Trilha do Advogado · Material técnico

Catálogo de Ferramentas OSINT para Uso Jurídico

Ferramentas de inteligência de fontes abertas classificadas por finalidade e por risco jurídico para o uso pela advocacia. A régua é única: só se acessa fonte aberta, sem invasão, sem quebra de sigilo e sem engenharia social. O risco indicado orienta a cautela, não é recomendação de uso indiscriminado.

Busca e buscadores

Google Dorks (operadores de busca avançada)

risco baixo

Refina buscas em mecanismos de pesquisa com operadores para localizar arquivos, subdomínios e conteúdo indexado específico.
Limite: Depende do que o buscador indexou e sofre com resultados desatualizados ou removidos do índice.

Consulta CNPJ (base pública da Receita)

risco baixo

Recupera situação cadastral, quadro societário e CNAE de empresas a partir de bases abertas de CNPJ.
Limite: A base pública pode estar defasada em relação à situação atual na Receita; validar em fonte oficial.

Phoneinfoga

risco médio

Levanta informações públicas associadas a um número de telefone, como operadora, país e presença online.
Limite: Resultados são indiciários e frequentemente incompletos; muitos dados úteis não são públicos.

Redes sociais (SOCMINT)

Sherlock

risco médio

Procura um mesmo nome de usuário em centenas de plataformas para mapear a presença online de um apelido.
Limite: Gera falsos positivos e não confirma que perfis homônimos pertencem à mesma pessoa.

Maigret

risco médio

Enumera perfis por nome de usuário em muitos sites e extrai metadados públicos de cada perfil encontrado.
Limite: Sujeito a bloqueios das plataformas e a coincidências de apelido que exigem validação manual.

Nitter / ferramentas de captura de redes

risco médio

Facilita a leitura e preservação de conteúdo público de redes sociais sem necessidade de login.
Limite: Instâncias são instáveis e mudanças nas plataformas quebram a coleta com frequência.

GHunt

risco médio

Reúne informação pública ligada a uma conta Google a partir de um e-mail ou identificador.
Limite: Alterações de política do provedor reduzem o que é acessível e podem quebrar a ferramenta.

Geolocalização (GEOINT)

Google Earth e Street View

risco baixo

Fornece imagens de satélite, histórico temporal e vistas de rua para caracterizar e datar locais.
Limite: A data das imagens pode não coincidir com o fato; resolução e cobertura variam por região.

OpenStreetMap

risco baixo

Mapa colaborativo aberto que permite consultar detalhes de vias, edificações e pontos de interesse com dados exportáveis.
Limite: Precisão depende de contribuições voluntárias e pode conter lacunas ou informação desatualizada.

FlightRadar24

risco baixo

Acompanha voos em tempo real e histórico de rotas a partir de dados de rastreamento de aeronaves.
Limite: Nem toda aeronave é rastreável e voos sensíveis podem ser filtrados; histórico detalhado é pago.

MarineTraffic — risco baixo
Rastreia embarcações e histórico de navegação por sinais AIS, com dados de porto e trajeto.
Limite: Depende de transmissão AIS ativa e cobertura de estações; histórico completo exige assinatura.

Exif e geolocalização (GeoGuessr assistido / SunCalc) — risco baixo
Apoia a datação e localização de fotos por sombras, sol e pistas visuais combinadas com mapas.
Limite: Método interpretativo que exige corroboração; margem de erro alta sem ponto de referência claro.

Google Maps / Places — risco baixo
Fornece endereços, pontos de interesse, avaliações e fotos de local para caracterização de endereços.
Limite: Fotos e avaliações são de terceiros e podem estar desatualizadas ou mal localizadas.

Domínios e rede

theHarvester — risco médio
Coleta e-mails, subdomínios e nomes associados a um domínio a partir de fontes públicas e buscadores.
Limite: Depende de fontes que impõem limite de requisições e pode retornar dados incompletos ou antigos.

registro.br (WHOIS .br) — risco baixo
Consulta a titularidade e os dados técnicos de domínios sob o .br, com datas e contatos quando públicos.
Limite: Dados de titular de pessoa física costumam ser mascarados por privacidade.

WHOIS internacional / RDAP — risco baixo
Recupera registro de domínios genéricos e faixas de IP, com responsável, datas e servidores.
Limite: Após regras de privacidade, muitos campos vêm redigidos, e a informação pode estar desatualizada.

Hunter.io — risco médio
Descobre e valida padrões de e-mail corporativo associados a um domínio a partir de fontes públicas.
Limite: Resultados são inferidos e podem incluir endereços inexistentes; volume útil exige plano pago.

Infraestrutura de rede

Shodan — risco médio
Indexa dispositivos e serviços expostos na internet, mostrando portas, banners e tecnologias de um host.
Limite: Mostra estado indexado que pode estar desatualizado e não cobre toda a internet.

Censys — risco médio
Mapeia hosts, certificados e serviços expostos na internet para análise de superfície de ataque e infraestrutura.
Limite: Cobertura e frescor variam; recursos avançados exigem plano pago.

Nmap — risco alto
Mapeia portas e serviços de hosts em rede para reconhecimento de infraestrutura.
Limite: É varredura ativa que interage com o alvo e pode ser detectada e bloqueada.

Imagem e mídia

Google Reverse Image e TinEye — risco baixo
Busca reversa de imagens para localizar onde uma foto aparece na web e identificar a fonte original.
Limite: Não indexa toda a web e falha com imagens editadas, recortadas ou de rostos pouco expostos.

Yandex Images — risco médio
Busca reversa de imagens com desempenho notável em reconhecimento facial e cenas, útil em geolocalização visual.
Limite: Resultados podem ser ruidosos e a ferramenta não confirma identidade, apenas semelhança visual.

Blockchain e cripto

Etherscan — risco médio
Explora transações, saldos e contratos na rede Ethereum a partir de endereços e hashes públicos.
Limite: Endereços são pseudônimos; a atribuição a uma pessoa exige informação externa de identificação.

Blockchain.com Explorer — risco médio
Consulta transações e endereços da rede Bitcoin, permitindo rastrear fluxos entre carteiras públicas.
Limite: Rastreamento é indiciário; mixers e múltiplas carteiras dificultam a atribuição e a leitura do fluxo.

Agregadores

Maltego — risco médio
Correlaciona entidades (pessoas, domínios, e-mails, empresas) em grafos visuais a partir de transformações de várias fontes.
Limite: Boa parte das transformações úteis depende de APIs pagas e a qualidade do grafo reflete a qualidade das fontes conectadas.

SpiderFoot — risco médio
Automatiza a coleta OSINT sobre um alvo (domínio, IP, e-mail, nome) integrando dezenas de módulos de reconhecimento.
Limite: Consultas ativas podem tocar a infraestrutura do alvo e gerar ruído; requer curadoria dos resultados para evitar falsos positivos.

Recon-ng — risco médio
Framework modular de reconhecimento web que organiza a coleta OSINT sobre domínios e pessoas.
Limite: Muitos módulos exigem chaves de API e alguns realizam consultas ativas ao alvo.

OSINT Framework (diretório) — risco baixo
Cataloga e organiza centenas de fontes e ferramentas OSINT por categoria para orientar a pesquisa.
Limite: É apenas um índice de links; muitos recursos listados ficam obsoletos ou fora do ar.

Bellingcat Toolkit / Online Investigation Toolkit — risco baixo
Compila metodologias e ferramentas de verificação, geolocalização e análise de mídia para investigação aberta.
Limite: É curadoria de recursos; a eficácia depende da habilidade do investigador em aplicá-los.

Forense digital

Wayback Machine — risco baixo
Recupera versões arquivadas e datadas de páginas da web para comprovar conteúdo passado ou removido.
Limite: Cobertura irregular; ausência de captura não prova inexistência do conteúdo.

ExifTool — risco baixo
Lê e edita metadados de arquivos de imagem e documento, incluindo data, dispositivo e coordenadas geográficas.
Limite: Muitos serviços removem metadados no upload, e datas podem ser adulteradas, exigindo cautela probatória.

Have I Been Pwned — risco baixo
Verifica se um e-mail ou telefone consta em vazamentos de dados conhecidos, sem revelar senhas.
Limite: Cobre apenas incidentes catalogados e não entrega o conteúdo do vazamento.

Metagoofil / FOCA — risco médio
Extrai metadados de documentos públicos de um domínio para revelar autores, softwares e caminhos internos.
Limite: Depende de documentos ainda disponíveis online e de metadados não terem sido higienizados.

Da ferramenta ao dossiê

Ferramenta sem método não vira prova. O escritório opera o Scanner OSINT, que cruza dezenas de bases públicas e privadas e consolida o resultado em dossiê estruturado, com mapa de relações e matriz de risco, sob cadeia de custódia. Conheça em gabrielbulhoes.com.br/osint ou fale pelo WhatsApp (84) 98164-1881.