Coordenador
Higor Vinicius Nogueira Jorge

MANUAL DO PLANTÃO POLICIAL

Um Guia para o Atendimento de Ocorrências e suas Providências

3.ª edição

2026

EDITORA JusPODIVM
www.editorajuspodivm.com.br

ATENDIMENTO [INICIAL] DAS FRAUDES ELETRÔNICAS

Alesandro Gonçalves Barreto,
Emerson Wendt
e Karolinne Brasil Barreto

1. CONTEXTUALIZAÇÃO

"Conto do vigário", "golpe do baludo" e do "bilhete premiado" são fraudes do passado. Outrora, o estelionatário atuava numa área delimitada de atuação: bairros, cidades vizinhas, microrregiões e, quiçá, outros Estados, visto que o *modus operandi* exigia o corpo a corpo para aplicar suas técnicas de engenharia social e calotear os abstraídos.

Todavia, verifica-se que a fraude presencial deixou de existir, ainda persistindo os registros de ocorrência nas delegacias de polícia, porém, de maneira isolada. Na terceira década do Século XXI, os infratores deram nova roupagem ao embuste com o uso da Internet.

A tecnologia acelerou a migração da burla para o ciberespaço, especialmente após a Covid-19. O transgressor saiu das ruas e passou a empregar os recursos eletrônicos, permitindo um alcance sem balizas físicas. Agora, a escalabilidade é um facilitador para granjear um número maior de vítimas e almejar uma lucratividade

considerável. Nessas ocasiões, a identidade dos fraudadores é protegida por conexões de internet e, aliada a uma possível investigação realizada de maneira incorreta, aumenta a crença de que os crimes praticados na Internet são impunes.

Em vista disto, a Estratégia Nacional de Segurança Cibernética traz números alarmantes sobre os crimes praticados na Internet e pontua sobre a utilização de códigos maliciosos por organizações criminosas[1]:

> O risco para a economia brasileira, gerado pela intrusão em computadores e pela disseminação de códigos maliciosos praticados pelo crime organizado já é uma realidade, conforme se vê pelos dados a seguir, referentes à conectividade do Governo, do setor privado e dos cidadãos, aos índices globais e aos crimes cibernéticos: o Brasil ocupa o 66º lugar no ranking da Organização das Nações Unidas – ONU de tecnologia da informação e comunicação; apenas 11% dos órgãos federais têm bom nível em governança de TI; o Brasil ocupa o 70º lugar no Global Security Index, da UIT; 74,9% dos domicílios (116 milhões de pessoas) com acesso à internet;98% das empresas utilizam a internet; 100% dos órgãos federais e estaduais utilizam a internet; em 2017, foram setenta milhões e quatrocentas mil vítimas de crimes cibernéticos; em 2018, 89% dos executivos foram vítimas de fraudes cibernéticas; as questões de segurança desestimulam o comércio eletrônico; em 2017, os crimes cibernéticos resultaram em US$ 22.500.000.000,00 (vinte e dois bilhões e quinhentos milhões de dólares) de prejuízo; e, o Brasil é o 2º com maior prejuízo com ataques cibernéticos. (Brasil, 2020).

A pandemia causada pelo coronavírus, como referido, acelerou a prática de fraudes. Enquanto ocorria o isolamento social, os criminosos não pararam, adequaram-se e não entraram em quarentena. Longe disso, enxergaram um cenário de oportunidades e, munidos de farta engenharia social, passaram a aplicar golpes de maneira implacável: venda de falsas vacinas; medicamentos e equipamentos de proteção que nunca eram entregues.

1. Estratégia Nacional de Segurança Cibernética, aprovada pelo Decreto nª 10.222, de 05 de fevereiro de 2020 (Brasil, 2020).

No Brasil, há uma infinidade de golpes e fraudes praticados na Internet, dentre os quais cita-se:

- Tabela do PIX;
- Invasão de redes sociais, para venda de produtos e serviços que nunca serão entregues;
- Sites falsos de leilão de veículos e venda de produtos eletrônicos;
- Estelionato sentimental (golpe da novinha, *scammers* do amor etc.);
- Venda *fake* de nudes;
- Golpe do motoboy e do bolo de aniversário;
- Falsa central de bancos com envio de SMS, chamadas de secretárias eletrônicas ou links maliciosos por e-mail.

Goodman (2015) menciona sobre as facilidades encontradas pelo crime nesta nova realidade e ressalta sobre os perigos da exposição online[2]:

> Os crimes da velha guarda estão sendo viabilizados cada vez mais pelas novas tecnologias, e o big data permite que os criminosos tradicionais nos rastreiem com uma precisão cada vez maior. Devido ao nosso estilo de vida online 24 horas, sete dias por semana, estamos acessíveis o tempo todo, mesmo por aquele que não gostaríamos. O que é estranho sobre esse fenômeno é que muitas vezes nós, a partir do fornecimento voluntário de informações ou via vazamento de dados, estamos tornando mais fácil para os perseguidores, assediadores e criminosos nos encontrarem. (Goodman, 2015, p. 101).

Neste diapasão, objetiva-se fazer uma abordagem sobre a importância do atendimento dos golpes (com interação da vítima) e fraudes eletrônicas (sem interação da vítima), sobre quais dados devem ser buscados, bem como as recomendações para a preservação do patrimônio da vítima e/ou terceiros envolvidos.

2. Marc Goodman, Future Crimes: Tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. p.101

2. FRAUDES 3.0 – DESAFIOS DA POLÍCIA JUDICIÁRIA

É importante iniciar a abordagem com um questionamento: quem é o cibercriminoso?

Na grande maioria das vezes, ele não precisa ter conhecimentos avançados em Tecnologia da Informação. Notadamente, quando se fala das *fraudes eletrônicas*, aquele indivíduo que aplicava técnicas de engenharia social para convencer às vítimas que tinha um bilhete premiado nas mãos, agora faz emprego destas "ciladas", porém, com recursos tecnológicos. Assim, a *trapaça eletrônica* é impulsionada por diversos facilitadores no nosso país.

O primeiro deles é referente aos *data brokers* ilegais ofertados livremente na internet, com informações como: endereços, filiação, lista de contatos, rendimentos, veículos, locais de vacina e até mesmo imagens de radares (Pinheiro; Carone, 2024). Com tanta informação, fica fácil convencer a vítima e/ou ativar o gatilho mental de cooperação.

Em segundo plano, adiciona-se as facilidades encontradas para fazer a portabilidade indevida dos números telefônicos. Em que pese a Agência Nacional de Telecomunicações – ANATEL – e as operadores de telefonia atuarem na mitigação do problema, os estelionatários apoderam-se do *SIMCARD* e invadem redes sociais e contas de e-mail das vítimas[3]. A partir de então, assumem a identidade do usuário e, de posse de documento de identificação armazenados na conta invadida, abrem contas bancárias numa facilidade sem igual. Pode-se, então, afirmar que, no Brasil, o telefone não é algo seguro para vincular às mídias sociais.

A vítima, não sabendo como fazer e nem a quem procurar, busca auxílio na Delegacia de Polícia mais próxima de sua residência e não encontra, muitas vezes, o atendimento adequado, além de escutar algumas justificativas: "crime na internet..., não tem solução";

3. A partir de agosto de 2023, a ANATEL mudou as regras para determinar às operadoras de telefonia móvel o ajuste no procedimento atual de portabilidade para evitar a ocorrência de fraudes relacionadas ao sequestro da linha telefônica. Agora, o titular da linha deve receber um SMS para confirmação da portabilidade. Caso não confirme ou permaneça silente, a mudança de titularidade não será efetuada.

"não tem o que fazer"; "procure a Polícia Federal"; "invasão de conta do Instagram não é crime, não vou nem registrar teu BO".

Certamente, houve avanços significativos na área de investigação policial e no âmbito cibernético. As polícias judiciárias nos níveis estaduais e federais responderam a este novo cenário por meio de suas delegacias ou unidades especializadas (conforme Lei 12.735/2012). Além disso, as operações policiais noticiadas, quase que diariamente, relatam a prisão de indivíduos que, outrora, eram tidos acima de qualquer suspeita.

A legislação brasileira, por outro lado, experimentou progressos notáveis em diversos aspectos, como com a capitulação de crimes específicos (Brasil, 2012; 2021), regulamentação do armazenamento, fornecimento de registros de conexão, disponibilização de acesso a aplicações de Internet e de dados pessoais ou outras informações relevantes para a identificação de usuários/terminais, além da quebra de sigilo telemático com a delimitação da competência para processar e julgar as fraudes eletrônicas[4].

3. ATENDIMENTO INICIAL DAS FRAUDES ELETRÔNICAS

Cabe destacar que, antes mesmo de procurar a polícia, a vítima de uma *fraude eletrônica* deve realizar alguns procedimentos importantes como, por exemplo, a preservação do conteúdo, caso possível. Apenas um *print screen* pode não ser suficiente, eis que foi realizado de forma unilateral e não captura a URL por completo ou deixa de visualizar outros elementos informativos, importantes na investigação criminal. Um salvamento de página ou a confecção de uma ata notarial são as melhores recomendações[5].

---

4. A lei nº 14.155, de 2021 estabeleceu, no art. 70, § 4º do Código de Processo que, nos crimes previstos no art. 171 do Código Penal, quando praticados mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.

5. Art. 384 do Código de Processo Civil – Art. 384. A existência e o modo de existir de algum fato podem ser atestados ou documentados, a requerimento do interessado, mediante ata lavrada por tabelião.

   Parágrafo único. Dados representados por imagem ou som gravados em arquivos eletrônicos poderão constar da ata notarial.

Nessa mesma linha, quando se tratar de compras fraudulentas ou invasão de contas bancárias (Brasil, 2021), a vítima deve entrar em contato primeiro com sua instituição financeira para fazer o bloqueio das transações ou fazer uso do mecanismo especial de devolução – MED –, nos casos de transações fraudulentas por meio de PIX. Esta regra também vai ser aplicada para o roubo de *smartphones*, objetos de desejo para os fraudadores, não pelo seu valor de revenda, mas em razão das informações financeiras guardadas consigo. O registro do Boletim de Ocorrência (BO), assim, deve, cronologicamente, ser feito apenas depois do bloqueio de contas bancárias, modificação de senhas nas redes sociais e e-mail e, por último, a inibição do *SIMCARD* perante a operadora de telefonia móvel[6].

Ainda, depois de todos esses processos, nos resta mais um desafio: qual Delegacia de Polícia procurar?

De acordo com a Lei 12.735, de 30 de novembro de 2012 (Brasil, 2012), os órgãos de Polícia Judiciária devem criar de setores e equipes especializadas para a repressão aos crimes cibernéticos. De lá para cá, os Estados criaram e ampliaram as delegacias especializadas para o atendimento de parte destas ocorrências (Wendt, 2023).

Acontece que o volume de casos aumentou consideravelmente, resultando no acúmulo de procedimentos nestas unidades, bem como na especialização apenas para crimes complexos. A delegacia local, em regra, é quem dará e a quem caberá o atendimento inicial. Algumas polícias estaduais oportunizam a confecção do registro online. Se assim o fizer, a orientação é de que a vítima tenha em preencher todas as informações necessárias.

3.1. Delegacia de Polícia – Entrevista e Obtenção de Dados

A conversa inicial com a vítima é crucial para o sucesso na investigação das fraudes eletrônicas. Antes mesmo de iniciar qualquer

6. O Governo Federal lançou, no ano de 2023, o aplicativo Celular Seguro para permitir ao cidadão a comunicação, de forma eficiente e ágil, as ocorrências de roubos e furtos de celulares. Quando há o cadastro prévio no serviço, o usuário aciona o contato de confiança após o roubo e consegue bloquear rapidamente as contas bancárias e o IMEI junto às operadoras de telefonia.

registro, o policial deve procurar saber se ela já realizou alguns procedimentos: (a) bloqueio de contas bancárias, (b) contato com a operadora de telefonia, (c) recuperação das mídias sociais invadidas e (d) se ela fez algum salvamento do conteúdo e (e) do contato com o suspeito (redes sociais, e-mail, chaves PIX, contas bancárias, números de telefone, valores transferidos e beneficiários, dia e hora que perdeu acesso às contas).

Estes dados devem, na medida do possível, estar presentes no BO ou em termos de declaração, em face da sua relevância para a investigação que se seguirá. Durante esta entrevista inicial, o investigador poderá identificar alguns procedimentos que não foram realizados e solicitar/orientar que a vítima o faça como, por exemplo: manter contato com a instituição financeira[7], repassar as orientações para a recuperação das mídias sociais e contas de e-mail[8]. Essa conversa com a vítima é importante sempre no intuito de uma maior preservação do patrimônio.

Outra boa prática, é a polícia realizar o contato diretamente com a instituição financeira, tanto para suspender a conta fraudulenta quanto para facilitar na obtenção de informações, sem embargo de ordem judicial. Na prática, o(a) Delegado(a) de Polícia pode oficiar diretamente ao banco para saber quais foram os beneficiários dos valores subtraídos[9].

---

7. Como boa prática, é recomendável orientar a vítima que insista com o banco o bloqueio das contas bancárias para mitigar o prejuízo independentemente de registro de ocorrência. A recusa na suspensão e eventuais prejuízos futuros denota, em tese, falha na prestação do serviço, nos precisos termos do art, 14 do Código de Defesa do Consumidor: "O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos".

8. Alguns procedimentos de recuperação de contas invadidas estão disponíveis no site www.delbarreto.app.

9. A Lei Complementar 105/2001 estabelece em seu art. 1º, § 3º, IV: "Não constitui violação do dever de sigilo: IV – a comunicação, às autoridades competentes, da prática de ilícitos penais ou administrativos, abrangendo o fornecimento de informações sobre operações que envolvam recursos provenientes de qualquer prática criminosa".

3.2. Preservação dos Dados

A volatilidade é a regra quando se trata da preservação de dados de crimes praticados com uso de tecnologia, notadamente nas postagens em mídias sociais e em outras plataformas.

Dentre as possibilidades ofertadas, recomendamos a utilização das plataformas Law Enforcement, quando a fraude eletrônica tiver ocorrido nas mídias sociais[10]. Nestes casos, apenas as agências de aplicação da lei (Polícia, Ministério Público e Poder Judiciário) são autorizadas a aceder ao serviço com um cadastro prévio e emprego de e-mail institucional. Apesar de os advogados, por exemplo, não terem permissão de acesso, a sugestão é que, no momento do registro da ocorrência, solicite à autoridade policial que utilize este recurso para salvaguardar o conteúdo[11].

As plataformas Law Enforcement são úteis, ainda, para o envio de ordens judiciais e recebimento das respostas, requisição de dados cadastrais e solicitações emergenciais. Neste último caso, sempre que a vítima esteja em risco de morte ou risco de lesão corporal de natureza grave, devem ser formuladas de maneira transparente e específica: (a) abordar a urgência da situação; (b) a necessidade iminente de obtenção dos dados; (c) a falta de alternativas mais rápidas e; (d) sempre que possível, incluir anexos como arquivos ou URLs pertinentes ao caso.

Para os demais casos de preservação de conteúdo, aconselha-se a utilização de:

a) Ofício extrajudicial para o responsável pelo serviço;

b) Certidão policial lavrada por servidor dotado de fé pública;

c) Salvamento de página diretamente no browser ou com softwares, como HTTrack Website Copier, Cyotec WebCopy e o Verifact (ata notarial virtual);

d) Utilização da tecnologia blockchain;

---

10. No site www.delbarreto.app estão disponibilizadas as maneiras para acessar as principais plataformas Law Enforcement das seguintes aplicações de Internet: Facebook, Instagram, WhatsApp, Google, Microsoft, TikTok, Apple, Discord, Ifood, Kwai, Twitter e UBER.

11. A salvaguarda do conteúdo também está prevista no Marco Civil da Internet, arts. 13 e 15 (Brasil, 2014).

e) Contato direto com o serviço;

f) Cooperação Policial Internacional[12].

Apesar de não aconselhável, não se descarta o *print screen* como meio de preservação. Por vezes, pode até ser utilizado, mas em razão da unilateralidade ele deve sempre ser corroborado com outros elementos informativos da investigação policial em andamento.

3.3. Busca de elementos informativos e fontes abertas

Registrada a fraude eletrônica e preservado o conteúdo, o policial deve utilizar de pesquisa em fontes abertas, pela metodologia de OSINT (*Open Source Intelligence*) – dados livremente disponíveis –, com o intuito de buscar elementos informativos relacionados ao delito em investigação. Os dados encontrados devem ser confrontados com outras fontes de informação abertas ou fechadas: bancos de dados da polícia, informações sobre processos, dentre outros, além da possibilidade de serem complementados com a requisição extrajudicial de dados cadastrais.

Assim, a coleta deve ser iniciada com os mecanismos de busca Google e Bing, sempre na ótica de realizar as tarefas mais fáceis, primeiramente, e colocar entre *aspas* alguns termos específicos para buscas: e-mail, telefone, chave PIX, nomes, endereços e *modus operandi* da atividade criminosa.

Posteriormente, deve-se fazer buscas sobre pessoas, e-mail e telefone do fraudador com a utilização de algumas ferramentas gratuitas ou *freemium*:

> Epieos – disponível em https://epieos.com/, é um mecanismo de busca que permite conhecer contas ou serviços vinculados pelo email ou número de telefone ao Google, Gravatar,

12. Decreto 11.491, de 12 de abril de 2023. A Convenção de Budapeste estabelece em seu art. 16: – Preservação expedita de dados de computador.1. Cada Parte adotará medidas legislativas e outras providências necessárias para permitir que a autoridade competente ordene ou obtenha a expedita preservação de dados de computador especificados, incluindo dados de tráfego, que tenham sido armazenados por meio de um sistema de computador, especialmente quando haja razões para admitir que os dados de computador estão particularmente sujeitos a perda ou modificação.

> Trello, Duolingo, Pinterest, Chess, Stava, Vivino, Emailchecker, Flickr, Skype e Hibp;
>
> Osint Industries – acessível em https://osint.industries/, realiza consultas em mais de 200 websites, possibilitando retorno também sobre telefones;
>
> Lampyre – https://lampyre.io/, realiza consultas em vários serviços, tendo por base e-mail, nome de usuário, telefone, IP, domínio etc.;
>
> IntelX – https://intelx.io/, realiza pesquisa sobre e-mail, domínios, URLs, IPs, CIDRs, endereços Bitcoin e *hashes* em locais como *darknet*, plataformas de compartilhamento de documentos, *whois*, vazamentos de dados públicos e outros. Além disso, mantém um histórico de resultados, semelhante ao Wayback Machine – www.archive.org –, armazenando cópias históricas de sites.
>
> Maltego – https://www.maltego.com/ – traz como resultado as informações de pessoas, e-mails, redes sociais, empresas e sites, todo em forma de vínculos.

Quanto aos domínios utilizados pelo fraudador para aplicar golpes, as pesquisas trazem dados relevantes para a investigação: proprietário, CPF OU CNPJ, e-mail, telefone de contato, outros domínios vinculados, histórico de mudanças e as informações sobre o registrador.

Em situações de fraude de leilão de veículos ou sites falsos de venda de eletrônicos, estas buscas são fundamentais para a investigação.

Os serviços *whois* são recomendados na obtenção de boa parte destes dados:

> Whois Registro BR (domínios terminados em .br, CPF e CNPJ) – https://registro.br/tecnologia/ferramentas/whois/;
>
> ICANN LookUp: https://lookup.icann.org/en;
>
> Domain Tools: https://whois.domaintools.com/;
>
> DNS Stuff: https://www.dnsstuff.com/freetools;
>
> Robtex: https://www.robtex.com/dns-lookup;
>
> View DNS Info: https://viewdns.info/.

Outro passo importante [de complementação de informações sobre domínios] é a busca nos domínios por dados relevantes de tráfego, interação dos usuários, monetização e gerenciamento da

página. Os individualizadores do Google – Analytics[13], AdSense[14] e Tag Manager[15] – são coletados tanto por meio de ferramentas disponíveis quanto no código-fonte da página.

Para o acompanhamento de fraudes e os respectivos *modus operandi*, é indicado o acesso ao Catálogo de Fraudes da RNP [https://catalogodefraudes.rnp.br/]. Criado no ano de 2008, possui um repositório das principais fraudes e golpes eletrônicos disponibilizados pela comunidade e traz mensagens e captura de telas das trapaças *online*.

Outra orientação [complementar] é o acompanhamento destas novas modalidades e sua divulgação em sites, *blogs* e perfis de redes sociais[16].

CONSIDERAÇÕES FINAIS

Sempre com atenção para as vulnerabilidades existentes, o General da Força Aérea Americana Donald Kutyna cita:

> Na Força Aérea, temos uma regra: verifique as seis. Um cara está voando, olhando em todas as direções e se sentindo seguro. Outro cara chega por trás dele (às 06 horas, em um relógio imaginário onde 12 horas é diretamente em frente) e dispara. A maioria dos aviões é abatida dessa forma. Achar que está seguro é muito perigoso! Em algum lugar, há um ponto fraco que você precisa encontrar. Você sempre deve verificar as 06 horas. (Feynman, 1987).

13. Coleta dados de sites e aplicativos e traz insights sobre os usuários (origem, páginas visitadas, dispositivos informáticos, navegadores etc.) Ele pode ser consultado no código-fonte pelo termo UA.
14. É uma plataforma de publicidade que relaciona anúncios ao seu site com base nos visitantes e conteúdo disponibilizado, ou seja, é uma da maneira que os responsáveis pelo domínio monetizam. Ele deve ser consultado no código-fonte por pub-.
15. Autoriza a atualização dos códigos de rastreamento e fragmentos (tags) associados a um site ou aplicativo sem a necessidade de alteração do código-fonte. A busca é feita pelo termo GTM-.
16. Os perfis do Instagram @delbarreto19 e @emersonwendt trazem recomendações diárias sobre golpes e fraudes e as melhores formas de prevenção.

As fraudes eletrônicas fazem parte da nova realidade da investigação criminal. O policial, por mais que recuse ou tenha receio desta nova realidade, não pode mais fugir e tem que encontrar os pontos vulneráveis e rastros deixados pelo suspeito. É certo que ele não vai precisar ser um especialista nas áreas de Tecnologia da Informação, apesar da necessidade das polícias em ter nos seus quadros profissionais como este.

Desse modo, o policial necessita, pois, conhecimentos básicos de funcionamento da Internet e quais os dados relevantes para a investigação da fraude eletrônica. A capacitação contínua do investigador, desde seu ingresso até a aposentadoria, deve ser regra para que as polícias judiciárias possam dar ao menos, um atendimento inicial adequado aqueles que procuram auxílio nas delegacias de polícia. Tal conclusão foi corroborada na tese defendida por Wendt (2023).

Outro ponto interessante para o atendimento das fraudes eletrônicas é o estabelecimento de protocolos de ocorrências com a disseminação para as unidades de polícia judiciária no estado. Essa boa prática é de grande valia, eis que a polícia local, independentemente de ser delegacia distrital ou especializada, atua de maneira uniforme na investigação de delitos cibernéticos. Um bom exemplo é a Polícia Civil do Distrito Federal, que tem adotado esta prática com muito sucesso.

Segundo Abraham Lincoln enunciava, dadas seis horas para derrubar uma árvore, seria necessário utilizar as quatro primeiras afiando o machado. Assim, o atendimento inicial da polícia nas fraudes eletrônicas ou em qualquer outra ocorrência é crucial para a investigação policial. Pois, é neste momento que a vítima ou o noticiante disponibilizam informações relevantes e que não podem ser desprezadas. Deixar de atender ou simplesmente registrar um boletim às pressas só traz benefícios a um lado: o fraudador.

REFERÊNCIAS

BARRETO, Alesandro Gonçalves; KUFA, Karina. SILVA, Marcelo Mesquita. **Cibercrimes e seus Reflexos no Direito Brasileiro**. São Paulo: Editora Juspodivm, 2020.

BARRETO, Alesandro Gonçalves; SILVA, Natália Siqueira. **É bom demais para ser verdade**. São Paulo. 2022. Disponível em: https://wbeduca.com.br/pt/cursos/ebook-e-bom-demais-para-ser-verdade. Acesso em: 28 jan. 2024.

BARRETO, Alesandro Gonçalves; BRAGA, Francisco das Chagas Leal Júnior; NERY, José de Anchieta Neto; SILVA, Natália Siqueira. **Conectado e Inseguro – Comportamentos que você deveria evitar na internet**. Porto Alegre: WB Editora. 2023. Disponível em: https://wbeduca.com.br/pt/cursos/ebook-conectado-e-inseguro-comportamentos-que-voce-deveria-evitar-na-internet. Acesso em: 28 jan. 2024.

BARRETO, Alesandro Gonçalves; RECHINHO, Bruno. **Crônicas de um investidor Inseguro** – Baseado em Fatos Reais sobre como perder dinheiro com golpistas. São Paulo. 2023. Editora do Autor.

BRASIL. Decreto-Lei no 2.848, de 7 de dezembro de 1940. **Código Penal**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 28 jan. 2024.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 28 jan. 2024.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 28 jan. 2024.

BRASIL. **Lei Complementar nº 105, de 10 de janeiro de 2001**. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm. Acesso em: 28 jan. 2024.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 – Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 28 jan. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 jan. 2024.

BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 28 jan. 2024.

BRASIL. **Decreto nº 10.22, de 05 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 28 jan. 2024.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 28 jan. 2024.

BRASIL. **Decreto nº 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 28 jan. 2024.

FEYNMAN, Richard P. Mr. Feynman goes to Washington. **Engineering and Science**, v. 51, n. 1, p. 6-22, 1987.

GOODMAN, Marc. **Future Crimes**: Tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. HSM Editora, 2015.

GOVERNO FEDERAL. **Celular Seguro já está disponível no GOV.BR**. Disponível em: https://www.gov.br/gestao/pt-br/assuntos/noticias/2023/dezembro/celular-seguro-ja-esta-disponivel-no-gov.br. Acesso em: 28 jan. 2024.

PINHEIRO, Mirelle; CARONE, Carlos. Grupo invade sistemas federais para vender dados a facções e policiais. **Metrópoles**, 31/01/2024. Disponível em: https://www.metropoles.com/distrito-federal/na-mira/grupo-invade-sistemas-federais-para-vender-dados-a-faccoes-e-policiais. Acesso em: 31 jan. 2024.

WENDT, Emerson. **As expectativas cognitivas e normativas dos atores de investigação policial em face dos crimes cibernéticos**. Orientador: Renata Almeida da Costa. 2023. 305 p. Tese (doutorado em Direito) – Universidade La Salle: Canoas, 2023.

APLICAÇÃO DAS FONTES ABERTAS PELA EQUIPE DO PLANTÃO POLICIAL

Emerson Wendt
e Higor Vinicius Nogueira Jorge

Sumário: 1. Introdução. 2. Plantão policial. 3. Fontes abertas [OSINT] no plantão policial. 4. Ambiente seguro para atividade de OSINT. 5. Perfil de investigação digital (assistentes virtuais de investigação). 6. Casos concretos de uso de fontes abertas. 7. Ferramentas de inteligência em fontes abertas [OSINT]: 7.1. Google e suas infinitas possibilidades: 7.1.1. Operadores de Pesquisa de Engenhos de Busca; 7.1.2. Tipos de Pesquisa; 7.1.3. Ferramentas Avançadas; 7.1.4. Configurações de Pesquisa; 7.1.5. Google Alerts. 8. Análise de redes sociais e comunicação digital. 9. Análise de imagens e vídeos. 10. Pesquisas de e-mail e domínio. 11. Análise de vulnerabilidades e segurança. 12. Geolocalização e informações geográficas. 13. Ferramentas de busca e coleta de dados. 14. Análise de documentos e vazamentos de dados. 15. Pesquisa e desenvolvimento. 16. Considerações finais. Referências.

1. INTRODUÇÃO

No período contemporâneo, caracterizado por um incremento exponencial na utilização de meios tecnológicos, o emprego da denominada Inteligência em Fontes Abertas (OSINT – *Open Source Intelligence*) tem sido fundamental na investigação criminal.

Essas técnicas, que envolvem a coleta, análise e utilização de dados disponíveis, tornam-se ferramentas importantes nas mãos dos integrantes das polícias judiciárias, permitindo uma ampla gama de operações investigativas com celeridade e sem maiores entraves burocráticos.

O amplo "mundo da Internet", das redes sociais aos bancos de dados públicos e, até mesmo, fontes mais tradicionais, como bibliotecas e arquivos de jornais e TVs, transformam-se em fontes valiosas de informações.

A revolução tecnológica mudou drasticamente o cenário da investigação criminal, aumentando o valor e a importância das fontes abertas, de modo que os avanços tecnológicos não apenas acrescentaram o volume de informações acessíveis, mas também incrementaram as metodologias para filtrar, analisar e usar esses dados com precisão e eficiência.

Um dos principais desafios reside em lidar de forma eficaz com esse imenso volume de dados de dados de forma eficaz, adotando estratégias que incluem o uso criterioso de palavras-chave, análise de redes sociais e avaliação de publicações, postagens em fóruns online etc.

Nesse contexto, uma infinidade de ferramentas está disponível aos policiais que realizam a investigação criminal, desde softwares especializados na análise das redes e mídias sociais até sistemas avançados para busca por imagem, pessoas, locais e empresas, além de plataformas para monitoramento da mídia.

Quando empregados de maneira estratégica, esses recursos não só ampliam a coleta de dados, mas também enriquecem a análise de padrões e a descoberta de relações entre conjuntos diversos de informações, alterando significativamente o panorama da investigação criminal.

Assim, o objetivo deste texto é estabelecer um panorama da aplicabilidade das fontes abertas durante o atendimento de vítimas nos plantões policiais.

2. PLANTÃO POLICIAL

O plantão policial em uma Delegacia da Polícia Civil é elemento fundamental para o funcionamento da Segurança Pública, atuando como a espinha dorsal de uma unidade de Polícia Judiciária, permitindo que o órgão permaneça operacional a todo o momento.

Os policiais que exercem suas atribuições no local geralmente são responsáveis por um vasto repertório de atividades, desde o atendimento inicial na unidade, até a realização de investigações