por outro lado, a proliferação de dispositivos digitais acessíveis com criptografia e mecanismos de segurança inter-relacionados, tornaram os métodos tradicionais de investigação ultrapassados.

Segundo (PEREIRA; RODRIGUES; VIEIRA, 2021), se por um lado a demanda por criptografia torna o cidadão comum mais blindado contra *hackers* e espiões, por outro pode acabar reforçando as defesas de grupos terroristas e facções criminosas, que acabam operando com mais facilidade sob os radares governamentais. Já outros métodos de segurança podem impossibilitar o acesso de agentes legais (e.g., biometria). Assim, as técnicas de investigação tradicionais tem se mostrado ineficazes na apuração de complexas engrenagens criminosas que fazem uso da tecnologia para ocultar as evidências de delitos e assegurar o proveito econômico das atividades criminosas (GIARDINI, 2022).

Esse contexto fez surgir a necessidade de utilização, pelos órgãos responsáveis pela investigação criminal, de práticas que envolvem técnicas de investigação digital e que visam o acesso excepcional a dispositivo eletrônico, aplicativo ou sistema informático utilizados pelo investigado, com o objetivo de coletar e armazenar prova digital, para instrução do processo penal (FERREIRA, 2021). Alguns autores denominam esta prática como "HL", "*Hacking Governamental*" e, também "*Hacking Policial*". Este trabalho se refere a essas denominações distintas sob um único termo de HL.

(MAYER, 2018) define o HL como a prática de explorar vulnerabilidades em sistemas, software ou hardware, realizadas por agentes governamentais e de segurança, para obter acesso a informações que de outra forma seriam criptografadas ou inacessíveis. Assim, o HL subverte as barreiras da segurança para dar aos investigadores acesso aos dados e recursos que eles precisam. As aplicações do HL podem ser divididas em duas categorias principais (LIGUORI, 2020):

1. Implantação de ferramentas de *hacking* no contexto de investigações criminais para acessar remotamente dados armazenados ou em trânsito (e.g., instalação remota de *malware* para vigilância como um envio de e-mail ao investigado contendo um anexo ou URL que conduz a instalação de um *malware*, que pode eventualmente copiar arquivos, acionar a *webcam*, ativar o microfone, etc.).
2. Implantação de ferramentas de *hacking* no contexto do exame forense de um HD/ *Pendrive* apreendido (e.g., acessar um *smartphone* cifrado, instalação de *keylogger*).

Em suma, pode-se dizer que o HL é o acesso excepcional do Estado a conteúdo protegido para fins de investigação criminal que, segundo (PEREIRA; RODRIGUES; VIEIRA, 2021) pode ser realizado de três maneiras:

- Usar vulnerabilidades públicas pré-existentes nos sistemas;
- Desenvolver tecnologia e/ou ferramentas de *hacking* internamente pelas instituições de segurança pública; ou
- Comprá-las de terceiro.

Para fins desta pesquisa, optou-se por abarcar duas subcategorias de HL (AMARAL et al., 2022) e (LIGUORI, 2020):

- Acesso a dados e informações a partir do controle físico do aparelho: implantação de ferramenta de *hacking* no contexto do exame forense de um HD/ *Pendrive* apreendido (e.g., acessar um *smartphone* cifrado, instalação de *keylogger*), possibilitando a extração em massa de dados do dispositivo, envolvendo tanto a quebra de criptografia em aplicações e em discos de armazenamento, ou mesmo o desvio a outros sistemas de segurança, como senhas alfanuméricas, padrões ou autenticação mediante biometria para desbloqueio do dispositivo ou acesso a aplicações;
- Acesso remoto a dispositivos, normalmente a partir da exploração de uma vulnerabilidade ainda não conhecida pelo fabricante do sistema vulnerável e que permita o acesso total ou parcial do aparelho: implantação de ferramentas de *hacking* no contexto de investigações criminais para acessar remotamente dados armazenados ou em trânsito (e.g., instalação remota de *malware* para vigilância como um envio de e-mail ao investigado contendo um anexo ou URL que conduz a instalação de um *malware*, que pode eventualmente copiar arquivos, acionar a *webcam*, ativar o microfone, etc.).

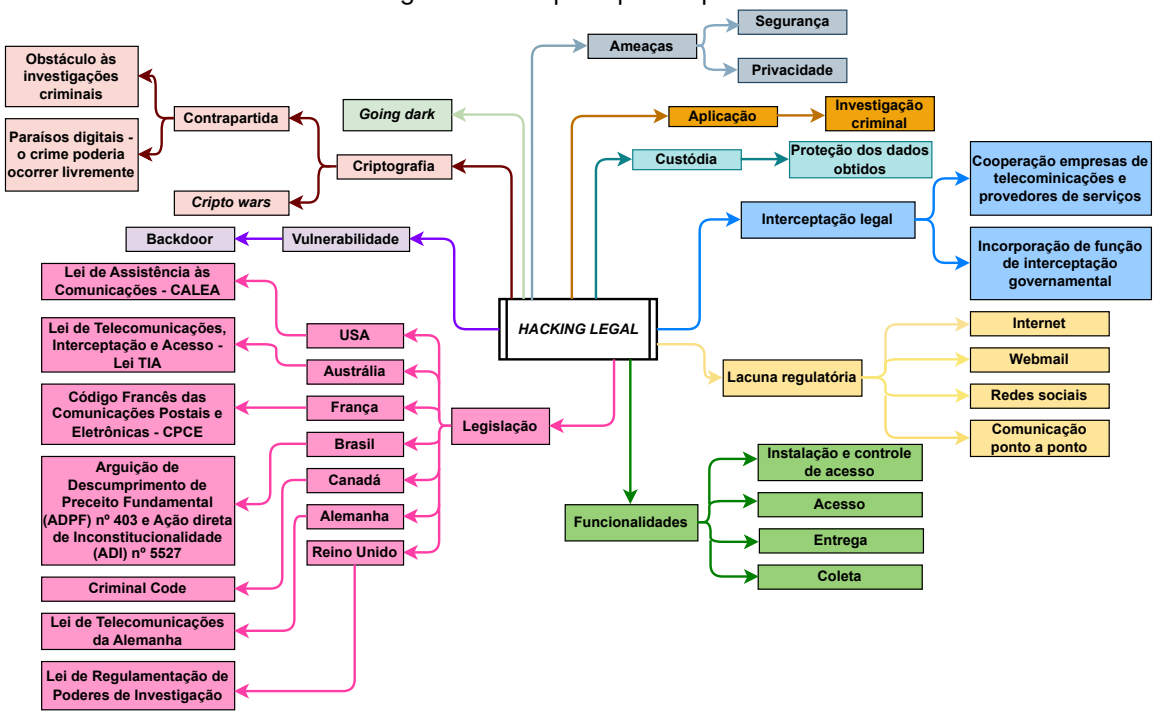
Para (ŠKORVáNEK et al., 2019), a principal ferramenta de HL é o *malware*[1], que pode ser instalado (ou entregue) a um computador alvo de três maneiras:

- Instalar *malware* através de acesso físico a um computador (e.g., numa ação de busca e apreensão instalar um *Keylogger* num computador, numa vistoria de fronteira/emigração ou induzir o usuário alvo a inserir um *pendrive* infectado em seu computador);
- Infectar remotamente o computador com *malware*, i.e., enviar uma mensagem a um usuário de computador e/ou *smartphone* alvos induzindo este usuário a abrir um arquivo anexo ou clicar em um *link* que então instalará secretamente o *malware*. Esta medida possibilita que o agente de investigação assuma o controle remoto do dispositivo sem o conhecimento do usuário, permitindo copiar, transmitir, alterar ou remover dados, ligar *webcam* e microfone, etc.;
- Acessar um computador usando o nome e a senha do usuário, que podem ser obtidos através de *phishing* e outras formas de engenharia social.

A Figura 8 resume os principais aspectos do HL.

[1] (GIARDINI, 2022) define *malware* como um programa que se instala ocultamente em um sistema de dados, permitindo o monitoramento e a captura remota de informações e dados recebidos, armazenados e transmitidos pelo dispositivo eletrônico infectado, além de possibilitar a ativação de algumas funcionalidades do equipamento, como microfone e câmera, e o acesso à sua geolocalização.

Figura 8 – HL: principais aspectos.



Fonte: A autora.

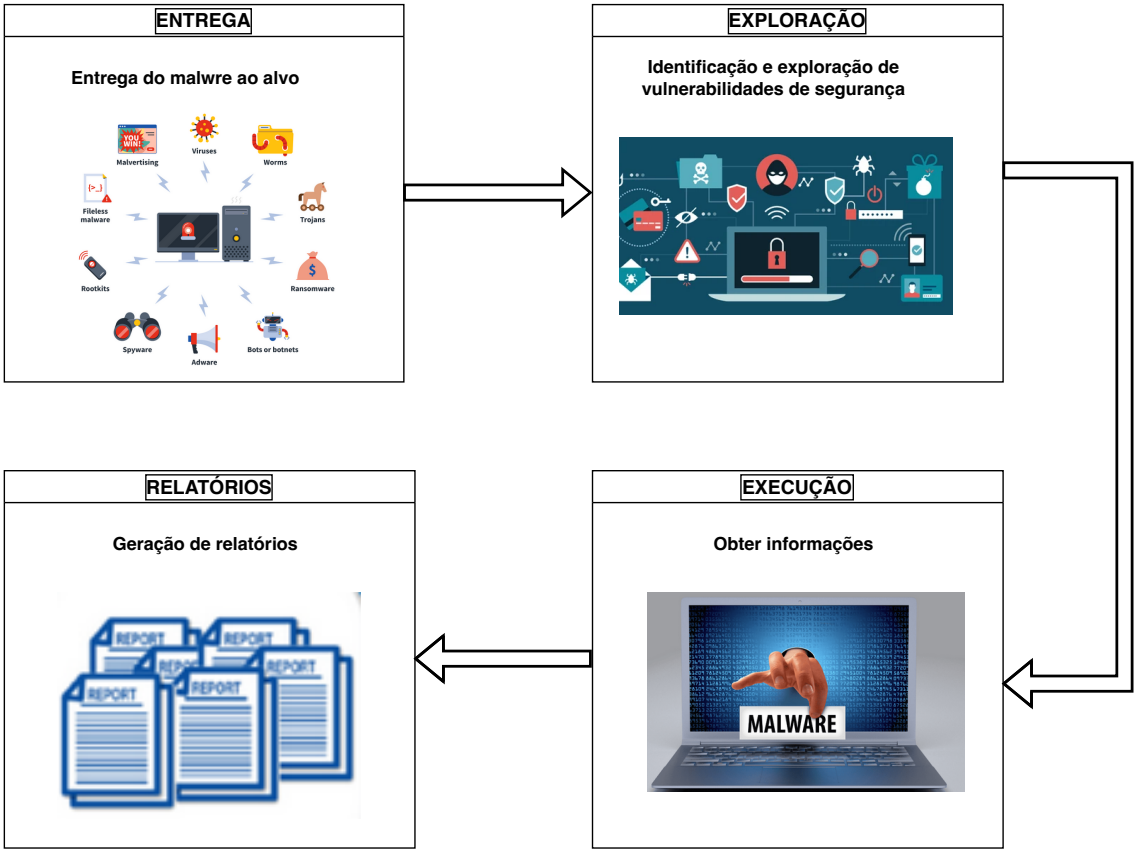
(MAYER, 2018) dispõe que o HL ocorre em quatro etapas técnicas distintas (Figura 9):

- Entrega: essa primeira etapa consiste em colocar o *malware* no dispositivo do criminoso. Uma forma pode ocorrer pela via de introdução de um dispositivo removível, como *pendrive* e dispositivo de armazenamento externo, fisicamente conectado nos dispositivo eletrônico, tendo a ênfase de infectar somente o sistema da pessoa alvo, ainda que desconectado da Internet. Outra forma de instalação ocorre por meio de acesso a páginas da web que contêm o *malware* capaz de infectar os dispositivos de um número indeterminado de pessoas que naveguem na página e cliquem em *links*, que no âmbito de investigações é usualmente inserido em URL com conteúdo voltado a atividades ilícitas para atrair criminosos. Por intermédio de *donwloads* voluntários de anexos de *e-mail*, programas executáveis e falsas atualizações de software legítimo contendo *malware*;

- Exploração: o HL necessariamente subverte as barreiras de segurança associadas ao *sandboxing* para dar aos investigadores acesso aos dados e recursos de que precisam. Os desenvolvedores de ferramentas investigativas identificam e exploram vulnerabilidades em aplicativos que permitem burlar as proteções de *sandbox*. A vulnerabilidade específica que o governo explora e como explora depende de inúmeros fatores, incluindo as informações que os investigadores buscam e a configuração de software usada pelos suspeitos;

- Execução: é a fase de obtenção de informações de identificação. Aqui, o *malware* implantado pode acessar arquivos, registrar teclas digitadas, interceptar comunicações, rastrear a localização e até habilitar a câmera do computador; e
- Relatórios: é a fase de geração de relatórios, responsável por relatar as informações investigadas.

Figura 9 – Etapas HL.



Fonte: A autora.

Considerando as estratégias de implementação do HL na fase de exploração, (BELLOVIN, 2021) apresenta como modalidades:

- Ataques *Man-in-the-Middle*: envolvem a inserção da entidade atacante entre as pontas de comunicação, estando a pessoa-alvo em uma das extremidades. O atacante se coloca como intermediário oculto e consegue trocar informações com a pessoa alvo aparentando ser a outra parte da comunicação e vice-versa;
- Vulnerabilidade *zero-day*: diz respeito à exploração de uma vulnerabilidade ainda não conhecida publicamente ou pelo fabricante do respectivo software ou dispositivo. A invasão do dispositivo da pessoa alvo decorre dessa falha ainda não contingenciada;

- Ataques *click-zero*: o acesso ao dispositivo acontece automaticamente, sem a necessidade de qualquer ação da pessoa alvo, como baixar um arquivo ou mesmo acionar qualquer comando. Essa abordagem dispensa o uso de técnicas de engenharia social para enganar e manipular o comportamento da pessoa alvo;
- *Spoofing*: pode ocorrer no sistema de domínio DNS, com a criação de uma versão falsa de um website a fim de que a vítima insira seus dados. Pode ocorrer através da usurpação do nome de domínio real do site legítimo, da criação de um endereço de URL similar que confunda o alvo, ou mesmo da priorização do domínio falso em mecanismos de busca.
- *Phishing*: envia-se para o alvo, por e-mail ou mensageiro instantâneo, uma mensagem, um link, um texto ou uma imagem atrativa que sirva de anzol levando o alvo a acessar um site controlado pela autoridade.

Algumas funcionalidades para o HL (FERREIRA, 2021):

- Captura de tipos específicos de dados;
- Busca remota de dados armazenados que pode ter como alvo o computador do investigado ou dados armazenados em nuvem, podendo ocorrer o espelhamento desses dados;
- Monitoramento remoto do uso do computador que possibilita a captura de dados, seja por *screenshots* ou *screencasting*, armazenados após a inserção do *malware* com vistas a enviar à autoridade responsável pela vigilância;
- Interceptação das comunicações eletrônicas, com a finalidade de obter seu conteúdo, e.g. *e-mail*, mensagens de texto e *chats* via *WhatsApp* ou Telegram, contornando a dificuldade de acesso ao conteúdo das comunicações cifradas; e
- Observação visual que objetiva “sequestrar” a *webcam* do investigado para identificar o usuário, determinar sua localização ou observar o comportamento do suspeito ou de pessoas suspeitas naquele ambiente, como se fosse uma câmera espiã.

Segundo (DUTRA et al., 2023), o HL pode ser categorizado em três grupos de acordo com a finalidade de sua adoção:

- Controle de mensagem: direcionado a dificultar o recebimento ou difusão de informações por determinadas pessoas. Nesse grupo estão os propósitos de evitar a disseminação de mensagens, manipular o DNS, reescrever conteúdo, sobrecarregar canais de comunicação e desfigurar sites.

- Geração de danos: são adotadas ações profundamente invasivas, ao tornarem inoperantes as tecnologias alvejadas, como modificar internamente ou externamente a parte física de sistemas ou dispositivos, modificar banco de dados e, também, gerar negação de serviço.
- Vigilância e inteligência: neste grupo são adotadas ações visam comprometer usuário ou intermediário, incluindo engenharia social, monitorar canais públicos ou privados de comunicação e, ainda, comprometer propriedades de sistemas protegidos por criptografia.

De um modo geral, o HL envolve o uso de *malware* desenvolvido ou adquirido pelos governos para interceptar as comunicações de um suspeito ou acessar suas informações (LI et al., 2018). Portanto, é necessária uma estrutura legal de forma a permitir, por um lado, atividades de investigação, e por outro, salvaguardar a segurança, os direitos fundamentais e o devido processo legal (LIGUORI, 2020). Nesse ínterim, é preciso analisar se o ordenamento jurídico brasileiro permite o emprego de analogia e interpretação extensiva em matéria processual penal, assim como se a reserva legal constitui impedimento ao emprego do HL.

Em síntese, o uso do HL pressupõe uma exploração às vulnerabilidades já existentes nos sistemas de segurança, e é incitado como alternativa para a possibilidade de acesso aos dados criptografados. Assim, por meio de ferramentas tecnológicas próprias ou contratadas, os órgãos de investigação podem transpor as barreiras da segurança e proteção de dados, utilizando novas formas de produção de prova e vigilância.

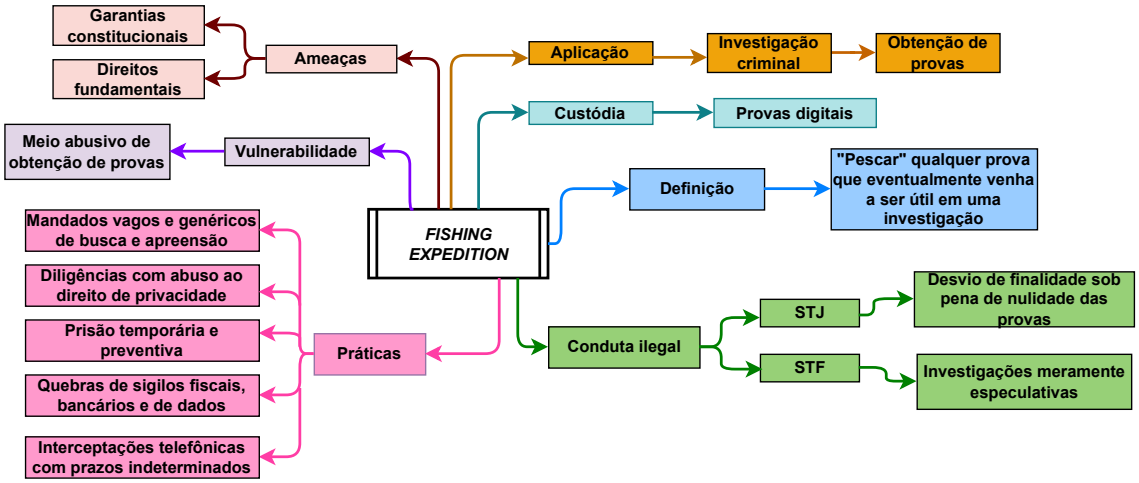
3.2 *Fishing Expedition* (FE)

(BANDEIRA, 2020) define FE como uma procura especulativa, no ambiente físico ou digital, sem causa provável, alvo definido, finalidade tangível ou para além dos limites autorizados (desvio de finalidade), de elementos capazes de atribuir responsabilidade penal a alguém. Ainda, a Sétima Turma do Tribunal Regional da 4ª Região (Brasil), firmou entendimento no sentido de existência de FE, “quando a ordem judicial, sem nenhuma justificativa plausível determina a quebra de sigilo por tempo inexato, completamente dissociada dos fatos e como fruto de mera especulação (TRF4, HC 5047227-48.2020.4.04.0000, Sétima Turma, Relatora Cláudia Cristina Cristofani, juntado aos autos em 18/11/2020).

Além disso, em (SILVA; SILVA; ROSA, 2022), o juiz Moraes da Rosa define FE como "*a prática relativamente comum de se aproveitar dos espaços de exercício de poder para subverter a lógica das garantias constitucionais, vasculhando-se a intimidade,*

a vida privada, enfim, violando-se direitos fundamentais, para além dos limites legais". Por vezes, esta técnica está relacionada com investigações prévias, antes mesmo da instauração do inquérito policial, outras vezes com procedimentos já formalizados. A Figura 10 mostra os principais aspectos da prática do FE.

Figura 10 – FE: principais aspectos.



Fonte: A autora.

A prática do FE, por se tratar de meio de obtenção de prova, tem largo campo de ocorrência na cultura penal, no aproveitamento, por parte dos agentes públicos, de diligências, com ou sem autorização. Contudo, o estabelecimento claro do objeto da investigação, desde a sua instauração, constitui limite ao Estado, impedindo a instauração de procedimentos obscuros, à margem da legalidade. Acrescente-se os reflexos da LGPD que, por mais que exclua a investigação criminal, demanda a edição de lei para o fim de regular o modo de aquisição, tratamento dos dados pessoais e sensíveis.

No âmbito do direito sancionador, o (STJ, 2022a) já decidiu que "*admitir a entrada na residência especificamente para efetuar uma prisão não significa conceder um salvo-conduto para que todo o seu interior seja vasculhado indistintamente, em verdadeira pescaria probatória (fishing expedition)*". Nesse sentido, também o STF já censurou o uso de FE naquilo que, aos seus olhos, já se tornou uma prática adotada por determinadas autoridades e órgãos de investigação no desempenho de suas atividades. (SILVA, 2017) elenca como táticas de aplicação e/ou modalidades de FE:

- Busca e apreensão, sem alvo definido, tangível e descrito no mandado (mandados genéricos);
- Busca e apreensão estendida, em locais além daqueles que eram mencionados expressamente na ordem judicial);
- Vasculhamento de todo o conteúdo do celular apreendido;

- Continuidade da busca e apreensão depois de obtido o material objeto da diligência;
- Investigações criminais dissimuladas de fiscalizações de órgãos públicos (Receita Federal, controladorias, Tribunais de Contas, órgãos públicos etc.);
- Interceptação ou monitoramento por períodos longos de tempo;
- Quebra de sigilo telefônico com base em uma lista ampla e não individualizada de alvos;
- Prisão temporária ou preventiva para forçar a descoberta ou colaboração premiada ou incriminação;
- Buscas pessoais ou residenciais desprovidas de fundada suspeita prévia e objetiva; e
- Quebra de sigilo (bancário, fiscal, dados etc.) sem justificativa do período requisitado.

No âmbito do direito sancionador, o (STJ, 2022a) já decidiu que "*admitir a entrada na residência especificamente para efetuar uma prisão não significa conceder um salvo-conduto para que todo o seu interior seja vasculhado indistintamente, em verdadeira pescaria probatória (fishing expedition)*". Nesse sentido, também o STF já censurou o uso de FE naquilo que, aos seus olhos, já se tornou uma prática adotada por determinadas autoridades e órgãos de investigação no desempenho de suas atividades.

Exemplos de FE

De forma exemplificar a abordagem do FE e ilustrar os entendimentos dos tribunais superiores acerca do tema, são apresentados alguns julgados:

1. **Operação Pelicano** (MPPR, 2015): Deflagrada em março de 2015 e liderada pela GAECO, teve como objetivo desarticular organização criminosa formada por auditores fiscais da Receita Estadual, contadores e empresários que se uniram para facilitar a sonegação fiscal mediante o pagamento de propina. Além de corrupção, tratava-se de crimes de falsidade de documentos e lavagem de dinheiro. Foram realizados 24 mandados de busca e apreensão, porém o STF declarou ilícitas as provas obtidas no curso das diligências, tendo em vista a inespecificidade dos mandados, ou seja, os agentes valeram-se de mandado judicial para ir além daquilo que foi delimitado, caracterizando FE. Ao analisar o caso, a 2ª Turma do STF considerou que a diligência foi ilegal, por ter sido realizada em

local diverso do especificado no mandado judicial. O caso aconteceu no âmbito do HC144.159.

2. **Caso Marielle Franco e o uso de *geofencing*** (STJ, 2020): Como técnica de investigação, o *geofencing* é um mapeamento de presença digital, numa área determinada, que permite saber quem esteve naquele ambiente em determinada janela de tempo. Ao julgar o RMS 62.143/RJ, o STJ decidiu que o Google fornecesse ao Ministério Público e à Polícia Civil do Rio de Janeiro os dados estáticos (tráfego e metadados) de usuários dos serviços Google e Waze, que passaram pela Transolímpica num período de 15 minutos no dia 2 de dezembro de 2018, bem como buscas no Google de qualquer usuário que tenha procurado por determinados termos específicos (“Marielle Franco”, “vereadora Marielle”, “agenda Marielle”, “agenda vereadora Marielle”, “Casa das Pretas”, “Rua dos Inválidos 122” e “Rua dos Inválidos”) até cinco dias antes do crime. No caso concreto, pelo mapeamento digital (*geofencing*) pretendeu-se saber quem estava no veículo Cobalt, de placas clonadas KPA-5923, no dia e horário do crime, carro usado na execução da vereadora Mariele Franco e seu motorista. A Google alegou prática de FE, dada a amplitude da ordem mencionada, uma vez que junto aos dados pessoais e de comunicações dos possíveis suspeitos, o órgãos de investigação teriam acesso aos dados de qualquer pessoa que estivesse próxima da cena do crime e/ou que tenha pesquisado pelas referidas palavras-chave, ainda que elas não tenham relação alguma com o ato criminoso. Para a provedora, a medida, determinada de forma genéria, seria desproporcional.

3. **Revista pessoa baseada em comportamento suspeito - RHC 158.580** (STJ, 2022b): a 6ª Turma do STJ considerou ilegal a realização de busca pessoal ou em veículo sem mandado judicial, quando motivada apenas pela impressão subjetiva da polícia em relação à aparência ou atitude suspeita do indivíduo. Os policiais alegaram ter encontrado drogas durante a revista pessoal, justificando a abordagem com base em "atitude suspeita"do réu, sem fornecer outras razões. Alegou-se a prática de FE na abordagem e revista exploratória, baseada em suspeitas genéricas sobre indivíduos ou atitudes.

4. **Indícios de autoria devem ser anteriores às medidas de busca e apreensão - RMS 62.562** (STJ, 2021): No julgamento do RMS 62.562, a 5ª Turma do STJ determinou a destruição de todo o material apreendido em uma empresa em razão do reconhecimento de FE durante a diligência de busca e apreensão. Segundo o processo, no curso da investigação de suposta organização criminosa que estaria envolvida em desvios de patrimônio do Município de Poconé/MT, foi determinada a cópia de todo o banco de dados de uma empresa responsável

> pelo gerenciamento eletrônico de abastecimento e manutenção da frota da prefeitura. A empresa recorreu ao STJ para que os dados apreendidos fossem destruídos, ao argumento de que seus cartões seriam utilizados por mais de 130 mil estabelecimentos, entre clientes públicos e privados, sendo ilegal a apreensão de forma ampla, principalmente por não fazer parte da investigação.

Assim, por meio do FE, a parte, em um processo penal, pretende obter informações do seu adversário (parte contrária) sem que se tenha um objeto pré-definido de investigação, de modo que, nesse caso, as provas deixam de servir como uma demonstração de hipóteses previamente formuladas, passando a serem a própria construção de hipóteses. O equilíbrio entre a observância de garantias constitucionais e o adequado controle de admissibilidade das provas mostra-se fundamental para a formação qualificada da cognição ao longo do processo. Portanto, a correta compreensão e o efetivo controle em torno do uso da ferramenta do FE poderá, certamente, contribuir para que os anseios e desafios em torno da eficiência e efetividade na prestação jurisdicional sejam aprimorados em direção a um processo mais eficiente e efetivo.

3.3 COMPARAÇÃO: HL VS. FE

Considerando este cenário, a necessidade de regulamentação, tanto nacional quanto estrangeira, se apoia na ideia maior de segurança nacional, concomitante com a segurança individual e coletiva dos usuários da Internet. Assim, este trabalho apresenta uma proposta que tem por objetivo análise comparativa dos aspectos legais e técnicos das práticas de HL e FE no contexto interno e estrangeiro. Visando proporcionar maior embasamento para realizar o estudo comparativo proposto neste trabalho foram analisados alguns critérios abordados pelas práticas do HL e FE, apresentados na Tabela 2.

Tabela 2 – Critérios comparativos HL e FE.

Critério	*Hacking* Legal	FE
Foco	Obtenção de acesso a dados, pelas autoridades policiais e de inteligência	Obtenção de provas para subsidiar uma futura acusação
Aplicação	Investigação criminal e exame forense	Investigação prévia, realizada de maneira muito ampla e genérica para buscar evidências sobre a prática de futuros crimes
Vulnerabilidade	Restringir a criptografia, com a implementação de *backdoors*	Meio abusivo de obtenção de provas
Ameaças	Ameaças à privacidade e segurança; permitir que as mesmas ferramentas sejam capturadas e reaproveitadas por criminosos; adicionar mais complexidade e insegurança aos sistemas *online*.	Ameaças às garantias constitucionais e direitos fundamentais, violando a intimidade e a vida privada para além dos limites legais.
Limitações	Limitações de escopo e duração, a fim de evitar abusos	Vedação , necessário que a investigação defina antecipadamente o seu objeto, de modo que a diligência, o pedido e a decisão judicial devem respeitar expressamente: quem, quando, como, onde, por e para quê, o que e qual a sua motivação concreta. Do contrário, não preenchem os pressupostos e requisitos legais. A decisão judicial deve motivar de modo adequado, sob pena de nulidade (CPP, Art. 315, §2º).
Legislação	A GPDR prevê que o tratamento de dados pessoais para fins de investigação é objeto de ato jurídico específico da UE. USA: Lei de Assistência às Comunicações - CALEA (2014); Austrália: Lei de Telecomunicações, Interceptação e Acesso - TIA (2018); França: Código Francês das Comunicações Postais e Eletrônicas - CPCE; Reino Unido: Lei de Poderes de Investigação-IPA(2016)	A LGPD apesar de excluir a investigação criminal, demanda edição de lei para o fim de regular o modo de aquisição, tratamento e guarda dos dados pessoais e sensíveis. Constituição Federal, Código de Processo Penal (Lei nº 3.689/1941) e o Pacote Anticrime (Lei 13.964/2019)
Custódia	O uso de ferramentas de *hacking* legal para coletar dados dos dispositivos de um suspeito é semelhante a uma operação forense remota, protegendo os dados obtidos e observando-se a cadeia de custódia	São inadmissíveis as provas digitais sem registro documental acerca dos procedimentos adotados pela polícia para a preservação da integridade, autenticidade e confiabilidade dos elementos informáticos (STJ, 5a Turma. RHC 143169/RJ, 07/02/2023)
Ferramentas	Ferramentas de software que exploram vulnerabilidades. Uso duplo: podem ser usados por criminosos por um lado, mas também são úteis para defensores, pesquisadores e administradores de sistemas. Ferramentas para hackear dispositivo cifrado. As ferramentas precisam incorporar abordagens como criptografia de dados, capacidade de dados por meio de redes anônimas e serem capazes de passar pelos mais novos conjuntos de antivírus e *firewalls*	Mandados vagos e genéricos de busca e apreensão, diligências com abuso ao direito de privacidade, prisão temporária e preventiva, quebras de sigilos fiscais, bancários e de dados, dentre outras
Métodos	As autoridades podem: -usar vulnerabilidades públicas preexistentes, implantando ferramentas de *hacking* com vistas a exploração de vulnerabilidades de sistema (software, firmware e hardware) ou desenvolvimento de *malware*, para acessar dados criptografados em repouso (dados armazenados em um dispositivo) ou em trânsito (dados que fluem de um dispositivo para outro através de uma rede); -desenvolver a tecnologia/ferramenta de *hacking* internamente ou; -comprá-la de terceiros	Busca e apreensão sem alvo definido, tangível e descrito no mandado (mandados genéricos); vasculhamento de todo o conteúdo do celular apreendido; continuidade da busca e apreensão depois de obtido o material objeto da diligência; investigações criminais dissimuladas de fiscalizações de órgãos públicos; Interceptação ou monitoramento por períodos longos de tempo; Prisão temporária ou preventiva para "forçar"a descoberta ou colaboração premiada ou incriminação; buscas pessoais (ou residenciais) desprovidas de "fundada suspeita"prévia e objetiva; e, Quebra de sigilo (bancário, fiscal, dados etc.) sem justificativa do período requisitado
Coleta de dados e volatilidade	Os fornecedores de ferramentas de *hacking* legal precisam garantir que os dados coletados sejam armazenados com segurança e não possam ser acessados por pessoas não autorizadas	Necessário o registro documental sobre o modo de coleta e preservação dos equipamentos, quem teve contato com eles, quando tais contatos aconteceram e qual o trajeto administrativo interno percorrido pelos aparelhos uma vez apreendidos pela polícia. Nem se precisa questionar se a polícia espelhou o conteúdo dos computadores e calculou a *hash* da imagem resultante

Fonte: A autora.

Assim, é possível estabelecer uma correlação entre suas aplicações e abrangências no contexto da privacidade dos dados pessoais.

3.4 TRABALHOS RELACIONADOS

A presente seção tem como objetivo levantar os trabalhos relacionados com o problema da pesquisa, buscando-se analisar as tendências em relação às questões propostas. Inicialmente, realizou-se um levantamento bibliográfico para traçar o referencial teórico sobre os principais conceitos relacionados à investigação digital, crimes cibernéticos e proteção de dados, com o propósito de se obter uma visão geral do tema objeto da pesquisa, apresentado no Capítulo 2. Na sequência, realizou-se uma

Revisão Sistemática da Literatura (RSL) com vistas a identificar estes trabalhos/estado da arte das práticas do HL e FE, como métodos de colheita de provas pelas agências policiais e de inteligência, e legislação aplicada no âmbito nacional e internacional. É apresentado o método e o processo de pesquisa realizado e por fim a descrição dos trabalhos identificados como relacionados.

3.4.1 Método

A RSL consiste em um método de estudo secundário, que tem por objetivo avaliar pesquisa relevante sobre uma questão, tópico ou interesse específico. Para (LEVY; ELLIS, 2006) a RSL é o processo de coletar, conhecer, compreender, analisar, sintetizar e avaliar um conjunto de artigos científicos com o propósito de criar um embasamento teórico-científico (estado da arte) sobre um determinado tópico ou assunto pesquisado. Neste trabalho, a RSL está pautada nas diretrizes propostas por (KITCHENHAM; CHARTERS, 2007):

- Planejamento: avaliar a necessidade do estudo, primeiramente fazendo uma pesquisa exploratória para ver se realmente o processo de revisão é necessário. Em sequência devem ser definidos os critérios de pesquisa e elaborar o protocolo de revisão;
- Condução: realização dos passos definidos anteriormente no protocolo, realizando as buscas nos mecanismos definidos, avaliando os trabalhos e fazendo a extração dos dados; e
- Relatório dos resultados: é a última parte da revisão e consiste na análise e escrita dos resultados.

3.4.2 Questões de pesquisa

Os critérios de avaliação para verificar se existem, na literatura, soluções para o problema apresentado na Seção 2.6 foram:

- QP1: Aborda a prática de HL nas investigações criminais?
- QP2: Apresenta ferramentas de HL?
- QP3: Aborda a prática de FE nas investigações criminais?
- QP4: Apresenta ferramentas de FE?
- QP5: Correlaciona GDPR?
- QP6: Correlaciona LGPD?

- QP7: Qual escopo?
- QP8: Qual tipo?

Partindo-se desses critérios/questões de pesquisa pode-se avaliar se o problema é resolvido ou não, e quais servirão de base para comparação e seleção dos trabalhos relacionados identificados na revisão bibliográfica.

3.4.3 Processo de pesquisa

Este levantamento dedicou-se a trabalhos a partir de 2015 e com foco em artigos primários e secundários. As bibliotecas digitais utilizadas foram IEEE Xplore, ACM Digital Library, Springer, Elsevier, biblioteca jurídica Escola Superior do Ministério Público da União[2] e CONJUR[3], escolhidas de acordo com a importância que estas bases possuem no meio acadêmico e jurídico, e outros.

Com relação às buscas nos sítios dos tribunais superiores, é importante destacar que nenhum resultado foi encontrado para a prática do HL. A busca foi realizada utilizando-se os termos “HL” ou “*Hacking* do governo” ou “*Hacking* policial”. A temática da FE, apesar de verificável na prática das buscas, apreensões e, em geral, nas investigações na âmbito penal, não tem a sua expressividade refletida no mundo acadêmico ou jurisprudencial, embora o STJ e o STF tenham acolhido, recentemente, a incidência deste instituto.

Para fins de validação desse argumento foi realizada pesquisa nos portais do STF e do STJ obtendo um número diminuto de resultados. Executou-se a busca digitando-se a expressão FE no campo destinado à pesquisa de jurisprudência de cada um dos sítios oficiais, selecionando as opções de pesquisa mais abrangentes, localizando 110 julgados no sítio do STF, sendo 11 acórdãos e 99 decisões monocráticas. Quanto a busca no sítio do STJ, foram encontradas 4 decisões sendo 1 acordão e 3 decisões monocráticas. Além da parca menção do FE na jurisprudência dos tribunais superiores, grande parte das vezes o termo aparece simplesmente da reprodução, no relatório da peça, dos argumentos feitos pelas partes, sem que haja real enfrentamento do tema pelos julgadores. Também, a escassez de julgados que abordam a questão demonstra desconhecimento do instituto por parte de advogados e defensores públicos, pois se o argumento acerca da prática de do FE fosse reiteradamente invocado, o tribunais precisariam debatê-lo analisando o mérito. Assim, tal pesquisa realizada nos sítios destes tribunais mostrou-se irrelevante para esta pesquisa.

A consulta nas bases IEEE Xplore, ACM Digital Library, Escola Superior do Ministério Público da União e CONJUR foi realizada por meio do termo de busca "Law-

[2] <https://escola.mpu.mp.br/publicacoes/obras-avulsas/e-books-esmpu>
[3] <https://www.conjur.com.br/pesquisa/?q=&mes=&ano=&tipo=>

ful Hacking"OR "Government Hacking"OR "Hacking Legal"OR "Fishing Expedition". Nas blibliotecas Elsevier, Springer e outros foi utilizada a *strings* de busca ("Lawful Hacking"OR "Government Hacking"OR "Hacking Legal"OR "Fishing Expedition") AND (GDPR OR LGPD), incluindo GDPR e LGPD de forma a restringir a consulta para o resultado pretendido. Após a busca nas bibliotecas, utilizou-se como método para realizar a pesquisa, três fases bem definidas, sendo estas:

- Fase 1: realizou-se a leitura dos títulos dos trabalhos, eliminando aqueles cujos títulos não faziam nenhuma relação com o tema;
- Fase 2: realizou-se a leitura dos resumos dos artigos, possibilitando um entendimento maior sobre os objetivos dos trabalhos, excluindo os trabalhos que não teriam relevância; e
- Fase 3: procedeu-se, por meio da leitura integral dos artigos, à eliminação daqueles que não tinham relação com as questões de pesquisa citadas anteriormente.

3.4.4 Critérios de Inclusão e Exclusão

Para análise e seleção dos trabalhos foram definidos os seguintes critérios de inclusão e exclusão:

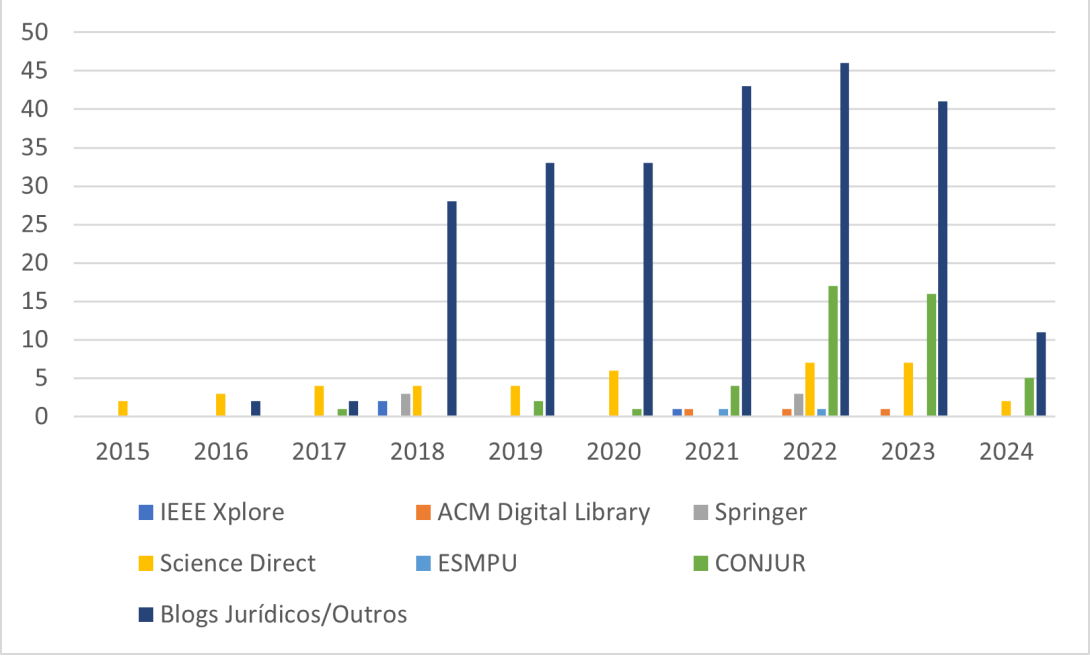
- **Critérios de Exclusão**: Com vistas a embasar as eliminações em cada fase, foram aplicados alguns critérios de exclusão, sendo eles:
  - Critério de Exclusão 01: trabalhos duplicados que falam sobre o mesmo assunto;
  - Critério de Exclusão 02: trabalhos que não abordam as práticas do HL e FE;
  - Critério de Exclusão 03: trabalhos hospedados em serviços pagos não financiados pela universidade;
  - Critério de Exclusão 04: trabalhos classificados como de acesso restrito nas bibliotecas digitais jurídicas; e
  - Critério de Exclusão 05: trabalhos publicados anterior a 2015.
- **Critérios de Inclusão**: Foram utilizados, também, alguns critérios de inclusão, que visam identificar quais trabalhos possuem relevância para a pesquisa, tais como:
  - Critério de Inclusão 01: o trabalho aborda HL e FE;
  - Critério de Inclusão 02: o trabalho correlaciona GDPR ou LGPD;

– Critério de Inclusão 03: o trabalho correlaciona GDPR ou LGPD;
– Critério de Inclusão 04: o trabalho possui palavras do tema no título/resumo/palavras chave;
– Critério de Inclusão 05: trabalhos publicados entre 2015 e 2024; e
– Critério de Inclusão 06: trabalhos escritos em inglês e português.

3.4.5 Execução

Na busca geral nas bibliotecas eleitas como fonte de pesquisa, foram encontrados um total de 338 trabalhos que, a princípio, atendem a pesquisa usando os fraseamentos definidos conforme Subseção 3.4.3. A indicação do quantitativo relacionado a cada biblioteca está contida na Figura 11.

Figura 11 – Número de trabalhos encontrados nas bibliotecas, por ano.



Fonte: A autora.

A Figura 11 mostra que a maior parte dos trabalhos foi publicada a partir de 2018, coincidindo com a publicação da LGPD. A análise mostra uma tendência de crescimento nas publicações, com ressalva ao ano de 2024, em curso, em que foi realizada a presente pesquisa, não sendo possível contabilizar todos os trabalhos.

Para seleção dos trabalhos foram aplicados os critérios de inclusão e os critérios de exclusão definidos na Subseção 3.4.4, e posteriormente realizada uma análise qualitativa, com verificação do resumo e principais tópicos da publicação e sua correlação com o problema proposto.

3.4.6 Elegibilidade

A elegibilidade dos trabalhos foi realizada aplicando-se os passos de filtragem, retirando-se os trabalhos repetidos e aplicando-se os critérios de inclusão e exclusão. A Tabela 3 apresenta a quantidade inicial de trabalhos resultantes da busca em cada uma das bases, e a referidas quantidades após aplicação dos critérios de exclusão.

Tabela 3 – Quantitativo do processo de elegibilidade.

Biblioteca	Nº trabalhos identificados	Nº de trabalhos avaliados para elegibilidade	Nº de trabalhos incluídos na síntese final
IEEE Xplore	3	2	2
ACM Digital Library	3	1	0
Springer	6	0	0
Science Direct	39	2	1
ESMPU	2	2	1
CONJUR	46	13	2
Blogs Jurídicos/Outros	239	9	5
Total	338	29	11

Fonte: A autora.

Nesta etapa os trabalhos passaram por um filtro de remoção de trabalhos duplicados, posteriormente foram submetidos à avaliação de elegibilidade de acordo com os critérios de inclusão e exclusão e então, incluídos numa síntese qualitativa, cujo conteúdo do resumo, palavras chave e principais tópicos do texto foram analisados e avaliados. Por fim, chegou-se ao número de trabalhos obtidos da síntese final.

Quanto às ameaças à validade deste estudo, pode-se citar:

- Mecanismo de busca: dificuldade na escolha da *string* para realização da busca e sua adequação às bibliotecas utilizadas. Efetividade da *string* escolhida e consistência dos dados obtidos. Porém, as métricas utilizadas tiveram um propósito definido, conforme descrito na Subseção 3.4.3.
- Quantidade de trabalhos selecionados: embora, num primeiro momento, possa parecer pequeno o número de trabalhos encontrados que atendessem às questões de pesquisa, este fato se justifica pelo número significativo de artigos com abordagem ambiental de "pescaria", *hacking* num contexto genérico e relacionados técnica de *phishing*, conceito diverso da prática abordada neste trabalho apresentado na Seção 2.4.
- Qualidade dos trabalhos selecionados: embora seja importante a avaliação da qualidade dos estudos que suportam a pesquisa, neste trabalho observou-se a pequena abordagem do tema nas bibliotecas científicas.

3.4.7 Agregação

Nesta RSL, chegou-se à apreciação de 11 trabalhos que se tornaram elegíveis à pesquisa. A Tabela 4 lista estes trabalhos relacionando-os com as questões de pesquisa.

Tabela 4 – Trabalhos relacionados identificados.

Ref.	QP1: aborda HL?	QP2: apresenta ferramentas HL?	QP3: aborda FE?	QP4: apresenta ferramentas FE?	QP5: correlaciona GDPR?	QP6: correlaciona LGPD?	QP7: qual escopo?	QP8: qual tipo?
(LI et al., 2018)	Sim	Sim	Não	Não	Não	Não	Austrália, França, Alemanha, Reino Unido e USA	Funcionalidade, ferramentas e lei
(BELLOVIN, 2021)	Sim	Não	Não	Não	Não	Não	Não	Não
(ŠKORVáNEK et al., 2019)	Sim	Sim	Não	Não	Não	Não	USA, Holanda, Itália, Reino Unido e Alemanha	Método, ferramentas e lei
(ANTIS, 2021)	Sim	Sim	Não	Não	Não	Não	Não	Ferramentas, tecnologias e contratos
(GIARDINI, 2022)	Sim	Sim	Não	Não	Não	Não	Não	Ferramenta
(KOLOCHENKO, 2022)	Sim	Sim	Não	Não	Sim	Não	França, Alemanha, Países Baixos, Reino Unido, USA	Estrutura, ferramentas, métodos e legislação
(FERREIRA, 2021)	Sim	Sim	Não	Não	Não	Sim	Brasil, Reino Unido, Alemanha, Itália, Holanda, USA	Funcionalidades, lei e jurisprudência
(LIGUORI, 2020)	Sim	Sim	Não	Não	Não	Não	Alemanha, França, Austrália e EUA	Ferramentas, vulnerabilidades, limitações e regulamentação
(ROSA, 2021)	Não	Não	Sim	Sim	Não	Não	Brasil	Ferramentas e hipóteses
(CANI; ROSA, 2021)	Sim	Sim	Sim	Não	Não	Não	Europa	Ferramenta
(HERPIG, 2021)	sim	sim	Não	Não	Não	Não	Alemanha e mundo	Requisitos, ferramentas e vulnerabilidades

Fonte: A autora.

Depreende-se da Tabela 4, que não foram encontrados trabalhos que preencham todos os requisitos derivados do problema de pesquisa aqui proposta, de forma que a proposta será realizada observando-se as questões levantadas no problema e não resolvidas nos trabalhos relacionados. Sendo assim, faz-se relevante a proposição de solução que atenda a questão em estudo abrangendo ambas as práticas do HL e FE à luz do GDPR e da LGPD.

3.4.8 Descrição dos trabalhos identificados como relacionados

(LI et al., 2018) explora o tema acerca da aplicação e limitações do HL na manutenção de um equilíbrio adequado entre a segurança nacional e ao direito fundamental à privacidade. Apresenta uma visão geral do status do HL e regras de interceptação legal, discutindo sua técnicas, métodos e preocupação com riscos à segurança da Internet. Para tanto, parte da revisão do estado atual do HL em cinco países (i.e., Austrália, França, Alemanha, Reino Unido e EUA) analisando as limitações das soluções atuais, além da existência de regulamentação que implica em alguma forma de autorização.

(BELLOVIN, 2021) fala sobre a aplicação do HL por parte do governo dos

Estados Unidos, preferível a colocar *backdoors* em sistemas de criptografia. Aponta como problema a falta de legislação específica que permita o uso desta prática. Destaca que as questões de privacidade devem ser consideradas. Defende a necessidade de restrições ao HL de forma a preservar a privacidade dos dados do investigado. Defende um debate público acerca do tema.

O trabalho de (ŠKORVáNEK et al., 2019) apresenta um análise comparativa da proteção da privacidade no âmbito do direito processual penal nos Estados Unidos, Alemanha, Itália, Países Baixos e Reino Unido no contexto do HL. Defende que permitir o acesso remoto secreto a computadores pode ser a melhor forma de permitir que as autoridades detenham a capacidade de recolher provas. Destaca que vários países introduziram o HL em suas leis nacionais, portanto a extensão desta regulamentação varia consideravelmente de uma jurisdição para outra, desafiando a forma como os sistemas jurídicos lidam com a privacidade de dados pessoais. Busca responder a questão: Quais foram as principais preocupações dos legisladores e qual tipo de privacidade garantida constitucionalmente, se houver, foi aplicada? Foram analisadas, neste artigo, legislações e jurisprudências a nível federal e identificadas e discutidas quais salvaguardas se aplicam às diferentes funcionalidades do HL.

(ANTIS, 2021) considera a aquisição de tecnologia de *hacking* pelos governos e o papel dos processos de compras governamentais na regulação do mercado de *hacking* e na redução dos riscos para o comprador. Ressalta que, embora a proliferação da tecnologia de *hacking* para intervenientes governamentais tenha levado a várias soluções propostas, pouca relevância tem sido dada à compra pública desta tecnologia. Apresenta softwares, explorações, vulnerabilidades e *spyware* (e.g., Pegasus) e o mercado no qual essas ferramentas são compradas. Este artigo explora a questão da contratação pública poderiam de tecnologia de HL e os tipos de cláusulas contratuais e apoios institucionais que podem ser úteis para atingir esse objetivo. Argumenta que os requisitos de transparência e responsabilização inerentes ao sector público poderiam ser transferidos em parte para o sector privado e explora como os contratos públicos para a tecnologia de HL podem ser estruturados, a fim de reduzir os riscos colocados pela uso desta tecnologia.

O trabalho de (GIARDINI, 2022) aborda o uso de *malware* como meio de obtenção de prova utilizado pelo governo. Lista os tipos de *malware* e suas aplicações. Apresenta duas vertentes acerca da admissibilidade do uso desta ferramenta por parte do Estado na investigação criminal. Ressalta a ausência de regra específica e a importância de se estabelecer um equilíbrio entre os direitos e deveres fundamentais envolvidos e a garantia do sucesso da investigação e da segurança pública, à luz do garantismo penal integral.

(KOLOCHENKO, 2022) busca responder três questões acerca do HL: *i)* quais

são os principais obstáculos técnicos e barreiras legais na aplicação desta prática nas investigações de crimes graves e organizados; *ii)* se e como o HL pode ser substituído por outros meios técnicos ou legais menos invasivos de investigação criminal; e *iii)* se o HL é compatível com a integridade da justiça criminal, com a privacidade e proteção dos dados pessoais à luz do GDPR.

(FERREIRA, 2021) descreve a mudanças nas relações sociais e o impacto destas nas formas de obtenção de provas digitais e a preocupação do Governo, Sociedade Civil e Poder Judiciário com a segurança dos dados pessoais e confidencialidade do conteúdo das comunicações privadas. Aborda as hipóteses de acesso, por órgãos responsáveis pela investigação criminal, de comunicações criptografadas como técnica de obtenção de prova digital. Cita exemplos de previsão legal acerca do HL em países como Reino Unido, Alemanha, Itália, Holanda e USA. Discorre acerca do posicionamento do STF sobre o tema, mencionando a LGPD.

A proposta de (LIGUORI, 2020) é abordar a problemática do "*going dark*"e o acesso excepcional das autoridades policiais aos sistemas de criptografia a fim de permitir investigações criminais de dados em trânsito e em repouso. Descreve o HL como uma ferramenta investigativa alternativa sem comprometer a criptografia. Discorre acerca dos desafios regulatórios e as limitações e vulnerabilidades no exercícios desta prática. Mostra abordagens específicas do HL e sua regulamentação na Alemanha, França, Austrália e EUA. Ao final propõe uma estrutura legal robusta que permita prática do HL nas atividades de investigação criminal e, ao mesmo tempo, garanta a segurança dos dados pessoais, os direitos fundamentais e o devido processo legal.

(ROSA, 2021) explora a temática do FE. Discorre acerca da vedação desta prática ante as garantias constitucionais, mostrando-se fora do enquadramento normativo da investigação democrática. Indica que, ao mesmo tempo em que as regras investigativas não podem ser restritivas a ponto de impedir a apuração de condutas criminosas, os limites legais devem ser respeitados, i.e., o ato não pode ser movido por má-fé ou com desvio de finalidade, nem invadir os direitos individuais. Enumera as hipóteses de pescaria probatória realizada por agentes públicos no processo de investigação criminal. Por fim, aponta que o desafio do Processo Penal é punir observando as regras de obtenção de meios de prova.

O trabalho de (CANI; ROSA, 2021) expõe comentários à investida europeia contra criptografia e a pesca predatória. Enfatiza a problemática de estar de um lado a privacidade e a segurança e do outro os limites da criptografia de dados. A questão proposta está na possibilidade, para evitar ataques terrorista no território europeu, de se instalar *backdoors* em servidores com vistas a possibilitar o monitoramento constante de mensagens, resultando no dever para os servidores de fiscalizar o tráfego e comunicar atos suspeitos. Ainda, que máquinas e/ou humanos poderiam monito-

rar o conteúdo das comunicações em uma verdadeira pescaria probatória de forma a subsidiar futura acusação. Na visão trata-se de invasão abusiva do conteúdo privado manipulado sob o argumento de combate ao terrorismo, na medida em que extrapola os limites jurídicos de produção de prova.

(HERPIG, 2021) analisa questões de riscos com prática do HL como a criação de uma indústria de HL e mercados de vulnerabilidades; perda do controle exclusivo por parte do governo sobre suas ferramentas de *hacking*; redução da confiança dos usuários; hackear usuários inocentes, implicações extraterritoriais; preocupações com a segurança e privacidade. Este artigo sugere um padrão mínimo de como os governos devem agir ao hackear, estabelecendo requisitos estruturais e operacionais que definem como o *hacking governamental* deve ser conduzido,inclusive requisitos de supervisão judicial prévia. Propõe que a implantação do padrão proposto obedeça a cadeia de custódia das provas digitais e seja limitado a crimes graves. Por fim, propõe que seja estabelecido um processo nacional de avaliação e gestão de vulnerabilidades, ponto fundamental para a segurança nacional. Os requisitos sugeridos neste artigo servirão como orientação prática para que os estados (dentro da Europa ou fara dela) equilibrem os critérios preventivos e investigativos com as necessidades inerentes de segurança e privacidade.

Ante o exposto, analisando os trabalhos relacionados, percebe-se o abismo existente entre a utilização das práticas dos práticas do HL e FE, principalmente no ambiente digital, e o alinhamento destas com as garantias individuais de proteção de dados pessoais e as legislação em vigor, dada a relevância no processo de persecução penal e o potencial de penetração e/ou invasão de dados. A dimensão deste problema se potencializa no ambiente digital porque as vulnerabilidades são maiores, menos perceptíveis e tendencialmente devastadora na esfera dos direitos fundamentais.

3.5 CONSIDERAÇÕES DO CAPÍTULO

Neste capítulo foram apresentados os conceitos mais detalhados do HL e FE, fundamental ao entendimento do cenário da pesquisa e no qual se encontra inserida a problemática que o trabalho pretende resolver. Estes conceitos são primordiais para obtenção da análise comparativa destas práticas, considerando os desafios à tecnologia, às regras de interceptação legal e a legislação pertinente.

Surge, então, uma necessidade urgente de regulamentação transparente e específica que abarque o HL e o FE, com vistas a traçar uma linha reta e ousada separando os limites cibernéticos permitidos, operações ilícitas, cadeia de custódia da prova digital e segurança e privacidade dos dados digitais de forma a fornecer um

porto seguro para a segurança cibernética para ajudar as agências de aplicação da lei sem o grave risco de transcender a fronteira legal. O resultado obtido com a análise dos trabalhos relacionados vem reforçar e justificar uma solução para os problemas fundamentados e evidenciados neste capítulo.

4 ANÁLISE E ESTUDO DE CASO

Este capítulo aborda as ferramentas de extratação de dados digitais tanto por acesso remoto de dados armazenados ou em trânsito, como também para extração via acesso físico, mostrando exemplos e casos de uso. Ao final traz uma análise destas ferramentas e o estudo de caso.

4.1 ANÁLISE E FERRAMENTAS

As ferramentas de *hacking* se apresentam em um contexto no qual as instituições de segurança pública e persecução penal se insurgem contra o que chamam de impedimentos, entraves ou obscurecimento ("*going dark*") das investigações contra criminosos em ambientes cibernéticos. Para fins desta pesquisa, considera-se como ferramentas de *hacking* tanto as técnicas de extração de dados mediante superação de sistemas de segurança quanto as técnicas de acesso remoto a dados e comunicações pessoais. Esta seção apresenta as ferramentas que auxiliam a perícia digital e os órgãos de investigação no processo de extração de dados em vestígios digitais, tendo por objetivo qualificá-los como evidência ou prova no âmbito judicial.

4.1.1 Ferramentas para acesso remoto de dados armazenados ou em trânsito

A sofisticação do cometimento de crimes, bem como o ocultamento de provas sob sistemas de segurança da informação seria motivação suficiente para que fossem adotadas ferramentas que superassem tais barreiras, tornando eficaz a atividade de segurança pública. Assim, há uma tendência na busca de meios alternativos de investigação para contornar tal restrição.

A prática de explorar vulnerabilidades em sistemas informáticos carrega, fundamentalmente, uma ambivalência. Tanto pode ser explorada por agentes privados mal intencionados, constituindo crimes tipificados em ordenamentos jurídicos mundo afora, quanto pode ser utilizada por autoridades policiais e governamentais como forma de produzir provas em investigações criminais ou para fins de inteligência. Partindo da segunda categoria, o HL constitui rotina de agências governamentais e vem sendo enquadrada como aparato das forças da lei e de inteligência (AMARAL et al., 2022).

Nesse cenário, *malwares*[1] são utilizados para obter comunicações de dados

[1] software malicioso construído para invadir um dispositivo, móvel ou não, pessoal ou não, com o objetivo de coletar dados e enviar a uma parte terceira sem o consentimento do titular dos dados, além de um controle contínuo sobre uma pluralidade de funcionalidades (KASPERSKY, 2025)

de pessoas suspeitas, estando eles armazenados ou em trânsito (LIGUORI, 2020). Uma vez secretamente instalados, tais instrumentos aproveitam-se de falhas ou aberturas do sistema informático para criar um portal de acesso remoto e invisível ao utilizador (*backdoor*), por meio da qual se obtém, à distância, acesso aos dados e funcionalidades do dispositivo alvo, tais como arquivos, senhas, bem como armazená-los em servidor remoto e independente do meio invadido. Além disso, essas funcionalidades podem possibilitar o monitoramento e recolhimento de dados sobre atividades e hábitos do usuário na internet, como data/hora de acessos, páginas web, e-mails acessados, endereço IP, tipo de navegador utilizado (FILHO, 2020). É importante destacar que o *malware* não constitui um software único, trata-se de uma série de dispositivos que, a depender da sua natureza e funções, assumem variados nomes como:

- *spyware*: executado em segundo plano, coleta dados e informações do usuário;
- *keylogger*: registra as teclas digitadas pelo usuário, atividades do dispositivo e rastreiam ações. Captura informação confidenciais;
- vírus: usa a replicação para se inserir em diferentes aplicativos de um computador ou para se espalhar entre computadores;
- *worms*: semelhante ao vírus, porém se replica e se espalha entre computadores de uma empresa ou local;
- Trojam: usado para colocar outros tipos de malware em um computador;
- *rootkits*: fornece ao invasor acesso remoto ao dispositivo. Pode acessar e controlar arquivos, espionar o usuário, roubar dados;
- *botnet*: é uma rede que pode fazer um grupo de computadores infectados pelo mesmo malware trabalharem juntos sem o conhecimento dos usuários; e
- *logic bombs*: pedaço de código inserido intencionalmente em um sistema de software que acionará uma função maliciosa quando as condições especificadas forem atendidas.

Nesse contexto, vários Estados-membros do Conselho da Europa adquiriam e usaram *spywares* para vigilância direcionada de seus próprios cidadãos, como também de defensores de direitos humanos, oponentes políticos, advogados, diplomatas, chefes de Estado, jornalistas ao redor do mundo. No Brasil, também registram-se consecutivos sinais de contratação da ferramenta de *hacking* por agências de investigação e/ou inteligência brasileiras. No cenário internacional, tal prática vem sendo usada na investigação de crimes graves, tanto por agências de investigação de nível estadual, como por repartições federais.

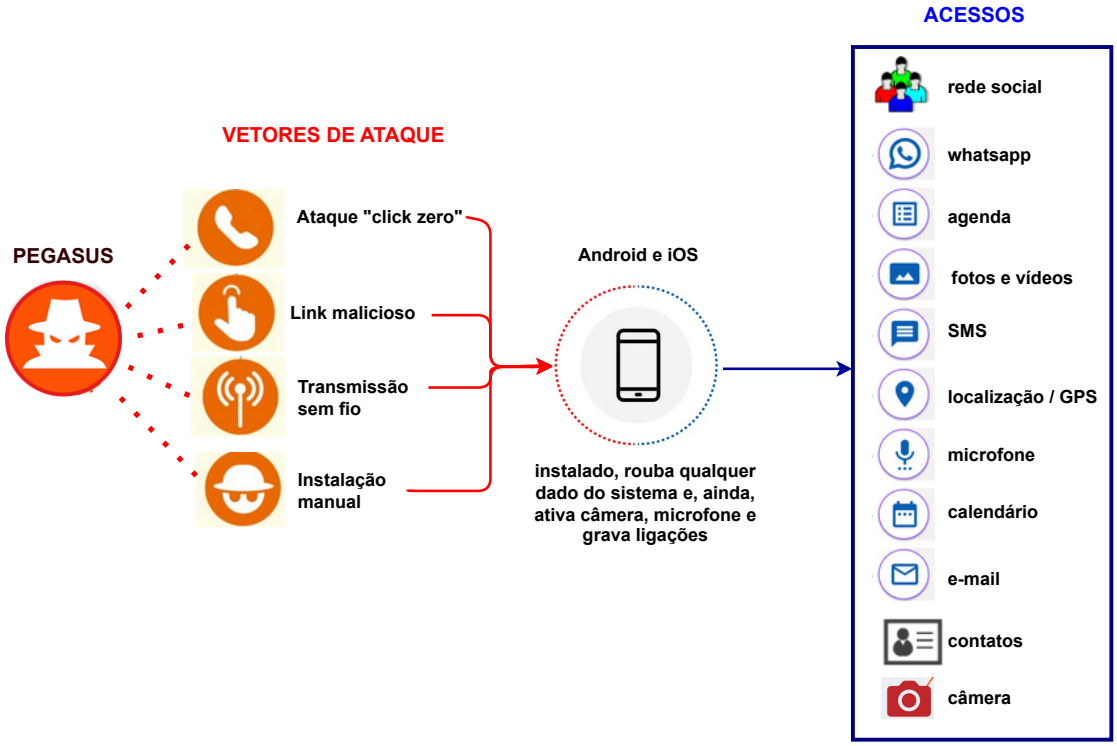
Exemplos de ferramentas de *hacking* para acesso remoto

1. **Carnivore**: software de vigilância desenvolvido pelo *Federal Bureau of Investigation* (FBI) em 1997 e utilizado para auxiliar nas investigações de atos terroristas e outras atividades, na Internet, de suspeitos criminosos, sendo utilizado até 2001. Posteriormente recebeu o nome de DCS1000 (DUTRA et al., 2023). Armazenava e escaneava certos tipos de dados, e.g., e-mails recebidos, páginas da Web visitadas, arquivos transferidos, etc. Basicamente, se posicionava em um segmento de rede e monitorava o tráfego de certos usuários designados, procurando por palavras-chave ou frases específicas. Se encontrar uma sequência de dados correspondente no tráfego monitorado, este interceptará e armazenará essa transmissão para análise posterior pelo seu administrador (OPENCARNIVORE.ORG, 2025).

2. ***Key Logger System* (KLS)**: ferramenta utilizada pelo FBI, na solução de uma investigação sobre a magia ítalo-americana, capaz de registrar o que era digitado no computador do suspeito. Quando os agentes baixaram o conteúdo do computador de Scarfo, um arquivo foi criptografado, usando um programa chamado *Pretty Good Privacy* (PGP). Com tecnologia KLS, o FBI recuperou a senha da chave PGP (arquivo cifrado) de Scarpo, obtendo acesso ao arquivo (QUINLAN; WILSON, 2016). Em síntese, o KLS foi utilizado pelo governo dos *United States of America* (USA) para capturar as senhas de Scarfo para o arquivo criptografado enquanto este as inseria em seu teclado.

3. **Pegasus**: *spyware* de vigilância altamente intrusivo, desenvolvido e comercializado pela empresa israelense NSO Group, capaz de comprometer a maioria dos dispositivos móveis com sistemas operacionais Android e iOS e de conceder ao usuário acesso completo e irrestrito a todos os sensores e informações no telefone celular alvo (DUTRA et al., 2023). A versão mais antiga do Pegasus, descoberta por pesquisadores em 2016, infectava celulares por meio de *spearphishing*, mensagens de texto ou *e-mails* que enganavam o alvo ao clicar em um link malicioso. Atualmente, as infecções por Pegasus podem ser por meio de ataques de "clique zero", que não exigem nenhuma interação do proprietário do celular para serem bem sucedidos. Uma vez instalado em um celular, o Pegasus é capaz de extrair contatos, registros de chamadas, mensagens, fotos, histórico de navegação na web, configurações, bem como coletar informações de aplicativos de comunicação (e.g., iMessage, Gmail, Facebook, WhatsApp, Telegram, Skype)(PEGG; CUTLER, 2021). Este transforma o *smartphone* em um dispositivo de vigilância 24 horas, acessando a câmera, microfone, dados de geolocalização, e-mails, mensagens, fotos, vídeos, senhas e aplicativos (Figura 12).

Figura 12 – Funcionamento básico do Pegasus.



Fonte: A autora.

4. **Prism**: programa de vigilância, utilizado pela *National Security Agency* (NSA) que visa monitor e coletar vários tipos de dados dos usuários que utilizam serviços da Internet, incluindo histórico de pesquisas, conteúdo de e-mails, transferências de arquivos, vídeos, fotos, chamadas de voz e detalhes de redes sociais. O Prism funciona através de grandes sistemas de roteadores pelos quais é analisada o tráfego de dados em escala global. O objeto analisado pode ser qualquer cliente das companhias que fazem parte do programa, sendo ou não cidadão norte-americano. O Prism coleta dados que são posteriormente analisados e armazenados através de outros programas que fazem parte do sistema de espionagem da NSA. Esta coleta de dados se dá através de acordos com as empresas provedoras de serviços de Internet (LIGER; GUTHEIL, 2023).

5. **Predador**: ferramenta de vigilância que oferece ao seu operador acesso total e contínuo ao dispositivo móvel alvo. É comercializado pela Cytrox, empresa sediada na Macedônia do Norte que pertence a israelense Inlellexa. A principal diferença com o Pegasus é que o Predador é um *exploit* de um clique, e portanto, requer alguma ação por parte da vítima, como clicar em um link ou abrir um anexo para que o *spyware* infecte o telefone alvo. O Predador permite que o operador extraia senhas, arquivos, fotos, histórico de navegação na web, contatos, faça capturas de telas, registre entradas do usuário, ative microfone e a

câmera do dispositivo, grave mensagens de texto enviadas ou recebidas, bem como chamadas telefônicas (LIGER; GUTHEIL, 2023).

6. **Anom**: é um aplicativo de mensagens criptografadas, privado, criado pelo FBI e anunciado como meio de comunicação seguro para grupos criminosos. Uma das características do Anom é o uso de criptografia para cifrar as mensagens enviadas, fazendo os usuários acreditarem tratar-se de aplicativo seguro. Em síntese, o Anom consistia em uma ferramenta de investigação distribuída para entidades criminosas por meio de pessoas infiltradas nesse meio. Permitiam que as autoridades possuíssem acesso ilimitado e em tempo real às comunicações realizadas dentro do aplicativo (VIEIRA, 2021).

7. **Augury**: é uma ferramenta, criada pela empresa norte-americana Team Cymru, que permite o rastreamento digital contínuo de cidadãos, com a captura de dados de tráfego, como *cookies* de sessão, detalhes de navegação e credenciais de acesso a contas em plataformas privadas (usuário e senha). O Augury coleta URLs e *cookies*, que podem ser considerados informações sensíveis, uma vez que carregam dados que podem identificar os usuários. A ferramenta também inclui dados de fluxo de rede, que descrevem o volume e o fluxo de tráfego dentro da internet. Essas informações, normalmente, só podem ser acessadas pelo proprietário do servidor e incluem quais servidores se comunicaram com outro, e servem para identificar as redes que o alvo está usando (MOTORYN, 2023).

8. **FirstMile**: trata-se de um software, desenvolvido pela empresa israelense Cognyte, com capacidade de monitorar a geolocalização de até 10 mil celulares por um período de um ano. A ferramenta não tem acesso a mensagens ou a ligações dos alvos rastreados. Ela invade e engana a rede de empresas de telefonia para conseguir rastrear o alvo do monitoramento. O celular emite informações (protocolo SS7) para uma estação rádio-base (antenas de celular espalhadas no país) e o FirstMile consegue bagunçar esse protocolo e conseguir que a operadora de celular forneça a geolocalização de seus clientes. Em síntese, o software FirstMile faz é atacar o sistema das operadoras de telefonia celular. O software foi adquirido sem licitação ainda no governo de Michel Temer durante a intervenção federal na área de segurança pública do Rio de Janeiro, mas foi usado mais intensamente no governo Bolsonaro para monitoramento de membros do STF, jornalistas, advogados e políticos (BRASIL, 2023).

Casos de uso.

A Tabela 5 mostra o uso das ferramentas no cenário internacional e no Brasil.

Tabela 5 – Casos de uso.

Ano/Data	Casos de uso	Ferramenta	Descrição do caso	País	HL / FE	LGPD	GDPR	Ref
1997	Carnivore	Carnivore (DCS1000)	Sistema de vigilância desenvolvido pelo FBI para ajudar nas investigações de atos terroristas e outras atividades na Internet de suspeitos criminosos	USA	HL e FE. Potencial em armazenar temporariamente e escanear todo o tráfego de dados, não apenas dos suspeitos dos crimes. Oportunidade de o governo espionar cidadãos inocentes e desavisados	NA	NA, porém a ferramenta foi alvo de críticas por questões legais e por ser considerada ameaça à privacidade.	(DUTRA et al., 2023)
1999	Caso Scarfo	Key Logger System (KLS)	Investigação sobre a máfia ítalo-americana. O FBI vasculhou a propriedade de Nicodemo Scarfo, em Nova Jersey. Agentes baixaram o conteúdo do computador de Scarfo, um arquivo foi criptografado usando o *Pretty Good Privacy* (PGP). Foi instadado secretamente um KLS para registrar o que era digitado, com o intuito de recuperar a senha da chave PGP do criminoso	USA	HL e FE. O investigado contestou a legalidade do uso do software de keylogger, alegando que a ferramenta era semelhante a grampo telefônico e que o FBI não havia obtido mandado adequado para seu uso	NA	NA	(QUINLAN; WILSON, 2016)
2013	Caso Edward Snowden	Prism	Denúncia de Edward Snowden sobre a vigilância massiva realizada pelo governo dos USA. Através do Prism, a NSA consegue dados de mídia a respeito dos investigados como senhas, arquivos transferidos, conversas de voz, fotos, vídeos, conversas por vídeo, dados de correio eletrônico e ações em redes sociais	USA	HL e FE. Monitoramento de pessoas comuns (qualquer pessoa usuária da Internet) e interceptações telefônicas de políticos de outros países tidos como "aliados"ou "considerados amigos", como e.g. Angela Merkel (Primeira Ministra da Alemanha) e Dilma Russeff (presidenta do Brasil)	NA	NA	(LIGER; GUTHEIL, 2023)
2015	FBI x Apple	*Backdoors*	FBI pressiona a Apple para desbloquear o iPhne 5C de Syed Rizwan Farook, um dos responsáveis pelo ataque em San Bernardino/Califórnia. O iPhone de Farook tinha um recurso de segurança reforçado por criptografia definido para apagar todos os dados após 10 tentativas frustradas de digitar uma senha	USA	HL e FE. O FBI queria que a Apple alterasse as funções de apagamento automático e atraso de senha de seu software, modificando o sistema operacional do celular de Farrok. A Apple argumentou que tal pedido colocaria os clientes em risco ao enfraquecer a segurança do iPhone. Para solucionar o caso, o FBI comprou ferramenta de *hacking* de terceiro	NA	NA, porém o caso tencionou a posição da empresa (de defender a proteção criptográfica dos dados armazendos nos celulares de sua marca) contra o interesse da unidade de polícia (em investigar o dispositivo de um terrorista morto). A questão seria se a empresa estaria legalmente obrigada a contornar a segurança de seu produto	(QUINLAN; WILSON, 2016)
2015	Movimento Catalão	Pegasus	Membros do movimento catalão pró-independência e seus familiares, incluindo o então presidente da Assembleia Nocional Catalã, Jordi Sánchez, foram alvos do Pegasus. Aproximadamente 65 pessoas foram alvos de ataques através do Pegasus entre 2015 e 2020.	Espanha	HL e FE	NA	Espanha manifestou intenção de atualizar sua legislação de forma a reforçar as garantias e assegurar o respeito pelos direitos fundamentais das pessoas, de forma a aplicar e fazer cumprir adequadamente a Diretiva (UE) 2016/680 (Diretiva Proteção de Dados na Aplicação da Lei) e assegurar à ANPD poderes de supervisão sobre o tratamento de dados pessoais nos termos do GDPR	(VELD, 2023)
2018	Operação Última Milha	FirstMile	Refere-se às investigações da Polícia Federal sobre a suspeita de uso ilegal do software de espionagem FirsrMile pela Abin, para monitorar opositores políticos de Jair Bolsonaro e seus filhos, com o intuito de favorecê-los. O STF informou que o software foi utilizado 30 mil vezes e entre os supostos monitorados estão os ministros do Alexandre de Moraes e Luis Roberto Barroso, o deputado Rodrigo Maia e outros. O monitoramento foi realizado por meio da invasão de aparelhos e computadores, além da infraestrutura de telefonia utilizando o FirstMile.	Brasil	HL e FE	o monitoramento dos alvos foi considerado ilegal (invasão de dispositivo informático alheio e interceptação de comunicações sem autorização judicial ou com objetivos não autorizados em lei, contrariando os fundamentos da LGPD	por se tratar de um caso de violação do direito fundamental autônomo à proteção de dados pessoais, fere subsidiariamente o GDPR	(BRASIL, 2023)
2019	Caso Krzysztof Brejza	Pegasus	O senador Krzysztof Brejza era diretor das campanhas eleitorais do partido da oposição, Plataforma Cívica, quando foi vítima do Pegasus. Foram registrados 33 ataques ao seu telefone durante a campanha para as eleições legislativas de 2019. As mensagens foram adulteradas e divulgadas em rede de televisão controlada pelo Estado, em uma suposta campanha de difamação contra ele	Polônia	HL e FE. No caso o Pegasus não foi utilizado para fins de inquérito policia, nem mesmo de segurança nacional, mas como ferramente de acesso a material utilizado em campanha de difamação do senador Krzysztof Brejza. O material obtido foi divulgado através da televisão pública.	NA	A Polônia ainda não aplicou adequadamente a Diretiva (EU) 2016/680 (que exige norma específica em matéria de proteção de dados no âmbito da prevenção da criminalidade e de segurança nacional)	(VELD, 2023)
2019	Caso Szabolcs Panyi	Pegasus	O telefone do jornalista e editor Szabolcs foi alvo do Pegasus durante um período de sete meses no ano de 2019	Hungria	HL	NA	Lei local autoriza a interceptação de dados e funciona como uma estratégia do governo de limitar a liberdade dos meios de comunicação e de expressão. O sistema viola as exigências e normas europeias em matéria de vigilância dos cidadãos, em especial a GDPR, apesar do governo alegar razões de segurança nacional	(VELD, 2023)
2020	Caso Augury	Augury	Na compra do Augury, a Abin passou a ter acesso a sites visitados, padrão de navegação e até mesmo a informações de e-mails enviados e recebidos de uma pessoa alvo ou de um grupo. Os alvos do monitoramento eram políticos, jornalistas e ministro do STF	Brasil	HL e FE	trata-se de acesso ilegal a dados de navegação e comunicações privadas, bem como dos referentes ao tráfego de internet em desrespeito a Lei Marco Civil da Internet que proíbe os provedores a disponibilizar seus registros e a LGPD pela coleta ilegal de dados pessoais	afronta de forma subsidiária o GDPR	(MOTORYN, 2023)
2021	Caso Stavros Malichudis	Predador	O jornalista investigativo, Stavros Malichudis, que relatava questões de migração, foi alvo de vigilância pelo Serviço Nacional de Inteligência da Grécia. Seu telefone havia sido hackeado pelo *spyware* Predador. Desde então, descobriu-se que os telefones de outros jornalistas e políticos haviam sido hackeados pelo mesmo *spyware*	Grécia	HL	NA	A utilização de software espião é ilegal ao abrigo da legislação grega. Porém, para fins de serviços de inteligência, o Serviço de Informação Nacional da Grécia (EYP) tem acesso a técnicas especiais de investigação, incluindo o levantamento de confidencialidade da comunicação, em consonância com o que prevê o GDPR	(LIGER; GUTHEIL, 2023)
2021	Caso Anom	Anom	Operação realizada pela Austrália em conjunto com o FBI, que consistiu na utilização do aplicativo de mensagens Anom por criminosos. Os alvos incluíam gangues de traficantes e pessoas ligadas às máfias. Os policiais foram capazes de ler mensagens em tempo real descrevendo tramas de assassinato, planos de importação de drogas em massa e outros esquemas	USA/Austrália	HL	NA	não se aplica. Porém, o sucesso da operação facilitou a aprovação de legislação para buscar meios de acesso excepcional - *backdoors*- como o Access and Assistance Bill, na Austrália	(VIEIRA, 2021)

Fonte: A autora.

4.1.2 Ferramentas de extração de dados digitais via acesso físico a dispositivo de armazenamento

No campo da perícia digital, as ferramentas de extração de dados de vestígios digitais estão fazendo parte do cotidiano das forças policiais. Devido à diversidade dos tipos de evidências armazenadas nos vestígios digitais, existem diferentes tipos de ferramentas de perícia computacional, incluindo: ferramentas de captura de disco e dados; visualizadores de arquivos, ferramentas de análise de arquivos, ferramentas de análise de registro; ferramentas de análise de internet, ferramentas de análise de e-mail; ferramentas de análise de dispositivos móveis, ferramentas de perícia de rede; e, ainda, ferramentas de perícia de banco de dados. Normalmente, as forças policiais utilizam os Mobile Device Forensic Tools (MDFT) (conjuntos de hardware e software) em custódia de dispositivos móveis para desbloqueá-los e extrair dados, através de conexão física, que alcançam serviços de e-mail, armazenamento em nuvem, DDoS de redes sociais, histórico de localização, comunicações privadas, fotos, vídeos e, basicamente, o que mais estiver armazenado e acessível no dispositivo apreendido, incluindo dados deletados pelo usuário (RAMIRO ANDRé ANDE AMARAL; CANTO; PEREIRA MARCOS CéSAR M., 2022).

Tratando-se de vestígio digital, o perito forense será o responsável por analisar os dispositivos, potencialmente ligados a um crime, extraindo os dados que forem considerados relevantes e gerando um relatório pericial, que poderá ser utilizado como evidência em um possível julgamento. Além do procedimento técnico empregado, é essencial e necessária, uma cadeia de custódia detalhada.

Ainda que os operadores da lei autorizem o uso específico e mais pontual dos dispositivos apreendidos e sob investigação, o procedimento de extração de dados permite uma coleta estendida em relação à finalidade, ou seja, devido ao volume de informações, uma autoridade investigativa teria acesso a uma quantidade de dados pessoais muito maior que o necessário para produzir uma investigação e produzir evidências. No Brasil, a norma técnica ABNT-NBR ISO/IEC 27037, estabelece diretrizes para identificação, coleta, aquisição e preservação da evidência digital.

Tipos de ferramentas de extração de dados digitais via acesso físico

1. **Cellebrite UFED**: o Universal Forensic Extraction Device (UFED) é uma ferramenta de investigação/perícia digital, criada pela empresa israelense Cellebrite, utilizada por autoridades policiais (Polícia Civil, Polícia Federal e Institutos de Criminalísticas), para exportar dados. Apresenta-se como solução de colaboração para exportar dados de vestígios digitais em investigação, podendo realizar pesquisas de palavras chave, marcar arquivos, criar relatórios, examinar o sistema

de arquivos e navegar por ele. Utiliza uma combinação de softwares e hardwares para encontrar brechas de segurança e extrair dados de celulares com Android e Apple iOS, Symbian e MS- Windows Mobile. A extração de dados pode ser realizada com a ferramenta Cellebrite 4PC (versão software instalada em uma estação forense) ou na versão Touch (versão móvel com hardware e software acoplada em um único dispositivo portátil). O UFED permite ao usuário realizar tanto extração física quanto extração lógica. Em nenhuma das duas opções é possível obter dados excluídos (CELLEBRITE, 2025d). Com a extração de dados realizada pelo UFED, é possível a verificação de diversas condutas do usuário do aparelho celular pelo uso diário e habitual, quais sejam (SILVA; SILVA, 2020):

- registro de dia e hora em que o aparelho foi ligado e desligado;
- quais locais de rede o aparelho teve acesso;
- localização geográfica pelas antenas ERBs;
- informações de número e conta de e-mail;
- agenda de contatos do telefone;
- contatos e interação pelo uso de aplicativos (e. g. *WhatsApp*; *Telegram*; *Facebook*; *Instagram; Pinterest*);
- senhas do aparelho para múltiplas finalidades;
- aplicativos para acesso à contas bancárias;
- lista de senhas utilizadas no aparelho celular;
- quando o proprietário do aparelho acessou aplicativos, sites, e-mails, registrado no aparelho; e
- banco de arquivos com fotos, inclusive, as deletadas e outros dados.

Essa tecnologia foi determinante para a resolução do caso da morte do menino Henry Borel, de repercussão nacional, ocorrida no Rio de Janeiro/Brasil. Conforme notícia publicada no sítio do governo do Estado de Santa Catarina, o IGP/SC tem utilizado esta ferramenta desde 2015, porém, a partir de abril de 2021, todas as gerências de SC estariam operando com a ferramenta Cellebrite/UFED padronizada nos setores de informática forense (BRASIL, 2021).

2. **FTK Imager**: ferramenta forense gratuita de visualização de dados e imagens, usada para adquirir dados (evidências), desenvolvida pela AccessData. Permite criar imagens de discos rígidos locais MS-Windows e GNU/Linux, CDs e DVDs, *pen drives* ou outros dispositivos USB, pastas inteiras ou arquivos individuais de vários lugares dentro da mídia; visualizar o conteúdo de imagens armazenadas

na máquina local ou em uma unidade de rede; criar *hashes* de arquivos para verificar a integridade dos dados. A interface gráfica é totalmente modular, sendo possível movimentar e redimensionar cada um dos painéis. A ferramenta FTK Imager cria cópias de dados sem fazer alterações na evidência original e consegue identificar e analisar diversos formatos de imagem, bem como sistemas de arquivos:

- sistemas de arquivos suportados: APS, CDFS, exFAT, Ext2FS, Ext3FS, Ext4FS, FAT16, FAT32, HFS, HFS+, NTFS, ReiserFS3, VXFS e XFS; e
- formatos de imagens suportados: EnCase, Safebck 2.0, Ghost, AccessData Logical Image (AD1), SnapBack, Espert Witness, ICS, SMART, Advanced Forensics Format (AFF).

Deve ser utilizada em conjunto com outras ferramentas de indexação e processamento de evidências, como e.g., o IPED, Autopsy ou similares (ACCESSDATA, 2021).

3. **EnCase Forensic**: é um sistema integrado de análise forense baseado no ambiente MS-Windows. Realiza investigações completas em dispositivos eletrônicos, padroniza laudos periciais, organiza banco de dados de evidências, recupera arquivos apagados, fornece senhas de arquivos criptografados, analisa hardwares e e-mails, pesquisa palavras chaves, além de fornecer relatórios detalhados. O EnCase Forensic produz uma duplicação binária exata do dispositivo ou meio original e logo a verifica gerando valores *hash* das imagens e atribui valores de CRC aos dados (INTERNATIONAL, 2025). Estas verificações revelam quando a evidência foi alterada ou manipulada indevidamente, ajudando a manter toda a evidência digital com validade para efeitos legais, para o seu uso em procedimentos judiciais. O EnCase Forensic se aplica, no tratamento de evidências digitais, nas fases de (INTERNATIONAL, 2025):

   - exame/aquisição: adquire dados de equipamentos com os sistemas operativos: Apple iOS, Google Android, Rim Blackberry, Nokia Symbian e Microsoft Windows Mobile;
   - análise: automatiza tarefas comuns associadas com a preparação de evidências para investigação, que inclui: recuperação de pastas, análise de assinatura de arquivo, análise de arquivo protegido, análise *hash*, expansão de arquivos compostos, encontrar e-mails, encontrar artefatos de Internet, procurar palavras chaves, index; e
   - resultados: cria relatórios personalizados que podem ser guardados nos formatos Text, RTF, HTML, XML, PDF.

Em síntese, o processo utilizado pelo EnCase começa com a criação das imagens dos discos (disquetes, Zips, Jaz, CD-ROMs e discos rígidos) relacionados ao caso investigado. Depois da criação das imagens, chamadas de EnCase Evidence Files, pode-se adicioná-las a um único caso (case file) e conduzir a análise em todas elas simultaneamente. O EnCase não opera na mídia original ou discos espelhados, este monta os Evidence Files como discos virtuais protegidos contra escritas. Este recurso garante que seja mantida a integridade e a confidencialidade das evidências. O EnCase (não o sistema operacional Ms-Windows) reconstrói o sistema de arquivos contido em cada Evidence File, permitindo ao investigador visualizar, ordenar e analisar os dados, através de uma interface gráfica (HOLPERIN; LEOBONS, 2025).

4. **IPED Digital Forensics**: software de código aberto, implementado em Java e desenvolvido no Brasil por peritos da Polícia Federal para a investigação da Operação Lava Jato, em 2012. Consiste num sistema para indexação e processamento de evidências digitais, que busca e organiza dados de interesse em arquivos visíveis, ocultos, apagados e fragmentados que estejam em dispositivos como discos rígidos, pendrives, cartões de memória, SSDs, CDs, DVDs e outros tipos de mídias de armazenamento. A ferramenta permite a análise integrada das informações armazenadas nos dispositivos apreendidos, recuperação de arquivos deletados, identificação de criptografia, localização de palavras, reconhecimento ótico de caracteres, detecção de nudez, cruzamento de informações, rastreamento de localização. Usa a biblioteca Sleuth Kit para decodificar imagens de disco e sistemas de arquivos (IPED. . . , 2025). Após a análise, o programa dispõe de recursos para geração de relatórios de fácil leitura com os resultados obtidos. Possui a funcionalidade de identificação de nudez (análises e exames que detectam a nudez em imagens), capaz de contribuir com investigações relacionadas aos casos de pornografia infantil (PINHEIRO, 2025).

5. **Autopsy**: ferramenta que permite analisar com eficiência discos rígidos e *smartphones*, realizando a análise da linha do tempo, filtragem de *hash*, pesquisa de palavras-chave, artefatos da web, multimídia. Possui uma arquitetura de *plugin* que permite encontrar módulos complementares ou desenvolver módulos personalizados em Java ou Python (AUTOPSY, 2025).

6. **Volatility**: ferramenta forense de código aberto para extração de artefatos digitais de amostras de memória volátil (RAM). Utilizado em ambientes Linux e sistema operacional MS-Windows. Possui vasta gama de *plugins* e consegue extrair informações como lista de processos, rastro de *malwares*, conexões de IPs e *payloads*. Suporta uma variedade de formatos de arquivos e capacidade de

convertê-los. As técnicas de extração são realizadas independentes do sistema que está sendo investigado (VOLATILITY, 2025).

7. **Oxygen Forensic**: ferramenta comercial desenvolvida pela empresa americana Oxygen Software, focada em dispositivos móveis. A plataforma foi construída para extrair, decodificar e proceder a análise de dados de diversas fontes digitais, como dispositivos móveis (google Android e Apple iPhone), nuvem, drones, cartões de mídia, backups e dados IoT. Esta usa métodos físicos para contornar a segurança do dispositivo (como bloqueio de tela) e coleta dados de autenticação para vários aplicativos móveis diferentes (POSTON, 2021).

8. **XRY**: é uma coleção de diferentes ferramentas comerciais para análise forense de dispositivos móveis, desenvolvida pela empresa sueca MSAB. É executado no sistema operacional MS-Windows. O XRY é conhecido por suas práticas seguras de gerenciamento de evidências, garantindo a integridade dos dados durante toda a investigação forense. Este pode recuperar dados que foram apagados. O XRY Logical é um conjunto de ferramentas projetadas para interagir com o sistema operacional do dispositivo móvel. Essa versão realiza a extração lógica do aplicativo e dos dispositivos móveis, recuperando dados de forma rápida e segura, tanto em cartão SIM quanto na memória interna. Outras informações que podem ser extraídas são agendas telefônicas, mensagem SMS enviadas, recebidas e arquivadas, fotos, arquivos de som, IMEI e outros dados. Já XRY Physical, permite a extração de forma rápida e eficiente do conteúdo protegido ou apagado existente no telefone celular, a aquisição física de dados é feita a partir de Hex-Dumps da memória do telefone e dos cartões (POSTON, 2021).

9. **Axiom**: funciona, especialmente, com muitas evidências digitais, quando a correlação de dados de vários dispositivos é necessária. A ferramenta analisa grandes volumes de dados de forma eficiente, consolidando as informações de todos os dispositivos relacionados a um só caso. A desvantagem é seu alto custo (MAGNET FORENSICS, 2025).

10. **Passware**: ferramenta de descoberta de evidências eletrônicas criptografadas que revela e descriptografa todos os itens protegidos por senha em um computador. O software, desenvolvido pela empresa Passware Inc, reconhece mais de 300 tipos de arquivos e funciona no modo de lote, recuperando senhas. Este permite aquisição de dados em nuvem, versão para Apple MacOS e MS-Windows. Executa tarefas de recuperação de senha para vários arquivos e imagens FDE, um por um, sem interação do usuário. Descriptografa e/ou recupera senhas para imagens de disco APFS, Apple DMG, BitLocker, Dell, FileVault2, LUKS, McAfee, PGP, Symantec, TrueCrypt e VeraCrypt (ONRETRIEVAL GROUP, 2025).

A Tabela 6 resume os dados das ferramentas apresentadas nesta subseção identificando sua fase na cadeia de custódia.

Tabela 6 – Ferramentas de extração de dados em perícia digital.

	Cellebrite UFED	**FTK Imager**	**EnCase Forensic**	**IPED Digital Forensics**	**Autopsy**	**Volatility**	**Oxygen Forensics**	**XRY**	**Axiom**	**Passware**
Tipo de ferramenta	Análise de dispositivos móveis	Ferramenta de captura de disco e dados	Ferramenta de captura de disco e dados	Ferramenta de exportação e extração de arquivos	Ferramenta de captura de disco e dados	Perícia de memória	Análise de dispositivos móveis	Análise de dispositivos móveis	Análise de dispositivos móveis	Ferramenta de descriptografia
Plataforma	MS-Windows, MAC	MS-Windows	MS-Windows	MS-Windows, Mac e Linux	MS-Windows, Linux	MS-Windows, Linux	MS-Windows, Mac e Linux	MS-Windows	MS-Windows	MS-Windows, Mac e Linux
Licença	Proprietário	Proprietário	Proprietário	Gratuito	Gratuito	Gratuito, GPL	Proprietário	Proprietário	Proprietário	Proprietário
Código	Fechado	Fechado	Fechado	Aberto	Aberto	Aberto	Fechado	Fechado	Fechado	Fechado
Fase perícia	Exame e análise	Exame e análise	Exame, análise e resultado/relatório	Exame, análise e resultado/relatório	Exame e análise	Exame e análise	Exame, análise e resultado/relatório	Exame, análise e resultado/relatório	Exame e análise	Exame e análise
Fase cadeia de custódia	Processamento	Processamento	Processamento	Processamento	Processamento	Processamento	Processamento	Processamento	Processamento	Processamento

Fonte: A autora.

Observa-se, do exposto nesta seção, que a extração de dados de dispositivos eletrônicos tem se tornado um meio fundamental de obtenção de prova, em especial em dispositivos móveis, o que tem resultado em transformações substanciais na matéria probatória dos processos penais.

4.1.3 Análise

A prática de explorar vulnerabilidades em dispositivos para extração em massa de dados pessoais e para acesso e monitoramento remoto, operam uma forma de *hacking* em sua grande maioria legitimado pelo Estado, colocando autoridades investigativas e de inteligência no polo ativo de uma dinâmica que explora falhas de segurança da coletividade e do devido processo investigativo e legal.

Objetivou-se, aqui, apresentar o *status quo* das ferramentas de *hacking* tanto na estrutura investigativa no Brasil, quanto a nível internacional, incluindo suas funcionalidades, sua categorização dentro da cadeia de custódia da perícia digital e os riscos relacionados à proteção da privacidade e de dados, não somente dos indivíduos, mas da coletividade, em sintonia ou não com as bases legais para o tratamento de dados pessoais do GDPR e LGPD.

Nota-se, também, uma diversidade de empresas que fornecem essas ferramentas para as forças de investigação e vigilância nos países, bem como a imaturidade do estado regulatório e procedimental, devendo a capacidade investigativa do Estado se necessariamente limitada em seu uso, a fim de evitar abusos e desvios de finalidade, de forma a caracterizar a prática do FE. É importante ressaltar, neste momento, a importância da obediência a cadeia de custódia no processo de investigação criminal e persecução penal. Pode-se dizer que o valor da cadeia de custódia é sensivelmente incrementado quando o elemento probatório é de natureza digital, dado o grau de dificuldade de se preservar sua integridade e autenticidade, além dos riscos concretos de manipulação e alteração dos dados. Segundo (PRADO, 2021), quando a prova está armazenada em dispositivos móveis, incidem duas diferentes cadeias

de custódia: uma sobre o equipamento em si, e outra sobre os dados coletados no equipamento apreendido.

Nesse cenário, em que as demandas relacionadas às provas digitais são cada vez maiores, é difícil imaginar um caminho que não passe por um rigor técnico maior e inciativas legais e jurídicas especificamente no que diz respeito com os temas de responsabilização criminal, segurança pública e proteção dos dados pessoais. Esse é o contexto que perneia o GDPR e a LGPD quando o tema é a segurança pública, defesa nacional, segurança de Estado e atividades de investigação e repressão penal.

Em relação à LGPD, ainda que o legislador tenha optado por não contemplar esta questão em seu corpo legal, apontando a necessidade de que a matéria seja tratada em lei específica (art. 4, III) seus princípios norteadores deverão abarcar a legislação superveniente, tendo em vista a compreensão de que privacidade e proteção de dados pessoais são direitos fundamentais. Portanto, princípios de devido processo, necessidade e proporcionalidade deverão incidir e serem observados no âmbito da persecução penal e de fins investigativos. Como já mencionado neste trabalho, a regulação do tratamento de dados para os fins do inciso III do art. 4º da LGPD ainda é anteprojeto de lei, recentemente apresentado à Câmara dos Deputados com a finalidade específica de propor regulamentação para o tema.

No contexto da UE, a Diretiva (UE) 681/2016, implementando o que restou determinado no GDPR, estabeleceu um regime geral de proteção de dados pessoais no âmbito de investigações criminais, consolidando diretrizes e princípios de legalidade, necessidade e proporcionalidade no uso de métodos que envolvam o processamento de dados pessoais, aplicável, portanto, a casos que envolvam técnicas de *hacking* por agências investigativas (RAMIRO ANDRé ANDE AMARAL; CANTO; PEREIRA MARCOS CéSAR M., 2022). Mais especificamente, com relação ao Pegasus e softwares de vigilância similares, foi elaborada uma Recomendação do Parlamento Europeu, datada de 15 de junho de 2023, na sequência da investigação de alegadas contravenções e má administração na aplicação do Direito da UE relacionadas com a utilização do software espião de vigilância Pegasus e equivalentes (PARLAMENTO EUROPEU, 2023).

As Tabelas 7 e 8 mostram uma síntese das ferramentas de *hacking*, apresentando suas características, identificando-as dentro da cadeia de custódia digital e relacionando-as com as legislações GDPR e LGPD e correlações.

Tabela 7 – Análise ferramentas acesso remoto de dados armazenados ou em trânsito.

Ferramentas/ softwares	Tipo	Características	HL	FE	LGPD	GDPR	Cadeia de custódia	Técnicas/ métodos ataques	Acessos	Ref.
Carnivore (DCS1000)	Software de vigilância para redes de dados	Desenvolvido pelo FBI para auxiliar nos investigações de atos terroristas (1997-2001)	Sim	Sim	NA	NA	Processamento	Posiciona-se em um segmento de rede e monitora o tráfego de usuários designados, procurando por palavras-chave específicas	Identifica e armazena o tráfego da Internet (e-mail, navegação na web, etc) em uma relde local específica	(OPENCARNIVORE.ORG, 2025)
KLS	Keylogger	Malware que registra a digitação do teclado ou toques de celular ou tablet e envia informações para o controlador	Sim	Sim	NA	NA	Processamento	Registra as teclas digitadas no dispositivo alvo	Captura de senhas, informações de contas, e-mails, pesquisas e outras informações digitadas no dispositivo no qual foi instalado	(QUINLAN; WILSON, 2016)
Pegasus	Spyware	Transforma o *smartphone* em um dispositivo de vigilância 24 horas	Sim	Sim	Sim, embora a LGPD preveja legislação específica, ainda não editada, aplica-se, por analogia, a Lei 12.965/2014 (Marco Civil da Internet) e Lei 9.296/1996 (Lei da Interceptação telefônica)	Sim, inclusive foi elaborada, pelo Parlamento Europeu uma Recomendação de 2023 referente a utilização do Pegasus e equivalentes	Processamento	Ataque "click zero", link malicioso, transmissão sem fio, instalação manual	Rede social, Whatsapp, agenda, fotos e vídeos, SMS, geolocalização/GPS, microfone, calendário, e-mail, mensagens, contatos, câmera, senhas	(PARLAMENTO EUROPEU, 2023); (PEGG; CUTLER, 2021)
Prism	Programa de vigilância	Coleta dados posteriormente analisados e armazenados através de outros programas que fazem parte do sistema de vigilância e espionagem implantado pela NSA	Sim	Sim	NA	NA, USA promulgaram em 06/ 2015 a lei USA Freedom Act. Aprovaram a reautorização da seção da Foreign Intelligence Surveillance Act -FISA), que permite monitorar e recolher dados pessoais, sem mandados, de cidadãos americanos e não americanos em todo o mundo, incluindo europeus, em dissonância com o GDPR	Processamento	Funciona através de grandes sistemas de roteadores pelos quais é analisada o tráfego de dados em escala global	Serviços da Internet, hitórico de pesquisas, e-mails, transferências de arquivos, vídeos, fotos, redes sociais	(LIGER; GUTHEIL, 2023); (ELCI, 2024)
Predador	Spyware	Ferramenta de vigilância da Cytrox, que oferece ao operador acesso total e contínuo ao dispositivo móvel alvo	Sim	Sim	Sim, embora a LGPD preveja legislação específica, ainda não editada, aplica-se, por analogia, a Lei 12.965/2014 (Marco Civil da Internet) e Lei 9.296/1996 (Lei da Interceptação telefônica)	Sim, inclusive foi elaborada, pelo Parlamento Europeu uma Recomendação de 2023 referente a utilização do Pegasus e equivalentes	Processamento	*Exploit* de um clique, requer alguma ação por parte da vítima	Senhas, arquivos, fotos, histórico de navegação na web, contatos, captura de telas, registro de entradas do usuário, microfone, câmera, mensagens de texto e chamadas telefônicas	(LIGER; GUTHEIL, 2023)
Anom	Aplicativo de mensagens	Uso de criptografia para cifrar mensagens enviadas, fazendo os usuários acreditaram ser um aplicativo seguro. Parceria entre FBI e governo da Austrália	Sim	Sim	NA	NA, em decorrência, a Austrália aprovou a Lei Access and Assistance Bill. Em vários países foram aprovadas legislações para acesso excepcional como *backdoors* e apoio ao *Going Dark*	Processamento	Uso de criptografia para cifrar as mensagens enviadas	Acesso ilimitado e em tempo real às comunicações realizadas dentro do aplicativo	(VIEIRA, 2021)
Augury	Spyware	Criado pela empresa Team Cymru, permite o rastreamento digital contínuo de cidadãos	Sim	Sim	Sim, embora a LGPD preveja legislação específica, ainda não editada, aplica-se, por analogia, a Lei 12.965/2014 (Marco Civil da Internet) e Lei 9.296/1996 (Lei da Interceptação telefônica)	Sim, inclusive foi elaborada, pelo Parlamento Europeu uma Recomendação de 2023 referente a utilização do Pegasus e equivalentes	Processamento	Captura de dados de tráfego (com a indicação de endereço de IP)	URLs, cookies de sessão, detalhes de navegação, e-mails, credenciais de acesso como usuário e senha	(MOTORYN, 2023)
FirstMile	Spyware	Desenvolvido pela Cognyte, tem a capacidade de monitorar a geolocalização	Sim	Sim	Sim, embora a LGPD preveja legislação específica, ainda não editada, aplica-se, por analogia, a Lei 12.965/2014 (Marco Civil da Internet) e Lei 9.296/1996 (Lei da Interceptação telefônica)	Sim, inclusive foi elaborada, pelo Parlamento Europeu uma Recomendação de 2023 referente a utilização do Pegasus e equivalentes	Processamento	Invade e engana a rede de empresas de telefonia para rastrear o alvo monitorado	Geolocalização dos clientes de empresas de telefonia	(BRASIL, 2023)

Fonte: A autora.

Tabela 8 – Análise ferramentas de extração de dados digitais via acesso físico a dispositivo de armazenamento.

Ferramentas/ softwares	Tipo	Características	HL	FE	LGPD	GDPR	Cadeia de custódia	Técnicas/métodos ataques	Acessos	Ref.
Cellebrite UFED	Ferramenta de extração de dados	Tem capacidade de desbloquear celulares com Android e iOs e acessar mensagens e dados apagados dos dispositivos	Sim	Sim. O acesso às informações e extração de dados deve observar os limites de suas autorizações, não podendo resultar em extração completa de dados do investigado ou de terceiros	Sim. Embora a LGPD preveja legislação específica, ainda não editada, com respaldo da Lei 9.613/98, e com a devida autorização judicial	Sim, devendo ser observadas as diretrizes e princípios da Diretiva (EU) 681/2016	Processamento	Extração de dados de aparelhos celulares, cartoes de memória e drones, incluse dados apagados	Quebra de senha, descriptografia, leitura facial, relatórios	(CELLEBRITE, 2025d);(SILVA; SILVA, 2020)
FTK Imager	Ferramenta de extração de dados e imagens	Ferramenta gratuita, desenvolvida pela AccessData	Sim	Sim. O acesso às informações e extração de dados deve observar os limites de suas autorizações, não podendo resultar em extração completa de dados do investigado ou de terceiros	Sim. Embora a LGPD preveja legislação específica, ainda não editada, com respaldo da Lei 9.613/98, e com a devida autorização judicial	Sim, devendo ser observadas as diretrizes e princípios da Diretiva (EU) 681/2016	Processamento	Cria imagens de discos rígidos locais, CDs e DVDs, *pen drives* ou outros dispositivos USB; visualizar conteúdo de imagens armazenadas em máquina local ou unidade de rede	Visualizar conteúdo de imagens armazenadas em máquina local ou unidade de rede	(ACCESSDATA, 2021)
EnCAse Forensic	sistema integrado de análise forense baseado no ambiente MS-Windows	Recupera arquivos apagados, fornece senhas de arquivos criptografados, analisa hardwares e e-mails, pesquisa palavras chaves e fornece relatórios	Sim	Sim. O acesso às informações e extração de dados deve observar os limites de suas autorizações, não podendo resultar em extração completa de dados do investigado ou de terceiros	Sim. Embora a LGPD preveja legislação específica, ainda não editada, com respaldo da Lei 9.613/98, e com a devida autorização judicial	Sim, devendo ser observadas as diretrizes e princípios da Diretiva (EU) 681/2016	Processamento	Produz uma duplicação binária exata do dispositivo ou meio original e gera valores *hash* das imagens e atribui valores CRC aos dados	Cria relatórios personalizados em formatos Text, RTF, HTML, XML, PDF	(INTERNATIONAL, 2025); (HOLPERIN; LEOBONS, 2025)
IPED Digital Forensics	Software forense de código aberto	Sistema para indexação e processamento de evidências digitais implementado em Java e desenvolvido no Brasil por peritos da Polícia Federal	Sim	Sim. O acesso às informações e extração de dados deve observar os limites de suas autorizações, não podendo resultar em extração completa de dados do investigado ou de terceiros	Sim. Embora a LGPD preveja legislação específica, ainda não editada, com respaldo da Lei 9.613/98, e com a devida autorização judicial	Sim, devendo ser observadas as diretrizes e princípios da Diretiva (EU) 681/2016	Processamento	Análise integrada das informações armazenadas, recuperação de arquivos deletados, identificação de criptografia, localização de palavras, reconhecimento ótico de caracteres, detecção de nudez, cruzamento de informações, rastreamento de localização	Busca e organiza dados em arquivos visíveis, oculto, apagados e fragmentados. Gera relatórios com os resultados obtidos	(IPED. . . , 2025)
Autopsy	Ferramenta forense e interface gráfica de código aberto	Análise de discos rígidos e *smartphones*, baseado em HTML	Sim	Sim. O acesso às informações e extração de dados deve observar os limites de suas autorizações, não podendo resultar em extração completa de dados do investigado ou de terceiros	Sim. Embora a LGPD preveja legislação específica, ainda não editada, com respaldo da Lei 9.613/98, e com a devida autorização judicial	Sim, devendo ser observadas as diretrizes e princípios da Diretiva (EU) 681/2016	Processamento	Realiza análise da linha do tempo, filtragem de *hash*, pesquisa de palavras-chave, artefatos da web, multimídia. Executa tarefas em segundo plano e em paralelo	Acessa arquivos e artefatos da *web* como histórico, favoritos e *cookies* do Firefox, Chrome e IE, fotos e vídeos	(AUTOPSY, 2025)
Volatility	Ferramenta forense de código aberto	Extração de artefatos digitais de amostras de memória volátil (RAM)	Sim	Sim. O acesso às informações e extração de dados deve observar os limites de suas autorizações, não podendo resultar em extração completa de dados do investigado ou de terceiros	Sim. Embora a LGPD preveja legislação específica, ainda não editada, com respaldo da Lei 9.613/98, e com a devida autorização judicial	Sim, devendo ser observadas as diretrizes e princípios da Diretiva (EU) 681/2016	Processamento	Possui vasta gama de *plugins* e suporta uma variedade de formatos de arquivos e capacidade de convertê-los	Extrai informações como lista de processos, rastro de *malwares*, conexões de Ips e *payloads*	(VOLATILITY, 2025)
Oxygen Forensics	Ferramenta comercial forense	Desenvolvida pela empresa americana Oxygen Software, focada em dispositivos móveis	Sim	Sim. O acesso às informações e extração de dados deve observar os limites de suas autorizações, não podendo resultar em extração completa de dados do investigado ou de terceiros	Sim. Embora a LGPD preveja legislação específica, ainda não editada, com respaldo da Lei 9.613/98, e com a devida autorização judicial	Sim, devendo ser observadas as diretrizes e princípios da Diretiva (EU) 681/2016	Processamento	Contorna a segurança do dispositivo (como bloqueio de tela) e coleta dados de autenticação para vários aplicativos móveis diferentes	Extrai, decodifica e procede a análise de dados de diversas fontes digitais, como dispositivos móveis (Android e iPhone), nuvem, drones, cartões de mídia, backups e dados Iot	(POSTON, 2021)
XRY	Ferramenta comercial forense	Análise forense de dispositivos móveis, desenvolvida pela empresa sueca MSAB	Sim	Sim. O acesso às informações e extração de dados deve observar os limites de suas autorizações, não podendo resultar em extração completa de dados do investigado ou de terceiros	Sim. Embora a LGPD preveja legislação específica, ainda não editada, com respaldo da Lei 9.613/98, e com a devida autorização judicial	Sim, devendo ser observadas as diretrizes e princípios da Diretiva (EU) 681/2016	Processamento	Realiza a extração lógica do aplicativo e dos dispositivos móveis, recuperando dados de forma rápida e segura, tanto em cartão SIM quanto na memória interna	Agendas telefônicas, mensagem SMS enviadas, recebidas e arquivadas, fotos, arquivos de som, IMEI e outros dados	(POSTON, 2021)
Axiom	Plataforma de investigação	Criada pela Magnet, oferece recursos avançados para visualização e análise inteligente de dados.	Sim	Sim. O acesso às informações e extração de dados deve observar os limites de suas autorizações, não podendo resultar em extração completa de dados do investigado ou de terceiros	Sim. Embora a LGPD preveja legislação específica, ainda não editada, com respaldo da Lei 9.613/98, e com a devida autorização judicial	Sim, devendo ser observadas as diretrizes e princípios da Diretiva (EU) 681/2016	Processamento	Identifica *deepfakes* ou mídias sintéticas e auxilia na localização de evidências. Realiza extrações de dispositivos móveis com suporte para ferramentas como Cellebrite, Oxygen e outros	Acessa dados do sistema de arquivos, registro e artefatos utilizando links ativos, múltiplas visualizações, filtros, pesquisas e gera relatórios personalizáveis	(MAGNET FORENSICS, 2025)
Passware	Ferramenta de descoberta de evidências eletrônicas criptografadas	Revela e descriptografa todos os itens protegidos por senha em um computador	Sim	Sim. O acesso às informações e extração de dados deve observar os limites de suas autorizações, não podendo resultar em extração completa de dados do investigado ou de terceiros	Sim. Embora a LGPD preveja legislação específica, ainda não editada, com respaldo da Lei 9.613/98, e com a devida autorização judicial	Sim, devendo ser observadas as diretrizes e princípios da Diretiva (EU) 681/2016	Processamento	Executa tarefas de recuperação de senha para vários arquivos e imagens FDE, um por um, sem interação do usuário.	Arquivos e imagens FDE	(ONRETRIEVAL GROUP, 2025); (PASSWARE, 2025)

Fonte: A autora.

A visto do que foi exposto, pode-se dizer que as tecnologias digitais modificaram a dinâmica da investigação e do processo penal, no que diz respeito à obtenção

de prova digital e cadeia de custódia, impondo a utilização de ferramentas *big tech* para a extração de dados de aparelhos digitais objeto de investigação criminal, sobretudo as desenvolvidas pela Cellebrite, o que vem a justificar o estudo de caso da próxima seção.

4.2 ESTUDO DE CASO CELLEBRITE

O avanço da investigação forense de dispositivos móveis tem sido significativo ao logo do tempo, decorrente da crescente dependência de *smartphones* e *tablets* em diversos ambientes pessoais e profissionais. À medida que os avanços tecnológicos continuam, os desafios e as complexidades relacionadas à extração e interpretação de dados de dispositivos móveis também progridem.

A variedade de dispositivos móveis e sistemas operacionais, bem como a criptografia, a proteção por senha e diversos recursos de segurança, podem dificultar a extração de dados durante a perícia forense. Além disso, o procedimento pode ser demorado e exigir equipamentos e conhecimento especializados para sua execução (PATEL; MANN, 2024). As tecnologias de extração de dados em dispositivos móveis envolvem a conexão física do dispositivo a ser analisado em um dispositivo/ferramenta que extrai, analisa e apresenta os dados contidos no dispositivo avaliado (PRIVACY INTERNATIONAL, 2019).

O Cellebrite UFED representa uma ferramenta poderosa para a extração e análise de dados de dispositivos móveis na área da perícia forense digital. Permite a extração, decodificação e análise de dados de uma gama de dispositivos digitais como e.g., *smartphones*, celulares básicos, celulares básicos, *tablets*, dispositivos GPS, drones e mídias de armazenamento removíveis (MALINDA, 2024). Utiliza metodologias e algorítimos que permitem aos profissionais forenses recuperarem dados que podem ter sido previamente ocultados ou excluídos no dispositivo, bloqueados ou criptografados, incluindo imagens de texto, registros de chamadas, e-mails, conteúdo de mídia social e outros (PRASHI; AMARNATH, 2023).

As técnicas de acesso e extração de dados em dispositivos móveis variam de acordo com o hardware e o software de dispositivo, desde o *chipset* (e.g., Qualcomm, MediaTek) até a versão do sistema operacional. Variam, também, em tecnicidade e no tipo e volume de dados que se quer extrair (PATEL; MANN, 2024). Após a fase de extração, os dados obtidos passam por uma análise, na qual os especialistas forenses examinam cada detalhe de forma a subsidiar os procedimentos investigativos (MALINDA, 2024). Em cada fase da perícia forense de dispositivos móveis, é de vital importância a manutenção da cadeia de custódia de a garantir a preservação, confiabilidade e integridade das evidências coletadas ao longo do inquérito.

4.2.1 Métodos de extração

Os métodos de extração suportados pelo Cellebrite UFED incluem extração lógica, extração de sistema de arquivos e extração física.

4.2.1.1 Extração lógica

A extração lógica recupera dados em arquivos e diretórios a partir do sistema operacional do dispositivo. Isto significa que a ferramenta de extração de dados se comunica com o sistema operacional do dispositivo e solicita as informações do sistema. Pode ser realizada de duas formas: Unidades Software-Hardware ou Softwares próprios para realização da extração lógica (SCHMITZ; MELO; CARDOSO, 2017).

A extração lógica envolve conectar o dispositivo móvel ao hardware forense ou a uma estação de trabalho forense via cabo USB, cabo RJ-45, infravermelho ou *bluetooth*. Depois que o dispositivo móvel é conectado, a ferramenta forense inicia um comando e o envia para o dispositivo que é interpretado pelo processador, comunicando-se com o sistema operacional do dispositivo alvo (PRASHI; AMARNATH, 2023).

A extração lógica de dados é realizada, em grande parte, por meio de uma interface de programação de aplicativos (API) designada, disponível no fornecedor do dispositivo . Assim como a API permite que aplicativos comerciais de terceiros se comuniquem com o sistema operacional do dispositivo, ela também permite a extração de dados. Após a conexão, a Cellebrite UFED carrega a API do fornecedor no dispositivo, fazendo camadas de API somente leitura para solicitar os dados do dispositivo alvo. O dispositivo móvel responde às solicitações válidas da API para extrair itens como mensagens de texto (SMS), entradas da agenda telefônica, fotos, etc (PRIVACY INTERNATIONAL, 2019).

Dos três tipos de extração, a lógica é vista como a mais rápida, menos invasiva e mais limitada. Nesse processo é criada uma cópia dos arquivos acessíveis ao usuário como e.g., agenda telefônica, chamadas, mensagens, dados de aplicativos e dados de *backup* do apple iTunes ou Google Android, ou seja, dados obtidos no exame manual das telas do dispositivo (PRASHI; AMARNATH, 2023).

4.2.1.2 Extração de sistema de arquivos

A extração de sistema de arquivos é tecnicamente vista como um tipo de extração lógica, porém é mais rica em dados, i.e., todo o sistema de arquivos e diretórios é acessado. Um sistema de arquivos contém os arquivos e pastas que o dispositivo usa para aplicativos, configurações de sistema e do usuário, juntamente com as áreas de armazenamento (PRIVACY INTERNATIONAL, 2019). Esse tipo de extração é diferente da extração física, que envolve o acesso direto aos meio de armazenamento do

dispositivo, e da extração lógica, que envolve a extração de dados usando um software especializado.

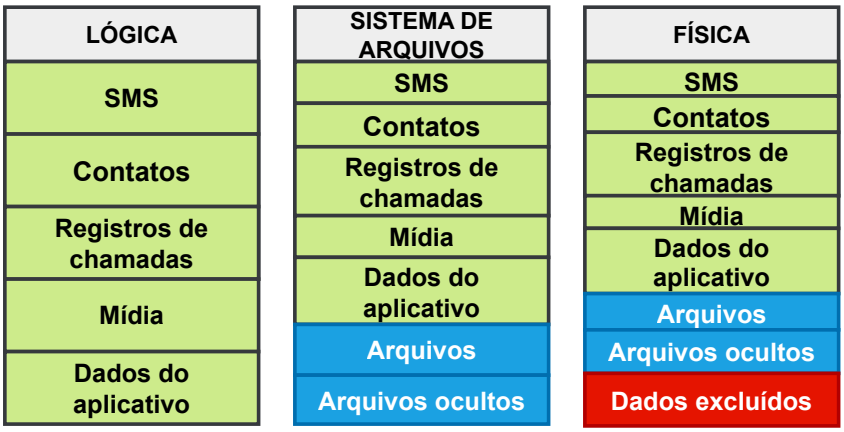
A extração de sistema de arquivos é usada para extrair tipos específicos de dados, como documentos, mensagens de e-mail ou fotos, em vez de todo o conteúdo do armazenamento do dispositivo. É, geralmente, feita por um usuário *root*, com controle privilegiado sobre o dispositivo. Os dados extraídos são então analisados para recuperar arquivos excluídos, extrair evidências ou investigar qualquer atividade suspeita no dispositivo (CELLEBRITE, 2025b). Ao contrário de uma extração lógica, uma vez obtido o sistema de arquivos, este precisa ser decodificado. O processo de decodificação converte os dados brutos em um arquivo de banco de dados para um formato reconhecível. Os dados extraídos por APIs e *backups* não exigem decodificação, pois são intrínsecos a esses métodos, como fotos e vídeos. No entanto, arquivos de banco de dados que contêm mensagens de texto devem ser decodificados separadamente para que se possa analisar as mensagens. Uma extração completa de sistema de arquivos pode obter aplicativos de terceiros excluídos de um backup do iTunes. Pode, também, identificar locais de interesse do dispositivo, revelar *logs* do sistema e dados de *log* do aplicativo (PRIVACY INTERNATIONAL, 2019).

4.2.1.3 Extração física

A extração físcia é uma cópia bit a bit do armazenamento físico, sistema de aquivos, memória do dispositivo ou *dump* hexadecimal. Geralmente, requer cabeamento específico e envolve a inicialização do dispositivo em um sistema operacional personalizado (SCHMITZ; MELO; CARDOSO, 2017). Este tipo de extração consiste de uma varredura seguida da aquisição de dados contidos na memória *flash* do dispositivo, sendo então realizada uma cópia minuciosa bit a bit e tendo a possibilidade da aquisição de arquivos apagados (CRUZ, 2017). É considerada a mais abrangente e invasiva das extrações e inclui todo o espaço não alocado no dispositivo, podendo incluir arquivos excluídos (SCHMITZ; MELO; CARDOSO, 2017).

A extração física pode usar o modo de resgate ou download do dispositivo, que permite a inserção de um pequeno pedaço de código, chamado *bootloaders*, na memória RAM durante a inicialização. O *bootloader* lê o conteúdo da memória do dispositivo alvo e o envia de volta ao dispositivo de extração. Os gerenciadores de inicialização do Cellebrite UFED são projetados levando em consideração as variedades de *chipsets*, periféricos, interfaces de chip de memória e controladores USB. O Cellebrite UFED tem permissão para acessar internamente os sistemas operacionais depois que os dados já foram descriptografados (PRIVACY INTERNATIONAL, 2019). A Figura 13 mostra os tipos de dados que podem ser extraídos usando extração lógica, sistema de arquivos e extração física.

Figura 13 – Extração Lógica, Sistema de arquivos e Física na ferramenta Cellebrite UFED.



Fonte: (INTERNATIONAL, 2019).

A extração de dados depende do tipo de dispositivo e da ferramenta forense utilizada. Portanto, de acordo com os níveis de proteção de dados e o sistema operacional utilizado (pois mecanismos de segurança e métodos de criptografia utilizados são diferentes), o investigador necessita usar metodologias de extração diferentes para a recuperação máxima dos dados, como é mostrado na Figura 13.

4.2.1.4 Extração baseada em nuvem

A adoção de metodologias de extração baseadas em nuvem proporcionam aos investigadores acesso sem precedentes aos dados armazenados em serviços de nuvem vinculados ao dispositivo alvo, incluindo plataforma com Apple iCloud ou Google Drive. A interface amigável para este tipo de extração é o Cellebrite UFED CLOUD, permitindo a coleta e análise de domínios públicos e privados, dados de mídias sociais, mensagens instantâneas, armazenamento de arquivos, páginas da *web* e outros conteúdos com base em nuvem (MALINDA, 2024). Esta ferramenta permite obter informações, inclusive, sobre as intenções de um indivíduo, seus interesses e relacionamentos ao analisar postagens, curtidas e conexões. Permite, ainda, ver atividades e localizações de um usuário a partir do Facebook, Google e Apple iCloud através de vários dispositivos, além de correlações e conexões sobre o indivíduo alvo a partir de diferentes fontes de dados (RAMIRO ANDRé ANDE AMARAL; CANTO; PEREIRA MARCOS CéSAR M., 2022). Ha cada nova atualização é incluído suporte a novos dispositivos para acesso e extração do Cellebrite UFED (CELLEBRITE, 2025a).

Emergency Download Mode (EDL)

Uma das vulnerabilidades usadas para obter dados, principalmente em dispositivos Android, é o uso do *Emergency Download Mode* (EDL) para dispositivos com o

chipset Qualcomm (PRIVACY INTERNATIONAL, 2019).

O EDL é um modo de inicialização especial em telefones Android da Qualcomm que permite a instalação forçada de aquivos de *firmware*. Esse processo é usado para desbloquear o dispositivo e fazê-lo funcionar novamente. Um dispositivo bloqueado é aquele que essencialmente não funciona mais. O Modo EDL funciona independentemente do modo Bootloader ou Fastboot, por estar localizado na interface Bootloader Primário, podendo ser acessado por: comandos ADB, modo Fastboot, botões de hardware, cabo *Deep Flash* e pontos de teste de PCB (CELLEBRITE, 2025c).

4.2.2 Utilização da ferramenta Cellebrite no Brasil

A Tabela 9 mostra a capilaridade da ferramenta Cellebrite no âmbito da Administração Pública Federal, apontando para a existência de ferramentas de extração de dados em órgãos que, tipicamente, não conduzem investigações criminais mediante técnicas forenses (RAMIRO ANDRé ANDE AMARAL; CANTO; PEREIRA MARCOS CéSAR M., 2022).

Tabela 9 – Distribuição da ferramenta Cellebrite em âmbito federal.

Órgão	**Fabricante/Revendedor**	**Ferramenta**
Ministério da Defesa/Comando da Marinha/Diretoria de Comunicação e Tecnologia da Informação da Marinha	Cellebrite/Techbiz Forense Digital	UFED 4PC
Ministério da Defesa/Comando do Exército/Base Administrativa do CCOMGE	Cellebrite/Techbiz Forense Digital	UFED
Ministério da Economia/Fundo Constitucional do Distrito Federal/FCDF-SSP-Polícia Civil do DF	Cellebrite/Techbiz Forense Digital	UFED Premium
Ministério da Justiça e Segurança Pública/Departamento de Polícia Federal/Superintendência Regional no Estado de SP	Cellebrite/Techbiz Forense Digital	UFED 4PC, UFED Touch2, UFED Cloud, UFED Desktop Analytics, Cellebrite Commander
Ministério da Justiça e Segurança Pública/Departamento de Polícia Federal/Superintendência Regional no Estado de AM	Cellebrite/Techbiz Forense Digital	Cellebrite Advanced Services
Ministério da Justiça e Segurança Pública/Departamento de Polícia Federal/Superintendência Regional da Polícia Rodoviária de Goiás	Cellebrite/Techbiz Forense Digital	UFED Touch, UFED Cloud, UFED Pathfinder
Ministério da Justiça e Segurança Pública/Departamento de Polícia Federal/Diretoria Técnico Científica	Cellebrite/Techbiz Forense Digital	UFED 4PC
Ministério da Justiça e Segurança Pública/Coordenação Geral de Logística e Contratos	Cellebrite/Techbiz Forense Digital	UFED
Ministério da Justiça e Segurança Pública/Conselho Administrativo de Defesa Econômica CADE	Cellebrite/Techbiz Forense Digital	UFED Touch
Ministério da Justiça e Segurança Pública/Fundo Nacional de Segurança Pública	Cellebrite/Techbiz Forense Digital	UFED

Fonte: A autora.

No nível estadual, a utilização das ferramentas Cellebrite UFED se dá, principalmente, pelas Secretarias de Estado de Segurança Pública - Polícias Civis, pelos Ministérios Públicos Estaduais e pelas Procuradorias Gerais de Justiça (Tabela 10) (RAMIRO ANDRé ANDE AMARAL; CANTO; PEREIRA MARCOS CéSAR M., 2022). Esse cenário de operacionalização das ferramentas de *hacking* (e.g., o Cellebrite Cel-

Tabela 10 – Distribuição da ferramenta Cellebrite por estados da federação.

UF	Órgão	Fabricante/Revendedor	Ferramenta
Acre	Secretaria de Estado da Justiça e Segurança Pública-SEJUSP	Cellebrite/Techbiz Forense Digital	UFED, UFED Touch
Amapá	Ministério Público Estadual	Cellebrite/Techbiz Forense Digital	UFED Cloud, UFED Touch e UFED Analyzer
Roraima	Ministério Público Estadual, Procuradoria de Justiça do Estado de Roraima	Cellebrite/Techbiz Forense Digital	UFED 4PC, UFED Cloud
Tocantins	Núcleo Especializado de Computação Forense do Instituto de Criminalistica, Procuradoria Geral de Justiça	Cellebrite/Techbiz Forense Digital	UFED, UFED Touch
Bahia	Ministério Público Estadual, SEAP	Cellebrite/Techbiz Forense Digital	UFED 4PC, UFED Cloud, UFED Pathfinder
Ceará	Secretaria da Segurança Pública e Defesa Social	Cellebrite/Techbiz Forense Digital	UFED Cloud, UFED 4PC, Cellebrite Advanced Services e UFED Analyzer
Maranhão	Polícia Civil	Cellebrite/Techbiz Forense Digital	UFED
Paraíba	Núcleo de Criminalística de João Pessoa e de Campina Grande, Polícia Militar	Cellebrite/Techbiz Forense Digital	Cellebrite Physical Analyser
Piauí	Ministério Público Estadual, Secretaria de Segurança Pública	Cellebrite/Techbiz Forense Digital	UFED 4PC
Rio Grande do Norte	Ministério ‘Público Estadual	Cellebrite/Techbiz Forense Digital	UFED 4PC, UFED Touch
Sergipe	Secretaria de Estado de Segurança Pública	Cellebrite/Techbiz Forense Digital	UFED
Minas Gerais	Polícia Civil / Polícia Militar, Secretaria de Estado da Fazenda, Secretaria de Estado de Justiça e Segurança	Cellebrite/Techbiz Forense Digital	UFED Cloud, UFED 4PC, UFED Touch e UFED Analytics
Rio de Janeiro	Ministério Público Estadual, Polícia Civil	Cellebrite/Techbiz Forense Digital	UFED 4PC, UFED Touch e UFED Analytics
Distrito Federal	Perícias de Informática do Instituto de Criminalistica-PCDF	Cellebrite/Techbiz Forense Digital	UFED Touch
Goiás	Superintendência da Polícia Técnico Científica-SPTC	Cellebrite/Techbiz Forense Digital	UFED Ultimate
Mato Grosso	Ministério Público Estadual, Procuradoria Geral de Justiça, Secretaria de Estado de Segurança Pública	Cellebrite/Techbiz Forense Digital	UFED Cloud, UFED Premium, UFED Pathfinder, UFED Touch, UFED 4PC
Mato Grosso do Sul	Fundo Estadual de Segurança Pública, Ministério Público Estadual	Cellebrite/Techbiz Forense Digital	UFED Cloud, UFED Premium, UFED Pathfinder, UFED Touch, UFED 4PC
Paraná	Departamento de Polícia Civil-DPC-SESP, Instituto de Criminalística-IC SESP	Cellebrite/Techbiz Forense Digital	UFED Cloud, UFED Premium, UFED Pathfinder, UFED Touch, UFED 4PC, Cellebrite Advanded Services
Santa Catarina	Ministério Público Estadual, Secretaria de Estado de Segurança Pública-Polícia Civil	Cellebrite/Techbiz Forense Digital	UFED Cloud, UFED Premium, UFED Pathfinder, UFED Touch, Cellebrite Advanded Services
Rio Grande do Sul	Ministério Público Estadual, Secretaria de Estado de Segurança Pública-Polícia Civil	Cellebrite/Techbiz Forense Digital	UFED Cloud, UFED Premium, UFED Pathfinder, UFED Touch, UFED Analytics, UFED 4PC

Fonte: A autora

lebrite UFED) por agências governamentais no Brasil, permite concluir que as técnicas de extração de dados já compõem o *modus operandi* das agências investigativas em praticamente todos os Estados brasileiros, incluindo Distrito Federal e entidades do Governo Federal.

4.2.3 Caso de Uso - Operação Guardião Digital

Trata-se de uma operação deflagrada em julho de 2024 e coordenada pela Diretoria Estadual de Combate a Crimes Cibernéticos (DECCC) da Polícia Civil do Pará com o apoio da Polícia Civil de São Paulo, tendo como foco o combate a crimes cibernéticos, e.g., golpe em plataforma digitais de vendas, invasões de contas de redes sociais, clonagem de WhatsApp, tabela PIX, falsos leilões de veículos e crimes contra vulneráveis, incluindo pornografia infantil e *cyberbulling*. O processo de perícia digital englobou pesquisa, coleta, extração, processamento e análise dos dados nos dispositivos apreendidos. Para tanto, utilizou-se a ferramenta Cellebrite UFED, permitindo a duplicação precisa dos dados, sem alteração no conteúdo original, preservando a integridade dos arquivos e garantindo a manutenção da cadeia de custódia durante todo o processo investigativo. Nos celulares foram feitas extrações de sistema de arquivos e/ou extrações físicas. A integridade e a observância da cadeia de custódia permitiram a validação das provas em Juízo, ou seja, a relatoria e documentação precisa de todas as etapas de manipulação das provas, desde a apreensão, passando pelo acondicionamento e lacre dos objetos apreendidos, até o deslacre, extração e análise. O resultado foi a extração de mais de 3 terabytes de dados de informações que geraram mais de 40 evidências digitais incorporadas aos processos judiciais (MACIEL, 2024).

4.3 ANÁLISE SOB PERSPECTIVA DA LEGISLAÇÃO

Percebe-se ao longo da última década, que a questão relacionada à utilização de ferramentas de *hacking* pelas agências dos governos e de investigação, tornou-se amplamente discutida a nível internacional, com vistas ao combate do crime organizado e terrorismo.

Na UE, a Diretiva 2016/680/UE estabeleceu um regime geral de proteção de dados pessoais no âmbito de investigações criminais, consolidando diretrizes e princípios de legalidade, necessidade e proporcionalidade no uso de métodos que envolvem o processamento de dados pessoais e técnicas de *hacking* por agências investigativas, estabelecendo um quadro abrangente para garantir um elevado nível de proteção de dados, tendo em conta a natureza específica do setor policial e da justiça penal. Esta Diretiva faz parte da reforma da proteção de dados da UE, juntamente com o GDPR e o Regulamento 2018/1725/UE relativo à proteção de pessoas singulares no

que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos, gabinetes e agências da UE, harmonizando a proteção de dados pessoais pelas autoridades policiais nos Estados Membros da UE e nos países do Espaço Schengen (EUR-LEX, 2022).

Nesse cenário, ressalta-se o debate sobre direitos humanos, vigilância das comunicações privadas, proteção de dados pessoais, criptografia como meio de garantia do direito à privacidade, cadeia de custódia de vestígios digitais, práticas de HL e *Fishing Expedition* no âmbito das investigações criminais pelo poder público. Assim, as ferramentas de *hacking* se apresentam, no contexto em que as instituições de segurança pública e persecução penal reagem aos impedimentos, obstáculos, entraves ou obscurecimentos (*going dark*) nas investigações contra criminosos em ambientes cibernéticos, como uma forma e/ou alternativa pelo poder público, de se realizar investigações criminais, promovendo a extração de dados digitais e explorando vulnerabilidades em bancos de dados, programas de computador, sistemas computacionais, redes de comunicação ou dispositivos eletrônicos, operando tanto via de acesso remoto quanto via de acesso físico em dispositivo de armazenamento.

Não se pode fugir aos olhos a existência de uma indústria, em crescimento, cujo modelo de negócio é integralmente baseado na extração de dados digitais e na exploração de vulnerabilidade de segurança em dispositivos digitais (e.g., Cellbrite e NSO Group) (RODRIGUES, 2021).

No Brasil, as técnicas de extração de dados já compõem o *modus operandi* das agências investigativas (e.g., Polícia Civil, Ministérios Públicos, Polícia Militar dos Estados, Ministério da Defesa). O emprego da tecnologia da Cellebrite em inquéritos e operação de investigação nacionais é uma realidade. Portanto, inexiste uma legislação processual penal que discipline a matéria de forma robusta no país.

O Marco Civil da Internet, por sua vez, estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil e promoveu o uso de medidas técnicas compatíveis com padrões internacionais e estímulo ao uso de boas práticas para a preservação da estabilidade, segurança e funcionalidade da rede, além da proteção da privacidade e dos dados pessoais, na forma da lei (Art. 3º) (BRASIL, 2014a). Nesta esteira, o "Pacote Anticrime"promulgado na forma da Lei nº 13.964/2016 (BRASIL, 2019) apresentou de maneira formal e legal a definição de cadeia de custódia e o reconhecimento de sua relevância.

A LGPD (BRASIL, 2018) versou sobre a adoção de padrões técnicos adequados para garantir a segurança e salvaguarda de dados pessoais que estiverem sob a tutela de agentes de tratamento. Porém, expressamente, excluiu do seu campo de aplicação a proteção de dados no âmbito das investigações criminais e as persecu-

ções penais e segurança pública, prevendo legislação específica, ainda não editada, mas cujo projeto tem sido chamado de LGPD Penal.

Assim, o desafio que se apresenta é o de se estabelecer um equilíbrio, dentro da ordem constitucional, entre o emprego das ferramentas de *hacking* em associação com as práticas do HL e *Fishing Expedition*, a cadeia de custódia e a restrição a direitos fundamentais e garantias processuais que delas decorrem.

4.4 CONSIDERAÇÕES DO CAPÍTULO

Neste capítulo foram apresentadas as ferramentas de acesso remoto a dados de comunicação pessoal, bem como as ferramentas utilizadas pela perícia digital e órgãos de investigação no processo de extração de dados em vestígios digitais, com destaque ao sistema Cellebrite UFED, por ser uma ferramenta de extração de dados de dispositivos móveis amplamente utilizada em investigações criminais no Brasil.

5 CONSIDERAÇÕES FINAIS

Ao passo em que ocorre o avanço de protocolos de segurança desenvolvidos pela comunidade tecnológica, um movimento de contramão fomenta a exploração de vulnerabilidades nesses mesmos sistemas por instituições governamentais, que pode envolver tecnologia produzida pelo próprio governo ou ferramentas vendidas pro empresas (e.g., NSO Group e Cellebrite).

O presente trabalho visa evidenciar a aplicação e repercussões das práticas do HL e FE dentro de um contexto de global de vigilância e investigação operada por setores governamentais, muitas vezes à revelia de ordens judiciais, e em (in)observância da cadeia de custódia, com a utilização de *spywares* e ferramentas de extração massiva de dados de dispositivos pessoais.

Neste contexto de ampla diversidade de ferramentas de coleta e monitoramento de dados, inclusive em tempo real, as contraposições ao seu uso se fundam nos riscos à privacidade e à proteção dos dados pessoais dos cidadãos, em observância ao princípios norteadores do GDPR e da LGPD, não obstante a ausência de regras legais específicas.

O estudo abordou o arcabouço legal brasileiro e europeu com foco na LGPD e GDPR, destacando a importância da cadeia de custódia para garantir a integridade da prova digital obtidas através das ferramentas de *hacking.*

Assim, na problematização dos aspectos legais, envolvendo a proteção dos dados pessoais e centrada na cadeia de custódia, a questão envolve saber se a utilização dessas ferramentas por instituições de segurança pública e de polícia científica pode criar um ambiente de controle irrestrito e não mapeável e quais devem ser os limites legais para captura e análise de dados, de forma a utilizar as práticas do HL e FE, sem comprometer a proteção da privacidade e dos dados pessoais.

Importante fator que contribuiu para o atingimento do objetivo deste trabalho foram as informações obtidas através da pesquisa exploratória realizada junto a Polícia Científica de Santa Catarina em Joinville que possibilitou maior compreensão do processo de cadeia de custódia da prova digital e das ferramentas de extração de dados por eles utilizadas.

A maior dificuldade encontrada por esta autora diz respeito à pesquisa bibliográfica pelo fato das literaturas referentes às práticas do HL e do FE estarem dispostas separadamente ou só na parte do Direito, muitas vezes em *blogs* e sítio jurídicos ou, então, na área de cibersegurança.

Portanto, pode-se dizer que a maior contribuição deste trabalho é a sintetização e agrupamento dos conceitos objeto desta pesquisa, sendo um instrumento de consulta, de forma a proporcionar um debate sobre o uso das práticas do HL e FE, de tecnologias e de ferramentas de *hacking* para fins de investigação criminal e segurança nacional, nos tribunais pátrios e internacionais.

Espera-se que este estudo possa contribuir como insumo ao debate público e como material que auxilie formuladores de políticas públicas e operadores do direito. O fenômeno do HL e FE é um desafio premente que deve ser tratado como prioridade e de interesse público. No que pese as técnicas de extração e acesso a dados em dispositivos pessoais serem fundamentais para a condução de atividades de segurança pública e investigação, os riscos colocados e inerentes devem ser antecipados em avaliações de impacto aos direitos e à segurança tanto de indivíduos investigados quanto da sociedade de forma ampla.

5.1 PRODUÇÕES

Durante o desenvolvimento deste trabalho foi realizada a seguinte publicação:

- SANTOS, Juliana de Paula; MIERS, Charles Christian. Hacking Legal e Fishing Expedition: uma análise das práticas sob perspectivas das legislações do Brasil e Europa. In: ESCOLA REGIONAL DE REDES DE COMPUTADORES (ERRC), 20. , 2023, Porto Alegre/RS. Anais da XX Escola Regional de Redes de Computadores. Porto Alegre: Sociedade Brasileira de Computação, 2023 . p. 103-108. DOI: https://doi.org/10.5753/errc.2023.883.

5.2 TRABALHOS FUTUROS

Como trabalho futuro sugere-se um estudo mais aprofundado das ferramentas de *hacking* utilizadas pelas polícias científicas no Brasil, apresentando uma análise de risco quanto às técnicas de extração de dados de forma a colaborar para a eficácia investigativa, processual e da jurisdição na esfera criminal.

Sendo assim, a recomendação para o futuro seria encontrar um equilíbrio entre a utilização das práticas doHL e FE e suas ferramentas, centrado na cadeia de custódia, e em observância aos fundamentos legais de privacidade e da proteção de dados pessoais com base na GDPR e LGPD.

5.3 SUPORTE

Este trabalho recebeu apoio da FAPESC e LabP2D/UDESC. Este trabalho recebeu apoio financeiro da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES (PROAP/AUXPE).

REFERÊNCIAS

ACCESSDATA. **Imager User Guide**. 2021. Disponível em: <https://d1kpmuwb7gvu1i.cloudfront.net/Imager/4_7_1/FTKImager_UserGuide.pdf>.

AMARAL, P. et al. Mercadores da insegurança: conjuntura e riscos do hacking governamental no brasil. **Instituto de Pesquisa em Direito e Tecnologia do Recife**, 2022. Disponível em: <https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf>.

ANTIS, S. Government procurement law and hacking technology: The role of public contracting in regulating an invisible market. **Computer Law & Security Review**, v. 41, p. 105536, 2021. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364921000091>.

ARABI, A. Y. M. UtilizaÇÃo de dados pessoais no combate ao crime organizado: Limites e possibilidades de tÉcnicas especiais de investigaÇÃo em meio digital. In: REVISTA JUDICIAL BRASILEIRA-REJUB. [S.l.], 2022. v. 2.

AUTOPSY. 2025. Disponível em: <https://www.autopsy.com/>.

AZEVEDO, C. P. G. e. a. Nota técnica: análise comparativa entre o anteprojeto de lgpd penal e o pl 1515/2022. In: INSTITUTIO DE REFERêNCIA EM INTERNET E SOCIEDADE (IRIS) E LABORATóRIO DE POLíTICAS PúBLICAS E INTERNET (LAPIN). 2022. Disponível em: <https://lapin.org.br/wp-content/uploads/2022/11/Nota-tecnica-Analise-comparativa-entre-o-anteprojeto-de-LGPD-Penal-e-o-PL-15152022-1.pdf>.

BANDEIRA, S. d. O. **A ilegalidade da pesca predatória por provas ("fishing expedition") nos mandados de busca e apreensão genéricos**. Dissertação (TCC) — Universidade Federal Rural do Semiárido, Mossoró, Brasil, 2020. Disponível em: <https://repositorio.ufersa.edu.br/handle/prefix/6317>.

BELLOVIN, S. M. The law and lawful hacking. **IEEE Security & Privacy**, IEEE Computer Society, Los Alamitos, CA, USA, v. 19, n. 04, p. 76–76, jul 2021. ISSN 1558-4046.

BELLOVIN, S. M. et al. Lawful hacking: Using existing vulnerabilities for wiretapping on the internet. **Nw. J. Tech. & Intell. Prop.**, v. 12, n. 1, 2014. Disponível em: <https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1>.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. código de defesa do consumidor. In: PLANALTO. 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. lei de interceptação telefônica e telemática. In: PLANALTO. 1996. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9296.htm>.

BRASIL. Lei complementar nº 105, de 10 de janeiro de 2001. lei do sigilo bancário. In: PLANALTO. 2001. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm>.

BRASIL. Lei nº 12.414, de 9 de junho de 2011. lei do cadastro positivo. In: PLANALTO. 2011. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. lei de crimes cibernéticos ou lei carolina dieckmann. In: PLANALTO. 2012. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. marco civil da internet. In: PLANALTO. 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

BRASIL. Portaria senasp nº 82, de 16 de julho de 2014. In: DIáRIO DAS LEIS. 2014. Disponível em: <https://www.diariodasleis.com.br/legislacao/federal/227818-cadeia-de-custudia-de-vestugios-estabelece-as-diretrizes-sobre-os-procedimentos-a-serem-observados-no-tocante-u-cadeia-de-custudia-de-vestugios.html>.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. lei geral de proteção de dados (lgpd). In: PLANALTO. [S.l.]: https://www.planalto.gov.br/ccivil$_0 3/_a to 2015 - 2018/2018/lei/l13709.htm, 2018.$

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. pacote anticrime. In: PLANALTO. 2019. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm>.

BRASIL. Anteprojeto de lei de proteção de dados pessoais para segurança pública e persecução penal. In: CâMARA LEGISLATIVA. 2020. Disponível em: <https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf>.

BRASIL. Resolução cnj nº 362/2020. In: CONSELHO NACIONAL DE JUSTIçA-CNJ. 2020. Disponível em: <https://www.stj.jus.br/internet_docs/biblioteca/clippinglegislacao/Res_362_2020_CNJ.pdf>.

BRASIL. **IGP entrega novos equipametos com tecnologia avançada de informática forense**. 2021. Disponível em: <https://estado.sc.gov.br/noticias/igp-entrega-novos-equipamentos-com-tecnologia-avancada-de-informatica-forense/>.

BRASIL. Portaria cnj nº 162/2021. In: CONSELHO NACIONAL DE JUSTIçA-CNJ. 2021. Disponível em: <https://atos.cnj.jus.br/files/compilado140230202106146 0c7617672ec5.pdf>.

BRASIL. Projeto de lei nº 1515/2022. In: CâMARA LEGISLATIVA. 2022. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274&filename=PL%201515/2022>.

BRASIL. **O que é o FirstMile, software que teria sido usado pela Abin para monitorar jornalistas e ministros do STF**. 2023. Disponível em: <https://www.bbc.com/portuguese/articles/c3g32mz1dzdo>.

CANI, L. E.; ROSA, A. M. D. Investida européia contra a criptografia dos e-mails e a pescaria probatória. **Conjur**, 2021. Disponível em: <https://www.conjur.com.br/2021-fev-19/limite-penal-investida-europeia-criptografia-mails-pescaria-probatoria/>.

CATARINA/SC, P. da Polícia Científica de S. **Entrevista realizada**. 2024.

CELLEBRITE. **Cellebrite Advanced Services**. 2025. Disponível em: <https://cellebrite.com/pt/servicos-avancados/#cas_form_m>.

CELLEBRITE. **File System Extraction Forensics**. 2025. Disponível em: <https://cellebrite.com/en/glossary/file-system-extraction-forensics/>.

CELLEBRITE. **Modo EDL - Modo de dowload de emergência - Perícia forense de dispositivos móveis**. 2025. Disponível em: <https://cellebrite-com.translate.goog/en/glossary/edl-mode-emergency-download-mode-mobile-device-forensics/?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt&_x_tr_pto=tc&_x_tr_hist=true>.

CELLEBRITE. **Product Overview | Cellebrite UFED**. 2025. Disponível em: <https://cellebrite.com/wp-content/uploads/2020/06/ProductOverview_Cellebrite_UFED_A4.pdf>.

CRUZ, C. **Innovate Learning in a Digital Forensics Laboratory:Tools and Techniques for Data Recovery**. 2017. 25 p.

DUTRA, L. C. d. M. et al. Hacking governamental uma resisão sistemática. In: IRIS INSTITUTO DE REFERêNCIA EM INTERNET E SOCIEDADE. 2023. Disponível em: <https://irisbh.com.br/wp-content/uploads/2023/02/Hacking-Governamental-uma-revisao-sistematica-IRIS.pdf>.

ELCI, A. **O que significa uma lei de vigilância dos EUA para a privacidade dos dados europeus**. 2024. Disponível em: <https://pt.euronews.com/next/2024/06/01/o-que-significa-uma-lei-de-vigilancia-dos-eua-para-a-privacidade-dos-dados-europeus>.

ERICKSON, A. Comparative analysis of the eu's gdpr and brazil's lgpd: Enforcement challenges with the lgpd. In: **Brooklyn Journal of International Law**. [s.n.], 2019. v. 44. Disponível em: <https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/9>.

EU. Gdpr.eu. In: EUROPEAN PARLIAMENT. **Official Journal of the European Union**. 2016. v. 44, p. 88. Disponível em: <https://gdpr.eu/tag/gdpr/>.

EU. Manual da legislação europeia sobre proteção de dados. In: AGENCIA DOS DIREITOS FUNDAMENTAIS DA UNIãO EUROPEIA E CONSELHO DA EUROPA. 2018. Disponível em: <http://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_pt.pdf>.

EUR-LEX. **Protecting personal data that is used by police and criminal justice authorities (from 2018)**. 2022. Disponível em: <https://eur-lex.europa.eu/EN/legal-content/summary/protecting-personal-data-that-is-used-by-police-and-criminal-justice-authorities-from-2018.html>.

FERREIRA, C. P. Hacking e infiltração policiais em resposta ao uso de criptografia por organizações criminosas. **Revista Brasileira de Ciências Policiais**, v. 12, n. 5, p. 19–48, maio 2021. Disponível em: <https://periodicos.pf.gov.br/index.php/RBCP/article/view/837>.

FERREIRA, D. A. A.; PINHEIRO, M. M. K.; MARQUES, R. M. Privacidade e proteção de dados pessoais: perspectiva histórica. **InCID: Revista de Ciência da Informação e Documentação**, v. 12, n. 2, p. 151–172, nov. 2021. Disponível em: <https://www.revistas.usp.br/incid/article/view/179778>.

FILHO, O. B. P. Investigação criminal tecnológica - a infiltração por malware nas investigações informáticas. In: FACULDADE DE DIREITO DA UNIVERSIDADE NOVA DE LISBOA. [S.l.], 2020.

GIARDINI, F. Malware estatal na investigação criminal. In: ESMPU. **Técnicas Avançadas de Investigação. Perspectivas pática e jurisprudencial**. 2022. v. 2, p. 63. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Tecnicas-avancadas-de-investigacao-v.2.pdf>.

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 4ª edição. ed. São Paulo/Brasil: [s.n.], 2002. Disponível em: <https://files.cercomp.ufg.br/weby/up/150/o/Anexo_C1_como_elaborar_projeto_de_pesquisa_-_antonio_carlos_gil.pdf>.

HENNESSEY, S. Lawful hacking and the case for a strategic approach to “going dark”. In: **Brookings**. [s.n.], 2016. Disponível em: <https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/>.

HERPIG, S. A framework for government hacking in criminal investigations. **Stiftung Neue Verantwortung**, 2021. Disponível em: <https://www.stiftung-nv.de/sites/default/files/framework_for_government_hacking_in_criminal_investigations.pdf>.

HOLPERIN, M.; LEOBONS, R. **Análise Forense**. 2025. Disponível em: <https://www.gta.ufrj.br/grad/07_1/forense/bibliografia.html>.

INTERNATIONAL, O. **EnCase Forensic software: características e funções**. 2025. Disponível em: <https://www.ondata-pt.com/recuperacao-dados/encase-forensic-2.htm>.

INTERNATIONAL, P. **A Technical look at Phone Extraction**. 2019. Disponível em: <https://privacyinternational.org/long-read/3256/technical-look-phone-extraction>.

IPED Digital Forensics. 2025. Disponível em: <https://github.com/sepinf-inc/IPED>.

KASPERSKY. Spyware: what it is and how to pretect yourself. In: . 2025. Disponível em: <https://www.kaspersky.com/resource-center/threats/spyware>.

KITCHENHAM, B.; CHARTERS, S. Guidelines for performing systematic literature reviews in software engineering. In: TECHNICAL REPORT EBSE. 2007. Disponível em: <https://legacyfileshare.elsevier.com/promis_misc/525444systematicreviewsguide.pdf>.

KOLOCHENKO, I. **Framework Proposal to Regulate Lawful Hacking by Police within Criminal Investigations**. Dissertação (Dissertação) — Capitol Tecnology University, 2022. Disponível em: <https://www.proquest.com/openview/7958f45bc813e48c2f831e26c97c26f3/1?pq-origsite=gscholar&cbl=18750&diss=y>.

LEVY, Y.; ELLIS, T. J. A system approach to conduct an effective literature review in support of information systems research. In: INFORMING SCIENCE JOURNAL. [S.l.], 2006. v. 9, p. 181–212.

LI, C.-Y. et al. A comprehensive overview of government hacking worldwide. **IEEE Access**, v. 6, p. 55053–55073, 2018.

LIGER, Q.; GUTHEIL, M. **The use of Pegasus and equivalent surveillance spyware**. 2023. Disponível em: <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf>.

LIGUORI, C. Exploring lawful hacking as a possible answer to the "going dark"debate. In: **Mich. Tech. L.** [S.l.: s.n.], 2020.

MACIEL, I. **Caso de uso: Ferramentas Digitais na Operação Guardião Digital**. 2024. Disponível em: <https://www.techbiz.com.br/caso-de-uso-ferramentas-digitais-na-operacao-guardiao-digital>.

MAGNET FORENSICS. **Axiom**. 2025. Disponível em: <https://www.magnetforensics.com/products/magnet-axiom/>.

MAHMOOD, S. Phishing vs. fishing: What's the difference and how to stay safe? In: NEXTDOORSEC. 2023. Disponível em: <https://nextdoorsec.com/phishing-vs-fishing/>.

MALDONADO, V. N.; BLUM, R. O. **LGPD Lei Geral de Proteção de Dados Gerais Comentada**. 3ª edição. ed. São Paulo/Brasil: Revista dos Tribunais, 2021. ISBN 978-6556144375.

MALINDA, T. W. Advancements in mobile forensics: A comprehensive analysis of cellebrite ufed. In: RESEARCHGATE. [S.l.], 2024.

MAYER, J. Government hacking. In: **The Yale Law Journal**. [s.n.], 2018. v. 3. Disponível em: <https://www.yalelawjournal.org/pdf/Mayer_k3iy4nv8.pdf>.

MOTORYN, P. **Hacking de governo**. 2023. Disponível em: <https://www.intercept.com.br/2023/04/19/abin-comprou-programa-que-pode-espionar-internet/>.

MPPR. **Operação Publicano**. 2015. Disponível em: <https://mppr.mp.br/Comunicacao/Pagina/Operacao-Publicano>.

NETO, M. F.; SANTOS, J. E. L. D. A lgpd. In: UNIVEM. **Revista em tempo**. 2020. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3130>.

NEVES, R. d. A. **GDPR e LGPD: Estudo comparativo**. Dissertação (TCC) — Centro Universitário de Brasília, Brasília, Brasil, 2021. Disponível em: <https://repositorio.uniceub.br/jspui/handle/prefix/15239>.

OLIVEIRA, V. M. d. Iso 27037 identificação, coleta, aquisição e preservação de evidência. In: ACADEMIA DE FORENSE DIGITAL. 2021. Disponível em: <https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicao-e-preservacao-de-evidencia/#8230>.

ONRETRIEVAL GROUP. **Passware**. 2025. Disponível em: <https://onretrieval.pt/hardware/passware/>.

ONU. Declaração universão dos direitos humanos (dudh). In: . 1948. Disponível em: <https://www.oas.org/dil/port/1948%20Declara%C3%A7%C3%A3o%20Universal%20dos%20Direitos%20Humanos.pdf>.

OPENCARNIVORE.ORG. **Carnivore Software Official Website**. 2025. Disponível em: <https://web.archive.org/web/20130714015134/http://opencarnivore.org/>.

PARLAMENTO EUROPEU. **Recomendação do Parlamento Europeu ao Conselho e à Comissão, de 15 de junho de 2023, na sequência da investigação de alegadas contravenções e má administração na aplicação do Direito da União relacionadas com a utilização do software espião de vigilância Pegasus e equivalentes (2023/2500(RSP)**. 2023. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:C_202400494>.

PASSWARE. **Passware Kit Forensic**. 2025. Disponível em: <https://www.passware.com/kit-forensic/>.

PASTORE, A. M.; FONSECA, M. A. C. Cadeia de custódia de provas digitais nos processos do direito administrativo sancionador com a adoção da tecnologia blockchain. In: REVISTA CGU. **Cadernos Técnicos da CGU**. 2022. Disponível em: <https://revista.cgu.gov.br/Cadernos_CGU/article/view/597>.

PATEL, B.; MANN, P. S. M. A survey on mobile digital forensic: Taxonomy, tools, and challenges. In: ACM DIGITAL LIBRARY. [S.l.], 2024.

PAULINO, G. d. C. et al. **Técnicas avançadas de investigação**. 2ª edição. ed. Brasília/Brasil: https://escola.mpu.mp.br/publicacoes/obras-avulsas/e-books-esmpu/tecnicas-avancadas-de-investigacao-2013-perspectivas-pratica-e-jurisprudencial-vol-1, 2021. ISBN 978-65-88299-92-0.

PEGG, D.; CUTLER, S. **What is Pegasus spyware and how does it hack phones?** 2021. Disponível em: <https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones>.

PEREIRA, A. B. G.; RODRIGUES, G. R.; VIEIRA, V. B. R. **Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise**. Dissertação — Instituto de Referência em Internet e Sociedade, Belo Horizonte, Brasil, 2021. Disponível em: <https://bit.ly/3kGTde3>.

PINHEIRO, P. P. **Proteção de Dados Pessoais Comentários à Lei n. 13.709/2018 LGPD**. 1ª edição. ed. São Paulo/Brasil: Saraiva Educação, 2018. ISBN 978-85-536-0831-7.

PINHEIRO, W. **Sistema IPED: conheça as principais funcionalidades do software utilizado na investigação da Operação Lava Jato**. 2025. Disponível em: <https://blog.ipog.edu.br/tecnologia/sistema-iped-software-usado-pela-policia-federal/>.

POSTON, H. **Digital Forensics: Popular computer forensics top 19 tools [updated 2021]**. 2021. Disponível em: <https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-tools/>.

(PPSI), P. de Privacidade e Segurança da I. Guia de requisitos e obrigações quanto à privacidade e à segurança da informação. In: MINISTéRO DA GESTãO E DA INOVAçãO EM SERVIçOS PúBLICOS. 2024. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_requisitos_obrigacoes.pdf>.

PRADO, G. L. M. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital. In: . [s.n.], 2021. Disponível em: <https://geraldoprado.com.br/artigos/breves-notas-sobre-o-fundamento-constitucional-da-cadeia-de-custodia-da-prova-digital/>.

PRASHI, J.; AMARNATH. Extraction of data using cellebrite ufed 4pc. In: INTERNATIONAL JOURNAL OF MEDICAL TOXICOLOGY & LEGAL MEDICINE. [S.l.], 2023. v. 26, p. 222–232.

PRIVACY INTERNATIONAL. **A Technical look at Phone Extration**. 2019. Disponível em: <https://privacyinternational.org/sites/default/files/2019-10/A%20technical%20look%20at%20Phone%20Extraction%20FINAL.pdf>.

QUINLAN, S.; WILSON, A. **A brief history of law enforcement hacking in the United States**. 2016. Disponível em: <https://na-production.s3.amazonaws.com/documents/History_Hacking.pdf>.

RAMIRO ANDRé ANDE AMARAL, P.; CANTO, M.; PEREIRA MARCOS CéSAR M., P. **Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil**. 2022. Disponível em: <https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/>.

RODRIGUES, G. **Hacking governamental e a indústria da insegurança digital**. 2021. Disponível em: <https://irisbh.com.br/hacking-governamental-e-a-industria-da-inseguranca-digital/>.

ROSA, A. M. D. A prática de fishing expedition no processo penal. **Conjur**, 2021. Disponível em: <https://www.conjur.com.br/2021-jul-02/limite-penal-pratica-fishing-expedition-processo-penal/>.

SAAD, M. Editorial: Investigação criminal e novas tecnologias para obtenção de prova. **Revista Brasileira de Ciências Policiais**, v. 12, n. 5, p. 11–16, maio 2021. Disponível em: <https://periodicos.pf.gov.br/index.php/RBCP/article/view/856>.

SCHMITZ, K. F. T.; MELO, J. E. B. d.; CARDOSO, V. **O uso da informática na perícia criminal e suas ferramentas**. 2017. 25 p. Disponível em: <https://www.revistaespacios.com/a17v38n51/17385125.html>.

SERPRO. A lgpd. In: SERVIçO FEDERAL DE PROCESSAMENTO DE DADOS. 2023. Disponível em: <https://www.serpro.gov.br/lgpd/>.

SHIMABUKURO, A. Cibercrime: quando a tecnologia é aliada da lei. In: ESCOLA DE MAGISTRADOS DA JUSTIçA DA 3ª REGIãO-EMAG TRF3. **Investigação e prova nos crimes cibernéticos**. 2017. Caderno de Estudos 1, p. 17–31. Disponível em: <https://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf>.

SILVA, P. B. Melo e. A pesca predatória por provas por parte dos órgãos de investigação. In: **Empório do Direito**. [s.n.], 2017. Disponível em: <https://emporiododireito.com.br/leitura/fishing-expedition-a-pesca-predatoria-por-provas-por-parte-dos-orgaos-de-investigacao>.

SILVA, R. L. d.; SILVA, D. L. d. **A Extração de dados de dispositivos móveis na investigação criminal e a utilização do contéudo extraído**. 2020. Disponível em: <https://editora.pucrs.br/edipucrs/acessolivre/anais/congresso-internacional-de-ciencias-criminais/assets/edicoes/2020/arquivos/64.pdf>.

SILVA, V. G. d. **A ocorrência da fishing expedition e do encontro fortuito na busca e apreensão**. Dissertação (TCC) — Universidade Federal de Santa Catarina-UFSC, Florianópolis, Brasil, 2018. Disponível em: <https://repositorio.ufsc.br/handle/123456789/188018>.

SILVA, V. G. D.; SILVA, P. B. Melo e; ROSA, A. M. D. **Fishing Expedition e encontro fortuito na busca e na apreensão - um dilema oculto no processo penal**. 2ª edição. ed. Florianópolis/Brasil: Editora Emais, 2022. ISBN 978-65-86439-99-3.

STF. Arguição de descumprimento de preceito fundamental 403. In: STF. 2020. Disponível em: <https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf>.

STJ. O encontro fortuito de provas na jurisprudência do stj. In: SECRETARIA DE COMUNICAçãO SOCIAL DO STJ. 2015. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2015/2015-04-26_08-00_O-encontro-fortuito-de-provas-na-jurisprudencia-do-STJ.aspx>.

STJ. **Terceira Seção rejeita recurso da Google contra fornecimento de dados no caso Marielle Franco**. 2020. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/26082020-Terceira-Secao-rejeita-recurso-da-Google-contra-fornecimento-de-dados-no-caso-Marielle-Franco.aspx>.

STJ. **RMS62562/MT, Relator ministro Jesuíno Rissato, jul. 07/12/2021, pub. 13/12/2021**. 2021. Disponível em: <https://www.conjur.com.br/wp-content/uploads/2023/09/stj-pesca-probatoria.pdf>.

STJ. Hc 663055/mt, relator ministro rogério schietti cruz, sexta turma, julgado em 22/03/2022, dje de 31/03/2022. In: **RSTJ**. [s.n.], 2022. v. 265, p. 986. Disponível em: <https://scon.stj.jus.br/SCON/pesquisar.jsp?preConsultaPP=&pesquisaAmigavel=+%3Cb%3EHC+663.055%3C%2Fb%3E&acao=pesquisar&novaConsulta=true&i=1&b=ACOR&livre=HC+663.055&filtroPorOrgao=&filtroPorMinistro=&filtroPorNota=&data=&operador=e&thesaurus=JURIDICO&p=true&tp=P&processo=&classe=&uf=&relator=&dtpb=&dtpb1=&dtpb2=&dtde=&dtde1=&dtde2=&orgao=&ementa=&nota=&ref=>.

STJ. **RHC 158.580/BA, Relator ministro Rogério Schietti Cruz, jul. 19/04/2022, pub. 25/04/2022**. 2022. Disponível em: <https://processo.stj.jus.br/processo/pesquisa/?termo=rhc158580&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&chkordem=DESC&chkMorto=MORTO>.

STJ. Agrg no rhc n. 143.169/rj, relator ministro messod azulay neto, relator para acórdão ministro ribeiro dantas, quinta turma, julgado em 7/2/2023, dje de 2/3/2023. In: . [s.n.], 2023. Disponível em: <https://processo.stj.jus.br/SCON/pesquisar.jsp>.

STJ. Caiu na rede: é fishing expedition ou serendipidade? In: SECRETARIA DE COMUNICAçãO SOCIAL DO STJ. 2023. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/22102023-Caiu-na-rede-e-fishing-expedition-ou-serendipidade.aspx>.

TAMMAY, R.; MAURíCIO, T. **Provas no Direito Digita: conceito da prova digital, procedimentos e provas em espécie**. São Paulo/Brasil: Thomsom Reuters-Revista dos Tribunais, 2020. ISBN 3.

TST, T. S. do T. A lgpd. In: SECRETARIA DE COMUNICAçãO SOCIAIL DO TRIBUNAL SUPERIOR DO TRABALHO. 2021. Disponível em: <https://www.tst.jus.br/provas-digitais>.

UE. Diretiva (ue) 2016/680. In: PARLAMENTO EUROPEU. **EUR-Lex**. 2016. Disponível em: <http://data.europa.eu/eli/dir/2016/680/oj>.

UE. Proteção de dados pessoais. In: **Fichas técnicas sobre a União Europeia**. [s.n.], 2023. Disponível em: <https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf>.

VELD, S. i. t. **Relatório sobre a investigação de alegadas contravenções ou má administração na aplicação do Direito da União relacionadas com a utilização do software espião de vigilância Pegasus e equivalentes**. 2023. Disponível em: <https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_PT.html>.

VIEIRA, V. **O caso Anom e o poder investigativo estatal: estamos de fato "Going Dark"?** 2021. Disponível em: <https://irisbh.com.br/o-caso-anom-e-o-poder-investigativo-estatal-estamos-de-fato-going-dark/>.

VILARES, F. R. **A reserva de jurisdição no processo penal: dos reflexos no inquérito parlamentar**. Dissertação (Disseração Mestrado em Direito) — Universidade de São Paulo, São Paulo, Brasil, 2010. Disponível em: <https://www.al.sp.gov.br/alesp/biblioteca-digital/obra/?id=23199>.

VOLATILITY. 2025. Disponível em: <https://github.com/volatilityfoundation/volatility>.

WEISS, F. L. Paralelo entre a lei geral de proteção de dados, o ccpa e o gdpr europeu. In: **Consultor Jurídico**. [s.n.], 2020. Disponível em: <https://www.conjur.com.br/2020-out-28/weiss-paralelo-entre-lgpd-ccpa-gdpr-europeu>.

ŠKORVáNEK, I. et al. "my computer is my castle": New privacy frameworks to regulate police hacking. In: BRIGHAM YOUNG UNIVERSITY. [S.l.]: https://digitalcommons.law.byu.edu/lawreview/vol2019/iss4/7, 2019.

UDESC UNIVERSIDADE DO ESTADO DE SANTA CATARINA | JOINVILLE CENTRO DE CIÊNCIAS TECNOLÓGICAS

UNIVERSIDADE DO ESTADO DE SANTA CATARINA – UDESC
BIBLIOTECA UNIVERSITÁRIA
REPOSITÓRIO INSTITUCIONAL

CENTRO DE CIÊNCIAS TECNOLÓGICAS – CCT

ATESTADO DE VERSÃO FINAL

Eu, Charles Christian Miers, professor do curso de Mestrado em Computação Aplicada, declaro que esta é a versão final aprovada pela comissão julgadora da dissertação/tese intitulada: **"*HACKING LEGAL* E *FISHING EXPEDITION*: UMA ANÁLISE DAS PRÁTICAS SOB PERSPECTIVAS DAS LEGISLAÇÕES DO BRASIL E EUROPA"** de autoria da acadêmica Juliana de Paula Santos.

JOINVILLE, 18 de setembro de 2025.

Assinatura digital do orientador:

gov.br Documento assinado digitalmente
CHARLES CHRISTIAN MIERS
Data: 18/09/2025 20:21:22-0300
Verifique em https://validar.iti.gov.br

Dr. Charles Christian Miers - UDESC