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

Juliana de Paula Santos[1], **Charles Christian Miers**[1]

[1] Programa de Pós-Graduação em Computação Aplicada (PPGCAP)
Universidade do Estado de Santa Catarina (UDESC)

jla01@jfsc.jus.br - charles.miers@udesc.br

Abstract. *Governments are intensifying the practice of collecting cell phones, tablets, and computers in search of helpful information in investigations. Several of these devices employ services running in clouds or remote providers that end up being involved in this procedure. Two of these investigative practices are Legal Hacking and Fishing Expeditions. Our work presents a review and a proposal to analyze the feasibility and implications of Legal Hacking and Fishing Expedition practices to address the needs of police and intelligence agencies. Our proposal moves between legal aspects of the Brazilian legal system and international courts, as well as technological practices for obtaining data.*

Resumo. *Os governos vem intensificando a prática de coletar celulares, tablets e computadores na busca de informações úteis em investigações. Diversos destes dispositivos empregam serviços executados em nuvens ou provedores remotos que acabam sendo envolvidos neste procedimento. Duas destas práticas investigativas são o Hacking Legal e Fishing Expedition. Este artigo 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. Esta proposta transita entre aspectos legais do ordenamento jurídico brasileiro e junto aos tribunais internacionais, bem como as práticas tecnológicas de obtenção dos dados.*

1. Introdução

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 do relacionamento direto entre cliente e provedor para um ambiente complexo no qual o cliente pode usar vários métodos de acesso para manter interações simultâneas com vários provedores [Steven M. Bellovin and Landau, 2014]. 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.

A criptografia e outros métodos de segurança da informação (e.g., biometria) tornaram-se uma proteção indispensável. Todavia, as instituições de segurança pública ao redor do mundo alegam que estas medidas constituem um obstáculo para o cumprimento das suas funções [Hennessey, 2016]. Por outro lado, há a preocupação de enfraquecimento dos padrões de privacidade tendente a colocar em risco a segurança da Internet

e a proteção dos dados pessoais [Li et al., 2018]. Assim, ocorre um debate contínuo e acelerado no âmbito das políticas públicas acerca da atuação e limitações dos governos e das agências policiais e de investigação com vistas a se estabelecer um equilíbrio entre segurança nacional e privacidade de dados. Duas são as principais abordagens desse contexto: *Hacking Legal* e *Fishing Expedition*.

Este artigo apresenta uma proposta de análise comparativa entre a práticas do *Hacking Legal* e *Fishing Expedition* relacionadas aos desafios tecnológicos e legislação aplicada no âmbito nacional e internacional, por meio de um levantamento sistemático para identificar as práticas abordadas na produção de provas digitais pelas agências policiais e de investigação. O artigo está organizado como segue. A Seção 2 fundamenta o contexto e introduz *General Data Protection Regulation* (GDPR) e Lei Geral de Proteção de Dados (LGPD), bem como as práticas *Hacking Legal* e *Fishing Expedition*, seguida de breve análise comparativa. A Seção 3 descreve o problema de pesquisa, e a Seção 4 descreve a proposta.

2. Fundamentação

As pessoas passaram a ser vistas como um dado estatístico analisado de acordo com suas postagens nas redes sociais, sendo seus dados pessoais e sua vida privada considerados insumos do comércio virtual [Ferreira et al., 2021]. Assim, as regulamentações sobre proteção de dados passaram por diversas fases até chegar ao momento atual quando o direito à proteção de dados adquire enfoque de direito fundamental e ganha legislações específicas e completas como o GDPR e a LGPD.

O GDPR foi aprovado em 2016 e padronizou a proteção de dados pessoais, estabelecendo os princípios norteadores de seu tratamento na comunidade Europeia [GDPR, 2016]. No Brasil, em 2018, inspirada no GDPR, foi assinada a LGPD (Lei nº 13.709/2018) versando 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 [Pereira, 2021]. A Tabela 1 relaciona alguns critérios comparativos entre estas legislações.

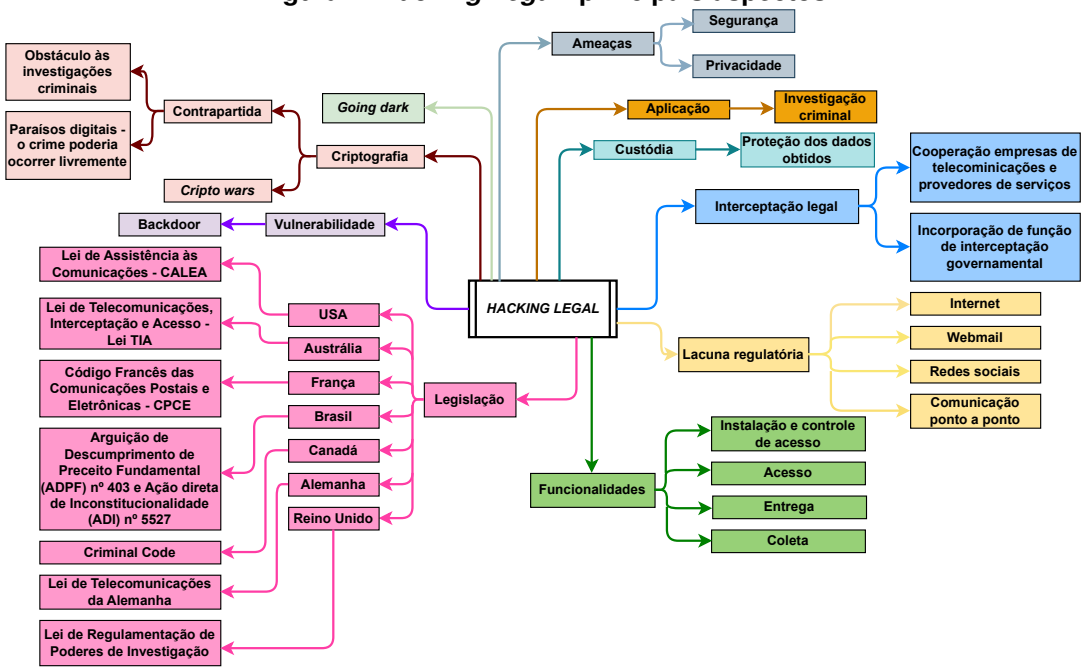
Tabela 1. Comparativo GDPR *vs.* LGPD.

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
Estrutura	173 *Recitals* (Considerandos) e 99 Artigos distribuídos em 11 Capítulos	66 Artigos distribuídos em 10 Capítulos
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: (i) empresa situada no território da União Europeia, independente do tratamento de dados ocorrer dentro ou fora dela; (ii) empresa não estabelecida na União Europeia, de titulares residentes no território da União Europeia; (iii) empresa não estabelecida na União Europeia, mas em local onde é aplicado o direito de um Estado-Membro	Tratamento de dados pessoais desde que: (i) operação de tratamento realizada em território nacional; (ii) a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; (iii) os dados pessoais do tratamento tenham sido coletados no território nacional
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

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. Assim, a investigação digital tornou-se essencial em uma sociedade cada vez mais conectada, sendo necessário entender os possíveis riscos de segurança e privacidade na implementação das práticas de *Hacking Legal* e *Fishing Expedition* como mecanismos de obtenção de provas relacionados a crimes cibernéticos. Na sequência, são introduzidas as definições elementares destas práticas:

- *Hacking Legal*. 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]. Trata-se de um procedimento legal 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. Para [Mayer, 2018], o *Hacking Legal* subverte as barreiras da segurança para dar aos investigadores acesso aos dados e recursos que eles precisam. [Bellovin, 2021] registra ser o *hacking legal* uma prática preferível a colocar *backdoors* em sistemas de criptografia. As aplicações do *hacking legal* 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*).

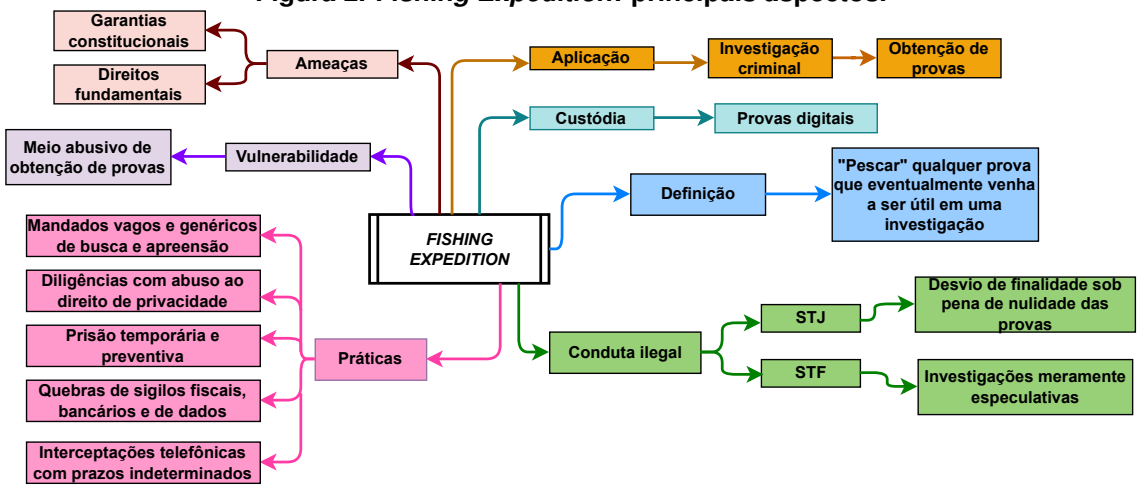
Figura 1. *Hacking Legal*: principais aspectos.



De um modo geral, o *Hacking Legal* 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, salvaguadar a segurança, os direitos fundamentais e o devido processo legal [Liguori, 2020]. A Figura 1 resume alguns dos principais aspectos desta prática.

- *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, 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. Para [Bandeira, 2020], é 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. Por se tratar de meio abusivo de obtenção de prova, a prática da *Fishing Expedition* tem largo campo de ocorrência na cultura penal, no aproveitamento, por parte dos agentes públicos, de diligências, com ou sem autorização. Além disso, em [Silva, 2022], o juiz Moraes da Rosa define *Fishing Expedition* 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 (Figura 2).

Figura 2. *Fishing Expedition*: principais aspectos.



Visando proporcionar maior embasamento para realizar o estudo comparativo proposto, foram analisados alguns critérios abordados pelas práticas do *Hacking Legal* e *Fishing Expedition*, listados na Tabela 2. Assim, é possível estabelecer uma correlação entre suas aplicações e abrangências no contexto da privacidade dos dados pessoais.

Tabela 2. Comparativo *Hacking Legal vs. Fishing Expedition*.

Critério	H*acking Legal*	*Fishing Expedition*
Foco	Obtenção de acesso a dados, pelas autoridades policiais e de inteligência	Obtenção de provas para subsidiar uma futura acusação
Aplicação	Investigação criminal	Investigação criminal
Vulnerabilidade	Restringir a criptografia, com a implementação de *backdoors*	Meio abusivo de obtenção de provas
Ameaças	Ameaças à privacidade e segurança	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.	Necessário que a investigação defina antecipadamente o seu objeto
Custódia	Semelhante a uma operação forense remota devendo obedecer a cadeia de custódia e a proteção dos dados obtidos	As provas digitais devem obedecer a cadeia de custódia.
Ferramentas	Ferramentas de software que exploram vulnerabilidades	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

3. Problema

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 de *Hacking legal* e *Fishing Expedition* para lidar com a necessidade das agências policiais e de inteligência, visando elucidar a aplicação no ordenamento jurídico brasileiro, em respeito às previsões legais, e junto aos tribunais internacionais. Para tanto, o objetivo geral deste estudo é realizar uma análise comparativa apresentando uma visão geral do status atual destas práticas abordadas e os desafios à tecnologia e às regras de interceptação legal com vistas a explorar a flexibilização dos métodos de colheita de provas.

4. Proposta de pesquisa

Este trabalho apresenta uma proposta de análise comparativa dos aspectos legais e técnicos das práticas de *Hacking Legal* e *Fishing Expedition*. Da análise da Tabela 2 e, partindo de um conjunto interseção entre práticas abordadas, pode-se definir quais os pontos de avaliação com vistas a verificar se existem, na literatura, trabalhos relacionados. Inicialmente, será feita uma pesquisa exploratória para traçar o referencial teórico sobre os principais conceitos relacionados ao tema de investigação de forma a se obter uma visão geral do assunto. Na sequência será realizada uma revisão sistemática da literatura para identificar os trabalhos relacionados/estado da arte das práticas abordadas e legislação aplicadas no âmbito nacional e internacional. Como resultado, será elaborada uma análise comparativa no âmbito nacional e estrangeiro, considerando e selecionando as legislações existentes acerca do tema e principal ferramental tecnológico e práticas investigativas. A etapa final da pesquisa visa apresentar o ordenamento jurídico em vigor de forma a auxiliar as autoridades competentes na salvaguarda dos interesses da segurança nacional, das relações exteriores, do bem-estar econômico, da integridade das informações armazenadas e veiculadas, entre outros. Por fim, adiciona-se a parte de correlacionar a tecnologia e aspectos legais que proporcione um ponte de ligação entre profissionais da segurança da infirmação e profissionais relacionados do direito e órgão do governo.

5. Considerações & Trabalhos futuros

A análise preliminar presente neste trabalho visa mostrar, em razão da extensão da tecnologia na vida das pessoas, a necessidade de haver clara regulamentação da dimensão da invasão da intimidade e vida privada e quais devem ser os limites legais para captura e análise de dados, de forma a utilizar as práticas do *Hacking Legal* e *Fishing Expedition*, sem comprometer a proteção da privacidade e dos dados pessoais. Finalmente, serão destacados os desafios em aberto e a direção futura destas práticas nos tribunais pátrios e internacionais.

Agradecimentos: Os autores agradecem o apoio do LabP2D/UDESC e a FAPESC.

Referências

Bandeira, S. d. O. (2020). A ilegalidade da pesca predatória por provas ("fishing expedition") nos mandados de busca e apreensão genéricos. Tcc, Universidade Federal Rural do Semiárido, Mossoró, Brasil.

Bellovin, S. M. (2021). The law and lawful hacking. *IEEE Security amp; Privacy*, 19(04):76–76.

Ferreira, D. A. A., Pinheiro, M. M. K., and Marques, R. M. (2021). Privacidade e proteção de dados pessoais: perspectiva histórica. *InCID: Revista de Ciência da Informação e Documentação*, 12(2):151–172.

GDPR (2016). General data protection regulation-gdpr. https://gdpr.eu/tag/gdpr/.

Hennessey, S. (2016). Lawful hacking and the case for a strategic approach to "going dark". In *Brookings*. https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/.

Li, C.-Y., Huang, C.-C., Lai, F., Lee, S.-L., and Wu, J. (2018). A comprehensive overview of government hacking worldwide. *IEEE Access*, 6:55053–55073.

Liguori, C. (2020). Exploring lawful hacking as a possible answer to the "going dark"debate. In *Mich. Tech. L.*

Mayer, J. (2018). Government hacking. In *The Yale Law Journal*, volume 3. https://www.yalelawjournal.org/pdf/Mayer_k3iy4nv8.pdf.

Pereira, Ana Bárbara Gomes; Rodrigues, G. R. V. V. B. R. (2021). Percepções sobre criptografia e investigações criminais no brasil: mapeamento e análise. Master's thesis, Instituto de Referência em Internet e Sociedade, Belo Horizonte, Brasil.

Silva, V. G. d. (2022). *Fishing expedition e encontro fortuito na busca e na apreensão: um dilema oculto do processo penal*. Emais, Florianópolis/Brasil, 2nd edition.

Steven M. Bellovin, Matt Blaze, S. C. and Landau, S. (2014). Lawful hacking: Using existing vulnerabilities for wiretapping on the internet. *Nw. J. Tech. Intell. Prop.*, 12(1).