Ministério Público nas ELEIÇÕES 2024

Guia Prático de Investigação na Internet

MPF
Ministério Público Federal

MINISTÉRIO PÚBLICO FEDERAL

Procurador-Geral da República
Paulo Gonet Branco

Vice-Procurador-Geral da República
Hindenburgo Chateaubriand Pereira Diniz Filho

Vice-Procurador-Geral Eleitoral
Alexandre Espinosa Bravo Barbosa

Ouvidor-Geral do Ministério Público Federal
Brasilino Pereira dos Santos

Corregedora-Geral do Ministério Público Federal
Célia Regina Delgado

Secretária-Geral
Eliana Péres Torelly de Carvalho

PROCURADORIA REGIONAL ELEITORAL no ESTADO do RIO DE JANEIRO

Procuradora Regional Eleitoral
Neide M. C. Cardoso de Oliveira

Procurador Regional Eleitoral Substituto
Flávio de Moura Paixão Júnior

Eleições 2024:
Guia prático de investigação na internet

Realização
Procuradoria Regional Eleitoral no Estado do Rio de Janeiro

Autora

Neide M. C. Cardoso de Oliveira

Procuradora Regional Eleitoral do Estado do Rio de Janeiro. Coordenadora adjunta do Grupo de Apoio sobre Criminalidade Cibernética da Câmara Criminal do MPF e Coordenadora Regional do Grupo Especial Nacional da Função Eleitoral (GENAFE) na 2ª Região. Membro do Grupo de Enfrentamento sobre Violência Política de Gênero da Vice-PGE. Graduada pela Universidade do Estado do Rio de Janeiro (UERJ). Especialista em Direitos Humanos nas Relações de Trabalho pela UFRJ.

Índice

I) Internet

A internet é um ambiente virtual, construído sobre uma estrutura simples, onde ocorre a transferência de pacotes de dados, de uma ponta a outra, entre redes de computadores, sem que haja descriminação sobre o conteúdo do que está sendo transmitido. E essa ausência de interferência sobre o que está sendo transmitido é que garante o que chamamos de neutralidade da rede. A Resolução TSE nº 23.732/2024 não alterou a previsão já contida na Resolução TSE nº 23.610/19 (dispõe sobre a propaganda eleitoral), art. 37, inc. I, que definiu o conceito de internet como "sistema constituído de conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes".

A principal característica de qualquer ato praticado em meio virtual é que ele deixa rastro. Isso porque para que um sistema informático ou para que a internet funcione existe uma coordenação de identificadores únicos de forma que o nome e número que são digitados na barra de endereços quando fazemos uma busca, por exemplo, identificam um endereço único que permite que os computadores se encontrem, isto é, permite a difusão das informações e a entrega de dados exatamente ao destino pretendido. Isso faz com que toda a movimentação nesse meio fique registrada, permitindo ao investigador seguir a pista e identificar o autor dessa movimentação.

No entanto, como esse funcionamento implica a geração de uma quantidade gigantesca de *bits* e *bytes*, a vida útil dessas informações não é garantida, restando preservados somente os dados relevantes ao próprio sistema, a menos que haja ordem específica para tanto. Aqui está a segunda característica dos atos, sejam delituosos ou não, praticados na internet: as provas digitais, que podem identificar o usuário, são voláteis, e, por isso, é imprescindível a existência de agilidade na sua coleta.

A investigação de qualquer ato na internet implica o conhecimento acerca da lógica do sistema informático e da própria rede, que se sofistica conforme diferentes aplicações de internet ou sistemas passam a ficar disponíveis para utilização.

II) A governança da internet

É preciso fazer um pequeno parêntese para explicar como funciona a governança da internet.

A internet é regulada pela Internet Corporation for Assigned Names and Numbers –

ICANN,[1] uma entidade multissetorial, sem fins lucrativos, de âmbito internacional, onde se fazem representados governos, setor técnico e a sociedade civil, que determina os rumos da internet. No seu início, na década de 60, era utilizada para fins militares e depois para fins acadêmicos, então controlada pelo Departamento de Comércio dos Estados Unidos. Após o escândalo Snowden, de controle sobre os dados de usuários de internet pela agência americana de segurança, National Security Agency (NSA), cresceu a pressão para que a ICCAN passasse ao controle de uma entidade também multissetorial, como é a natureza da internet, sem estar vinculada a nenhum governo especialmente, sendo esse o atual modelo adotado. O que importa compreender é que a ICCAN desempenha diferentes funções como o controle de nomes e domínios, funções de administração central da rede e, a função desempenhada pela IANA,[2] que é a responsável pela alocação dos *Internet Protocols* no mundo. Assim, cada região do globo recebeu um lote de IPs (*Internet Protocol*)[3] para gerir.

No Brasil, o Núcleo de Informação e Coordenação do .br (NIC.br)[4][4] é o braço executivo do Comitê Gestor da Internet no Brasil – CGI.br, entidade privada multisetorial, que controla o ".br", e é o responsável por alocar os números IP para as operadoras de telecomunicações que, por sua vez, disponibilizam um único número IP para cada conexão de internet, sendo, portanto, possível identificar o endereço a partir de onde foi feita aquela conexão.

III) O esgotamento do IPv4

No princípio, o *Internet Protocol* era composto por quatro grupos de *bytes* de 32 *bits* cada, o chamado IPv4. Porém, devido à utilização crescente da internet, com cada vez mais conexões sendo utilizadas pelo mesmo indivíduo, já que uma pessoa não representa mais somente uma conexão, mas várias, surgiu a necessidade de se dispor de mais números de Ips.

Uma só pessoa pode estar logada ao mesmo tempo no aparelho celular, no *tablet*, no *notebook*, no aparelho de TV e em uma infinidade de outros aparelhos, que apontam para o desenvolvimento da Internet das Coisas (IoT, Internet of Things), e, por isso, ocorreu o esgotamento do modelo IPv4.

Atualmente, muitos países (todos os desenvolvidos) já migraram para o IPv6: número de

---

1 Disponível em: http://archive.icann.org/tr/portuguese.html

2 IANA – Internet Assigned Numbers Authority

3 Res. TSE 23.610/2019, art. 37, inc. III - Endereço de protocolo de internet (endereço IP): o código numérico ou alfanumérico atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais.

4 No Brasil, o NIC.br – é o braço executivo do Comitê Gestor da Internet do Brasil – CGI.br, e é o responsável por alocar os números IP para as operadoras de telefonia que, dentre o lote de IPs a ela destinado, disponibiliza um único número IP para cada conexão de internet que algum dos seus clientes faça. A identificação do IP nessa etapa vai identificar o usuário titular daquela linha telefônica ou de banda larga, seus dados cadastrais como endereço residencial, que as companhias telefônicas ou outras têm justamente para realizarem a cobrança de seus serviços.

Internet Protocol com oito grupos de *bytes* de 4 dígitos hexadecimais e 128 *bits*, cada (o quádruplo do IPv4), o que aumentou consideravelmente as possibilidades de conexões à rede.

O que temos, atualmente, no Brasil, é a seguinte situação: os provedores de aplicações de internet já migraram para o IPv6, mas os provedores de conexão, no Brasil, aqueles que dão o acesso à internet, estão em fase de implantação do IPv6.

A falta de IPs disponíveis para conexões à internet, aliada ao alto custo para a implementação do IPv6, fez com que as operadoras brasileiras de telefonia passassem a utilizar, a partir de janeiro de 2015 (com o fim dos endereços IPs, na versão 4 - IPv4, brasileiros), o sistema conhecido como CGNAT-44: um sistema no qual um mesmo IP pode ser compartilhado por muitos usuários simultaneamente. Seria mais ou menos como utilizar um filtro de linha, com diferentes usuários se plugando nas tomadas/entradas de um mesmo IP.

Para a identificação unívoca do usuário seria necessário que cada "tomada" fosse identificado, isto é, cada porta lógica (porta de origem) - mais um dado identificado por números, precisaria ser guardado tanto pelos provedores de conexão à internet, quanto pelos provedores de aplicações de internet, além do número de IP, data e hora, o que demanda mais investimento.

A consequência disso é que, embora os provedores de conexão de internet estejam avançando na implementação do IPv6, a maioria deles permanece utilizando o sistema NAT 44, pelo menos na telefonia móvel, e muitas investigações que dependiam somente da informação referente àquelas conexões efetuadas por meio do NAT 44 (os dados cadastrais de usuário do titular dos serviços da operadora) acabaram ficando sem solução, porque, eventualmente, o provedor de conexão informa que vários (centenas/milhares) clientes seus utilizaram aquele mesmo número de IP, na data e horário requisitados.

Uma forma de contornar esse problema e vem sendo utilizada é ampliar o período da investigação no tempo. Por exemplo, se está investigando 4 postagens de um usuário, o investigador pede todos os *logs* de acesso, em determinado período. E a resposta veio com diferentes IPs em datas e horas diferentes, no período solicitado. E todos esses IPs são IPv4, foram utilizados por mais de um usuário ao mesmo tempo, então se são 4 postagens, pode se pedir todos os IPs de conexão dessas postagens, em um período de tempo maior (se antes tinha pedido só dos últimos 6 meses, pede de um ano), se se tiver sorte, só um endereço IP vai aparecer nas 4 listas, um IPv6 (para o qual não existiu compartilhamento), que é o do investigado.

Indico *links* de vídeos explicativos produzidos pelo NIC.br, que dão uma explicação didática sobre o funcionamento da internet.[5]

[5] Os vídeos mais importantes são o primeiro, sobre o Protocolo IP, e o quarto sobre Governança da Internet: 1. Como funciona a internet? Parte 1: O Protocolo IP https://www.youtube.com/watch?v=HNQD0qJ0TC4 ; 2.Como funciona a internet? Parte 2: Sistemas Autônomos https://www.youtube.com/watch?v=C5qNAT_j63M&t=41s ; 3. Como funciona a internet? Parte 3: DNS https://www.youtube.com/watch?v=ACGuo26MswI; 4. Como funciona a internet? Parte 4: Governança da Internet https://www.youtube.com/watch?v=ZYsjMEISR6E

IV) Marco Civil da Internet

Antes da publicação do Marco Civil da Internet, as alterações da Lei nº 9.613/1998 (Lei da lavagem de dinheiro) introduzidas pela Lei nº 12.683/2012 trouxeram no artigo 17-B a possibilidade de que a autoridade policial e o Ministério Público tivessem acesso aos dados cadastrais de um investigado, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de intemet e pelas administradoras de cartão de crédito, fazendo a primeira menção, portanto, aos dados mantidos pelos provedores de internet.

Porém, a grande inovação veio com a promulgação do Marco Civil da Internet, Lei nº 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e, em seu bojo, regulou as questões processuais referentes à preservação das provas digitais pelos provedores, disciplinando o acesso a elas.

Assim, o artigo 11 do Marco Civil[6] estabelece que será aplicada a legislação brasileira sempre que alguma das condutas referentes ao manuseio de dados ou comunicações por provedores de conexão e de aplicação de internet ocorrer em Território nacional. E seu § 2º esclarece que o *caput* se aplica mesmo que as atividades descritas sejam realizadas por pessoa jurídica sediada no exterior quando o serviço for ofertado ao público brasileiro ou ao menos uma integrante do mesmo grupo econômico possuir estabelecimento no Brasil.

O artigo 13 do Marco Civil trata da guarda e retenção dos registros de conexão à internet, que devem ser mantidos em sigilo e em ambiente controlado e de segurança, pelo prazo de um ano, podendo o Ministério Público ou as autoridades policial e administrativa requererem cautelarmente que a guarda e preservação se dê por período superior a um ano, cabendo à autoridade requerente providenciar a autorização judicial para acesso aos dados dentro de 60 dias.

O artigo 15 do Marco Civil estabelece o dever de guarda e retenção dos registros de acesso a aplicações de internet, sob sigilo e em ambiente controlado e de segurança, pelo prazo de seis meses, também sendo facultado ao Ministério Público e às autoridades policial e administrativa requererem, cautelarmente, a preservação dos registros de acesso a aplicações por prazo superior,

---

[6] Lei nº 12.695/2014, Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. (...) § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

desde que providenciem o ingresso do pedido de autorização judicial para o acesso aos dados no mesmo prazo de 60 dias.

A importância do Marco Civil, na questão das provas digitais, está em ser a primeira lei brasileira a prever prazos de retenção e possibilidade de preservação de registros de conexão e de acesso à aplicação de internet, que são, ao mesmo tempo, meios investigativos para se buscar a identificação do usuário e elementos probatórios para embasar a conclusão da individualização pessoal da conduta.

IV.1) Conceitos

O Marco Civil da Internet traz, em seu artigo 5º, conceitos básicos como a definição de **endereço de protocolo de internet (endereço IP - *Internet Protocol Address*)[7],** código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais (inciso III); definição do que é **registro de conexão[8]:** conjunto de informações referentes à data e hora de início e término de uma conexão à internet, mediante a atribuição ou autenticação de um endereço IP (inciso VI); definição do que é **registro de acesso a aplicações de internet[9]:** o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP (inciso VIII).

O artigo 10, §1º estabelece que as informações dos provedores de conexão e de aplicação somente poderão ser obtidas por ordem judicial. Mas para autoridades, o acesso a dados cadastrais dispensa a ordem judicial.

Neste ponto é de se destacar que o regulamento do Marco Civil da Internet, Decreto nº 8.771, de 11 de maio de 2016, define **dados cadastrais** como filiação, endereço e qualificação pessoal (nome, prenome, estado civil e profissão). Embora as informações financeiras não constem desse rol, é pacífica a jurisprudência no sentido de que os dados de pagamento de um serviço, seja ele por meio de conta bancária ou cartão de crédito, ou outro meio, não são protegidos pelo sigilo, de forma que os provedores tanto de conexão, quanto de aplicação de internet, devem informá-los às autoridades requerentes (polícia, Ministério Público e autoridade administrativa), independentemente, de ordem judicial.

Note-se, ainda, que no art. 13, §2º, incs. I e II do Regulamento, há a obrigação de exclusão dos dados pessoais, comunicações privadas e registros de conexão e de acesso a aplicações, após atingida a finalidade de seu uso, ou o prazo legal, se não houver solicitação de preservação por

---

7 É um rótulo numérico atribuído a cada dispositivo (computador, celular, notebook, etc) conectado à Internet, justamente para identificar a máquina que fez a conexão à Internet. Observe que a identificação não é do usuário, mas do dispositivo.

8 Res. TSE 23.671/2021, Art. 37, inc. VI.

9 Res. TSE 23.671/2021, Art. 37, inc. VIII.

prazo superior (um ano para provedores de conexão e seis meses para provedores de aplicação).

IV.2) Prazos de Retenção e de Preservação

O Marco Civil da Internet previu prazos de retenção para os registros de conexão pelo período de um ano (art. 13) e de retenção pelo período de seis meses (art. 15), com a possibilidade de pedido de preservação por período superior a ser feito pela polícia, Ministério Público ou autoridade administrativa.

Não há obrigação de guarda/retenção de conteúdo, mas este pode ser objeto de pedido de preservação enquanto se obtém a ordem judicial para o seu fornecimento. Bastará a ordem judicial para afastar o sigilo e obter o conteúdo armazenado, nos termos do art. 7º, inciso III do MCI. Para o conteúdo *online*, isto é, interceptação de conteúdo em tempo real, a ordem judicial deve ser na forma da lei (Lei nº 9296/96, Lei das Interceptações Telefônicas e Telemáticas), conforme art. 7º, inc. II do MCI, observando-se, portanto, os requisitos nela previstos.

IV.3) Jurisdição

Como já explicado acima, o artigo 11 do MCI deixa claro que se aplica a legislação brasileira para qualquer operação de tratamento de dados realizada em território nacional, devendo ser respeitados os direitos à privacidade, proteção dos dados pessoais e a o sigilo das comunicações privadas e dos registros quando pelo menos um dos terminais está localizado no Brasil. Ou seja, a coleta de dados se deu a partir de uma conexão feita no território nacional, não importando que a sede da pessoa jurídica do provedor de aplicação de internet esteja no exterior, desde que o serviço esteja sendo ofertado ao público brasileiro ou pelo menos um integrante do mesmo grupo econômico possua estabelecimento no Brasil (ex.: a empresa WhatsApp Inc. por integrar o mesmo grupo econômico do Meta Plataforms, que possui representação brasileira).

Esse dispositivo vem para assegurar que os dados do público brasileiro terão asseguradas as garantias de privacidade e segurança estipulados na lei nacional. Assim, da mesma forma para o afastamento do sigilo desses dados deve ser observada a lei brasileira, emprestando segurança quanto ao regime de proteção desses dados.

Note-se que a hipótese de oferta de serviços ao público brasileiro, sem que haja sede ou filial da empresa em Território nacional, também determina a jurisdição brasileira, embora possa haver problemas para dar eficácia às decisões direcionadas a essas empresas.

Para se determinar se a oferta de serviços é direcionada ao público brasileiro, aplica se o

targeting test da doutrina americana, verificando-se se os serviços são oferecidos na língua portuguesa; se é possível adquirir produtos e serviços na moeda local; e se os dados recolhidos no País são utilizados para fazer publicidade direcionada a esse mesmo público. Assim, nesses casos de ofertas de serviços ao público brasileiro, esses provedores de aplicação de internet também devem cumprir a legislação brasileira.

IV.4) Sanções: Art. 12 MCI pelo Descumprimento dos Arts. 10 e 11, MCI

As sanções estipuladas para o descumprimento dos arts. 10 e 11 do MCI, sem prejuízo das demais sanções cíveis, criminais ou administrativas cabíveis, são:

> I – advertência, com indicação de prazo para adoção de medidas corretivas;
> II – multa de até 10% do faturamento do grupo econômico no Brasil, observando-se a condição econômica do infrator e avaliando-se a proporcionalidade entre a gravidade da fala e a intensidade da sanção;
> III – suspensão temporária das atividades que envolvam os atos previstos no artigo 11;
> IV – interrupção das atividades que envolvam os atos previstos no art. 11.

Logo, há o dever legal da empresa de prestar informações requisitadas por ordem judicial (brasileira), notando-se que a multa cominatória (art. 12, parágrafo único): estabelece a solidariedade da empresa estrangeira pelo pagamento da multa fixada a sua filial, sucursal ou escritório ou estabelecimento situado no País.

V) Detecção de Desinformação

Boatos diversos – a checagem de informações sobre qualquer notícia passa por duas etapas: uma com a análise dos elementos da notícia e outra com a verificação do conteúdo em fontes seguras de informação.

Na primeira etapa, ao receber a notícia, verificar a linguagem usada e a aparência da mensagem. Erros de ortografia e de português, e logos de empresas conhecidas com aparência dos originais, mas com cores/fontes diversas ou outras imperfeições.

Ultrapassada a primeira etapa, consultar sites de grandes meios de comunicação e fontes oficiais relacionadas ao conteúdo da notícia (ex. se for sobre o processo eleitoral, o site do TSE etc) para apurar se a notícia é realmente verdadeira.

Em 2024, o TSE criou o Sistema de alertas de Desinformação Eleitoral – SIADE, cuja ferramenta permite qualquer pessoa indicar fatos incorretos ou descontextualizados e que podem

causar danos à eleição e à integridade do processo eleitoral[10].

Os seguintes endereços de grandes grupos de comunicação publicam checagem periódicas de notícias:

- Portal TSE "Fato ou Boato": https://www.justicaeleitoral.jus.br/fato-ou-boato
- Agência Lupa/Grupo Folha: https://piaui.folha.uol.com.br/lupa/tag/fake-news/
- Agência Estado: https://politica.estadao.com.br/blogs/estadao-verifica/
- Grupo Globo: https://g1.globo.com/fato-ou-fake/

Além disso, **o WhatsApp** disponibilizou consultas diretamente do aplicativo para checagem da veracidade de notícias no *Google* (https://www.ajudandroid.com.br/whatsapp-permite-pesquisar-google-conferir informacoes/?amp). Para mais informações, consulte: https://cartilha.cert.br/fasciculos/boatos/fasciculo boatos.pdf.

Golpes por meio de promoções – além de notícias falsas, podem surgir àquelas referentes a promoções falsas, no período eleitoral (ex. oferecimento de alguma vantagem ao eleitor). Caso haja o recebimento de *links* para promoções, aja da seguinte forma:

· faça a checagem mencionada no item anterior;

· verifique com o remetente do link se ele conhece a origem e pode atestar a procedência. Desconfie de correntes e links que pedem o compartilhamento com mais usuários;

· caso o link refira-se a uma empresa, verifique no site oficial da empresa se há alguma informação sobre a promoção ou a notícia;

· não forneça, em nenhuma hipótese, dados bancários ou senhas. Tanto bancos como empresas informam que não pedem senhas pessoais de seus clientes.

Cartão de crédito – fornecer o número do cartão só se estiver comprando realmente algo e em lojas online confiáveis.

Não havendo confirmação por fontes seguras de que o link é verdadeiro, tratá-lo como falso: não fornecer informações pessoais e, principalmente, não compartilhar.

Dica: colocar a palavra golpe junto de eventual promoção em sites de busca para ver se outras pessoas já sofreram o mesmo golpe.

Instalação de aplicativos que prometem informações sobre determinado assunto – procure sempre o produto/empresa na loja on-line oficiais do seu sistema operacional (*Android* ou *IOS*) ou de desenvolvedores. Antes de instalar, pesquise na Internet sobre o aplicativo. Ao instalar

[10] Disponível em: https://www.tse.jus.br/eleicoes/sistema-de-alertas

aplicativos, evite fornecer dados e permissões desnecessários.

V.1) Uso de Inteligência Artificial na Propaganda eleitoral

O TSE, por meio da Resolução nº 23732/2024, introduziu na Resolução nº 23.610/2019 a novidade sobre o uso de inteligência artificial na propaganda eleitoral. Ou seja, a possibilidade de se utilizar sistema informatizado, como programas/ferramentas de inteligência artificial, também denominado conteúdo sintético, para criar, substituir ou alterar, a imagem ou voz do candidato, em sua propaganda eleitoral. Vedado, por óbvio, a utilização desse tipo de conteúdo fabricado ou manipulado para propagar desinformação (noticiar fatos inverídicos ou descontextualizados), com *potencial de causar danos ao equilíbrio do pleito ou integridade do processo eleitoral*; assim como para *criar, substituir ou alterar imagem ou voz de pessoa viva, falecida ou fictícia*, seja para prejudicar ou mesmo favorecer a candidatura, e que caracterizaria a deepfake[11]. Cabe transcrever os respectivos artigos da Resolução TSE nº 23.610/2019, *in verbis*:

> Art. 9º-B. A utilização na propaganda eleitoral, em qualquer modalidade, de conteúdo sintético multimídia gerado por meio de inteligência artificial para criar, substituir, omitir, mesclar ou alterar a velocidade ou sobrepor imagens ou sons impõe ao responsável pela propaganda o dever de informar, de modo explícito, destacado e acessível que o conteúdo foi fabricado ou manipulado e a tecnologia utilizada.
>
> § 3º O submete-se ao disposto no caput deste artigo, candidata ou outra pessoa real.
>
> Art. 9º-C É vedada a utilização, na propaganda eleitoral, qualquer que seja sua forma ou modalidade, de conteúdo fabricado ou manipulado para difundir fatos notoriamente inverídicos ou descontextualizados com potencial para causar danos ao equilíbrio do pleito ou à integridade do processo eleitoral.
> § 1º proibido o uso, para prejudicar ou para favorecer candidatura, de conteúdo sintético para criar, substituir ou alterar imagem ou voz de pessoa viva, falecida ou fictícia.
>
> Art. 9º-F. No caso de a propaganda eleitoral na internet veicular fatos notoriamente inverídicos ou gravemente descontextualizados sobre o sistema eletrônico de votação, o processo eleitoral ou a Justiça Eleitoral, as juízas e os juízes mencionados no art. 8º desta Resolução ficarão vinculados, no exercício do poder de polícia e nas representações, às decisões colegiadas do Tribunal Superior Eleitoral sobre a mesma matéria, nas quais tenha sido determinada a remoção ou a manutenção de conteúdos idênticos.

[11] Deepfake é uma amálgama de "deep learning" (aprendizagem profunda em inglês) e fake (falso), técnica de síntese de imagens ou sons humanos baseada em técnicas de inteligência artificial. Disponível em: https://pt.m.wikipedia.org/wiki/Deepfake#:~:text=Deepfake%2C%20uma%20am%C3%A1lgama%20de%20%22deep,em%20t%C3%A9cnicas%20de%20intelig%C3%AAncia%20artificial

VI) Impulsionamento de conteúdo

É vedada qualquer tipo de propaganda eleitoral paga na internet, salvo no caso de **impulsionamento de conteúdos,** expressão adotada pelo modelo de negócios do provedor de aplicação Facebook, que acabou sendo incorporada à nossa legislação (LE, art.57-C, caput*;* Res. TSE nº 23610/19, art. 29; art. 37, inc. XIV e PLS 2630/20 – Combate às Fake News). Na verdade, trata-se de divulgação contratada. Suas características:

> 1) é um serviço oferecido na internet (como pelas aplicações: Facebook e Instagram, além das ferramentas de buscas, como os *sites* buscadores: Google e Yahoo);
> 2) só pode ser contratado exclusivamente por partidos, federações, coligações, candidata(o)s e seus representantes;
> 3) é um serviço pago, e que deve ser identificado de forma inequívoca como tal. Pode se usar hiperlink, que direcione para o CNPJ da campanha. E a identificação deve ser mantida ao se compartilhar ou encaminhar o conteúdo impulsionado (§§ 5º; 6º, 7º);
> 4) só pode ser contratado para promover ou beneficiar candidatura (vedada a propaganda negativa).

O impulsionamento deverá ser contratado diretamente com provedor da aplicação de internet com sede e foro no País, ou de sua filial, sucursal, escritório, estabelecimento ou representante legalmente estabelecido no país, justamente, para caso ocorra qualquer irregularidade naquele ambiente esteja sob alcance da Justiça Eleitoral, que poderá oficiar ao provedor de aplicação contratado. E, também, apenas pode ser contratado o serviço de impulsionamento com o fim de promover ou beneficiar candidatos ou suas agremiações, vedada a realização de propaganda negativa (LE, art. 57-C, § 3º e Res. TSE nº 23.610/19, art. 29, § 3º).

É vedada a utilização de impulsionamento de conteúdo e ferramentas digitais não disponibilizadas pelo provedor da aplicação de internet, ainda que gratuitas, para alterar o teor ou a repercussão de propaganda eleitoral, tanto próprios quanto de terceiros (LE, art. 57-B, § 3º e Res. TSE nº 23.610/19, art. 28, § 3º). Assim como, também é vedada a utilização de impulsionamento de conteúdo e ferramentas digitais não disponibilizadas pelo provedor da aplicação de internet, ainda que gratuitas, para alterar o teor ou a repercussão de propaganda eleitoral, tanto próprios quanto de terceiros (LE, art. 57-B, § 3º e Res. TSE nº 23.610/19, art. 28, § 3º).

Uma ótima fonte de pesquisa sobre os impulsionamentos contratados, pelas candidatas

(os), partidos, federações ou coligações, é a consulta que pode ser realizada na **Biblioteca de anúncios de natureza política e eleitoral** das aplicações Facebook/Instagram (https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=BR&media_type=all), cujos dados ficam disponíveis por sete anos. Informam o alcance da publicidade (quantas vezes apareceu); o período contratado; valor gasto em média e para quem os anúncios foram contratados (detalhamento por idade e gênero das pessoas).

É bom saber que o provedor X (ex-Twitter) não oferece serviço de impulsionamento com fins eleitorais (inclusive, proíbe globalmente), assim como o Google anunciou para as eleições 2024 que não disponibilizaria serviço de impulsionamento em suas plataformas (Youtube e serviço de busca)

VII) Provas Digitais

As inovações tecnológicas tornaram essencial a preocupação com as provas digitais, pois não somente os crimes tipicamente digitais, mas todos os ilícitos praticados na internet deixam pistas digitais, e essas pistas são essenciais para a elucidação dos ilícitos.

Qualquer crime comum ou ilícito eleitoral, por exemplo, pode vir a ser solucionado com o auxílio de provas digitais. *E-mails* recebidos e enviados; pesquisas de busca sobre determinados temas na internet*;* documentos armazenados em meio digital; entre outros, podem vir a ser pistas e provas acerca do cometimento de ilícitos.

VII.1) Características

As provas digitais apresentam características intrínsecas que as tornam aptas à verificação. Elas deixam marcas, ou seja, são o próprio rastro das condutas praticadas no mundo virtual, pois toda atividade nesse ambiente deixa rastro. Pode ser verificada. Uma vez que uma informação é registrada na Internet ou em algum dispositivo informático, essa informação pode ser recuperada dentro de um certo período, mesmo que seja apagada. Assim, a perícia forense tem condição de analisar as provas digitais para verificar sua autenticidade e integridade, podendo assim determinar seu grau de confiabilidade.

Como esclarecido em estudo específico sobre o assunto[10], as provas digitais possuem requisitos específicos de validade que precisam ser observados em qualquer transferência de

informações, seja ela interna ou transnacional. Deve ser primeiramente admissível, isto é, como qualquer outra prova, sua aquisição deve ser correta para que possa ser admissível. O segundo requisito, desta vez, específico à sua natureza, é que sua coleta e preservação devem ser realizadas observando-se os princípios da ciência computacional a fim de garantir sua **autenticidade** e **integridade**. Estas características podem ser verificadas na análise das provas digitais pela perícia forense que poderá determinar então o seu grau de **confiabilidade**. Dessa forma, a prova somente será convincente, em juízo, se bem esclarecido no laudo pericial o grau de confiabilidade dessa prova, pois na maior parte das vezes, é a prova determinante para a indicação de autoria do fato, delituoso ou não.

A perícia forense terá papel fundamental, portanto, na análise dessas provas, sendo in dispensável que o perito, ou agente apto, acompanhe as ações de busca e apreensão para garantir a correta coleta das provas digitais a fim de que nenhuma informação seja perdida ou corrompida.

Outro aspecto fundamental a ser observado é o tempo na obtenção dessas evidências, já que a prova digital é também extremamente volátil.

No dizer de Araújo Cintra, Ada Pelegrini e Cândido Dinamarco, *a prova constitui, pois, o instrumento por meio do qual se forma a convicção do juiz a respeito da ocorrência ou inocorrência dos fatos controvertidos no processo*[12]

Dentre os meios de prova tradicionais – exame de corpo de delito e perícias em geral, interrogatório, confissão, depoimento do ofendido, prova testemunhal, reconhecimento de pessoas e coisas, acareação, prova documental, prova indiciária e busca e apreensão – podemos dizer que praticamente todos eles sofreram alguma modificação ou influência em virtude das novas tecnologias.

Com a migração dos ilícitos para o meio virtual, os meios de prova, que passaram a merecer especial atenção dadas as peculiaridades da tecnologia digital, são a prova documental, a prova pericial e a busca e apreensão.

Quando falamos em ilícitos praticados pela internet, necessariamente serão examinados registros, os quais são considerados documentos. E mesmo para os crimes em geral, como já pontuado, as evidências digitais se fazem presentes no dia a dia, pois os documentos assumiram a forma digitalizada.

Documento é *toda base materialmente disposta a concentrar e expressar um pensamento, uma ideia ou qualquer manifestação de vontade do ser humano, que sirva para expressar e provar um fato ou acontecimento juridicamente relevante. São documentos: escritos, fotos, fitas de vídeo e som, desenhos, esquemas, gravura, disquetes, CDs, DVDs, pen drives, e-mails, entre outros.*

[12] CINTRA, Antônio Carlos de Araújo. Teoria Geral do Processo. Antônio Carlos de Araújo Cintra, Ada Pellegrini Grinover, Cândido R. Dinamarco. Editora Revista dos Tribunais. 8ªedição, revista e ampliada. 1991.

Trata-se de uma visão moderna e evolutiva do tradicional conceito de documento – simples escrito em papel – tendo em vista o avanço da tecnologia[13].

A Lei nº 11.419/2006, que regula os processos eletrônicos, ao dispor sobre a informa tização do processo judicial, prevê no seu artigo 11 que os documentos produzidos eletronica mente e juntados aos processos eletrônicos com garantia de origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais.

Essa disposição legal demonstra a assertiva de Nucci de que o conceito de documento não se restringe mais ao papel, tendo sido estendido aos registros digitais. As provas digitais possuem alto grau de volatilidade, sendo facilmente manipuláveis. Elas podem sofrer alteração pelo usuário ao tentar, este, apagar os rastros digitais do ilícito que cometeu. O próprio investigador pode, inadvertidamente, alterar as evidências digitais pela manipulação inadequada destas durante as etapas de aquisição e análise. A partir dessa assertiva, a perícia pode ser necessária para comprovar a autenticidade do documento digital, que pode ser evidência de um ilícito eleitoral, praticado por meio dos sistemas informatizados ou Internet, ou que possui associado a si evidências com registro digital.

As provas digitais possuem determinadas características que devem ser observadas no seu tratamento em geral. A alta volatilidade já mencionada, que possibilita fácil alteração da prova, recomenda atenção e verificação da autenticidade por meio das técnicas periciais. Por isso, as provas que se encontram em poder dos provedores de aplicação devem ser objeto de preservação imediata, tão logo os investigadores dela tenham conhecimento, pois mesmo que obedecidos os prazos de retenção, este pode estar findando. Logo, a primeira coisa a se fazer é pedir a preservação da prova para que esteja íntegra quando for obtida a necessária ordem judicial para sua entrega.

Já quando são encontradas diretamente, sem a intermediação dos provedores, todo cuidado deve ser tomado para que a integridade e autenticidade sejam asseguradas. O fato de poderem ser duplicadas sem maiores problemas vem como uma vantagem para a coleta e análise das provas digitais, pois dessa forma, pode-se preservar a prova original, analisando se a "cópia", não se correndo o risco de, na própria análise ocorrer algum tipo de adulteração acidental. A facilidade de duplicação também vem a ser característica relevante, na medida em que facilita aos peritos a coleta de grande quantidade de material a ser analisado. Em uma apreensão de grande quantidade de equipamentos ou em havendo equipamentos de dimensões muito grandes, não é necessário removê-los do local, bastando fazer o espelhamento do *hardware* para que se proceda à análise do conteúdo.

Outro fator que aponta vantagem aos investigadores do ilícito digital é a intangibilidade da evidência digital, tornando a sua destruição mais difícil. Devido à característica inerente dos

13 NUCCI, Guilherme de Souza. *Provas no processo penal*. São Paulo: Editora Revista dos Tribunais, 2009.

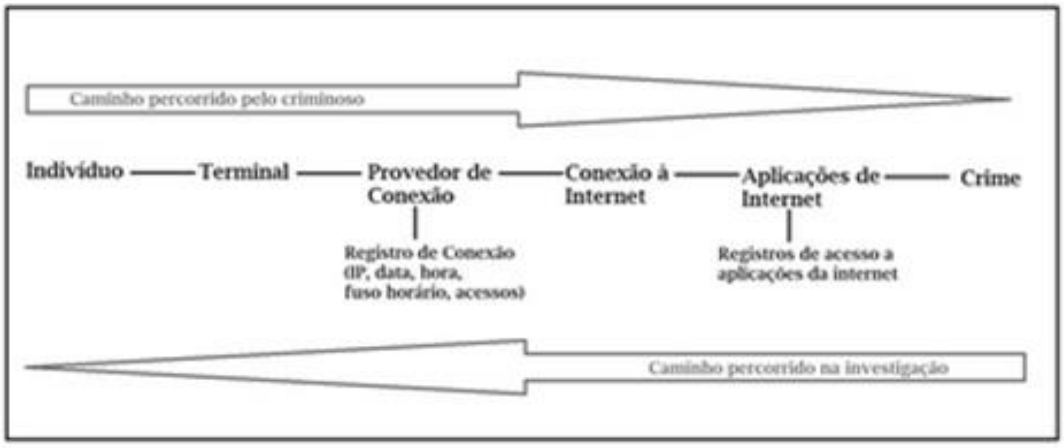
equipamentos informáticos, é possível, por meio da prova pericial, recuperar os dados apagados, mesmo em datas posteriores ao evento delituoso.

A manipulação da prova digital deve ser adequada também visando a obtenção de metadados, pois estes a permeiam, sendo facilmente coletados na perícia e devendo ser fornecidos também pelos provedores de aplicações.

Devido à abundância de informações que é possível obter-se numa perícia de evidências digitais, o perito deve ser capaz de reduzir a quantidade de informações a fim de que estas possam ser organizadas para que seja exposto somente aquilo que é relevante para a investigação.

VIII) Roteiro de Investigação

Para a investigação de uma conduta ilícita praticada pela internet é necessário atentar se ao trajeto realizado pelo agente para a realização de tal conduta, pois o investigador realizará o caminho inverso para a identificação do usuário, conforme bem ilustram Alessandro Gonçalves Barreto e Beatriz Silveira Brasil, em seu Manual de Investigação Cibernética[14]:



Para o funcionamento da rede mundial de computadores, é necessária uma conexão à rede, que se realiza por meio de um *modem*, disponibilizado por um provedor de conexão. Esta conexão pode ser paga ou gratuita, mas implica em receber um número IP, isto é, um endereço de protocolo de internet (*Internet Protocol)* exclusivo, pelo período da conexão, para acessar a infraestrutura de rede mantida pelas empresas de telecomunicações, como as operadoras de telefonia (Claro-Net

[14] Barreto, Alessandro Gonçalves; Brasil, Beatriz Silveira. *Manual de Investigação Cibernética: À luz do Marco Civil da Internet*. Brasport.

Virtua; OI-Telemar; Tim; Vivo; etc). Esse IP pode ser utilizado pelo usuário para acessar serviços mantidos pelos provedores de aplicação de internet (site, Facebook; Instagram; WhatsApp; YouTube; X; TikTok; email; etc.).

Importante: um mesmo número de IP pode ser utilizado por vários usuários durante determinado período, mas apenas por um único usuário em um dado dia e hora[15]. Por isso, é essencial que o IP venha acompanhado da data e horário exatos da conexão, incluindo o fuso horário, de forma a excluir outros usuários.

Em uma breve síntese, recebida uma denúncia de publicação de desinformação, com fins eleitorais, em alguma aplicação de internet (*site*; mensageiro instantâneo; rede social; *email* etc), com uma simples consulta no endereço http://registro.br (para endereços nacionais) e http://whois.icann.org (para endereços estrangeiros), é possível saber qual provedor de aplicação de internet é o responsável por aquele domínio pesquisado. O primeiro passo na investigação do ilícito deve ser o pedido de preservação de dados dos registros de acesso e *logs* de *upload* (postagem) e de acesso do usuário junto ao respectivo provedor de aplicação identificado. Os grandes provedores costumam disponibilizar portais[16] para as autoridades fazerem esse pedido. Após o pedido de preservação, cabe o ajuizamento de medida cautelar de afastamento de sigilo telemático (Res. TSE 23.610/19, art. 40 e MCI, art. 22), para que o provedor de aplicação de internet indique, mediante ordem judicial, o IP, data e hora utilizados pelo usuário investigado na conexão à internet. De posse dessas informações, outra consulta nos mesmos sítios[17] (com o número IP informado pelo provedor de aplicação), indicará qual empresa de telecomunicação é a responsável por alocar o IP pesquisado, à qual se deve dirigir o pedido de informação relativo à informação cadastral do cliente titular do serviço de conexão à internet. Essa informação será do endereço físico onde se deu a conexão de internet para a difusão/publicação do conteúdo investigado. A partir dos dados do titular do serviço, novas investigações devem ser feitas visando identificar o autor da postagem/publicação.

A seguir, será detalhado o procedimento de investigação do usuário na internet.

VIII.1) Passos da investigação: do que se trata a notícia?

Ao se tentar identificar o autor de um ilícito na internet, o que pode ser requerido pela parte

---

15 Exceção feita aos casos de uso do NAT-44, situação em que mais de um usuário está utilizando o mesmo IP no mesmo momento. Para esses casos, é preciso fazer um cruzamento de dados a partir de vários acessos com Ips diferentes para se identificar o usuário buscado.

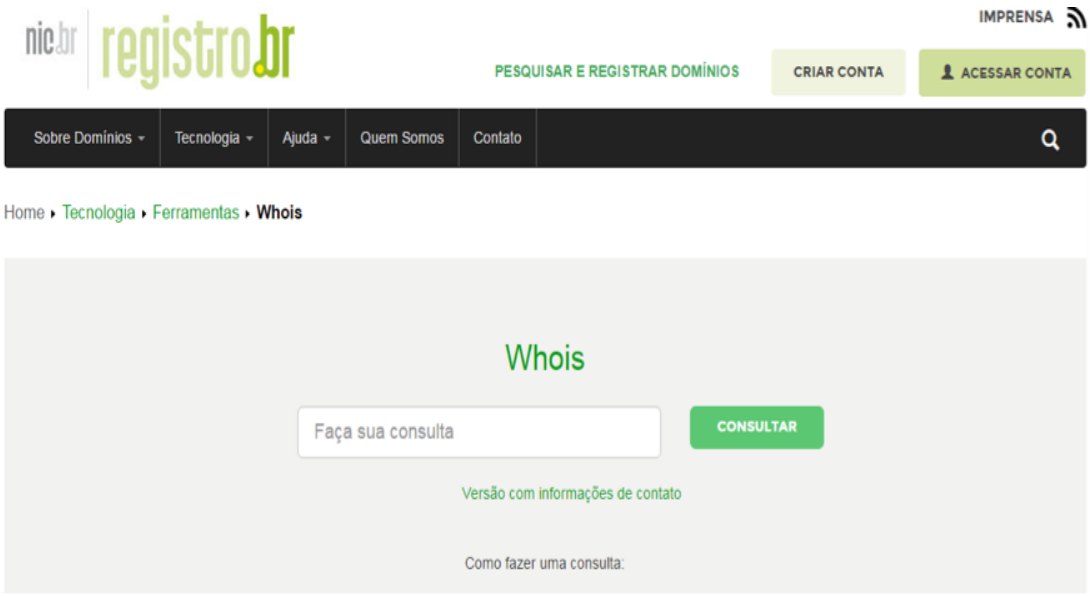
16 https://facebook.com/records (Facebook e Instagram); https://WhatsApp.com/records (WhatsApp); https://ler se.google.com (YouTube).

17 http://registro.br (para endereços nacionais) ou http://whois.icann.org (para endereços estrangeiros).

ao Juízo, em processo cível ou criminal, conforme prevê o art. 22 do MCI, reproduzido no art. 40 da Resolução TSE nº 23.610/2019, busca-se conhecer a materialidade reportada, a localização geográfica do conteúdo hospedado e finalmente o responsável pela sua publicação.

O primeiro passo para se iniciar uma investigação de um ilícito eleitoral, seja ele, civil, como a prática de abusos de poder político, econômico ou pelo uso indevido dos meios de comunicação social, via internet (art. 22 da LC 64/90) ou propaganda eleitoral irregular, pela internet; ou de natureza criminal, como a divulgação de uma notícia sabidamente falsa (art. 326-A, caput, do CE); contra a honra com fins eleitorais (arts. 324 a 326, do CE); violência política de gênero (art.326-B, do CE); publicar desinformação sobre candidatas (os) ou partidos (art. 323, caput, do CE e art. 90, da Res TSE nº 23.610/2019, e art.57-H, §§ 1º e 2º da Lei Eleitoral), entre outros, é a identificação do que se trata a notícia, ou seja, qual aplicação, das oferecidas pelos provedores de aplicações de internet, foi utilizada e o provedor responsável por ela.

Tal informação será necessária tanto para a adoção de medidas quanto à preservação da prova quanto para a obtenção de informações acerca da autoria e materialidade do ilícito. Os serviços mais comuns oferecidos pelos provedores de aplicações à internet são a formação de redes sociais (ex: Facebook, Instagram, Twitter, Tiktok, etc); troca de mensagens instantâneas (WhatsApp, Telegram, Signal, etc); email (@gmail, hotmail, terra, etc); páginas na word wide web - www (*site*s, *blogs, fotoblogs*); fóruns de discussão (ex.: Yahoo Groups); Voip (voz sobre IP); chat (salas de bate papo); hospedagem e compartilhamento de arquivos de fotos e vídeos (exs: eMule, Aresgalaxy, Gigatribe, etc), serviços de *streaming* (YouTube, Globoplay, Amazon, etc) e o e-commerce (ex.: Mercado Livre, Paypal, etc). Essa identificação dos responsáveis pelo serviço, se não for de fácil detecção ou mesmo para a obtenção de seus endereços, pode ser feita mediante consulta no serviço: https//:www.registro.br (para endereços nacionais) ou no http://whois.icann.org (para endereços no exterior).



VII

I.2) Passos da investigação: preservação das provas (autoria e materialidade)

A prova digital é extremamente volátil, pois o usuário pode a retirar tão rápido quanto publicou na internet. Devemos garantir também a sua autenticidade, ou seja, de que a informação foi veiculada exatamente onde se está noticiando que ela foi e para assegurar sua integridade, que o manuseio dela não a alterará. Por isso, a necessidade de se obter o mais rápido possível a preservação dos dados de identificação do usuário e da própria publicação diretamente do provedor de aplicações.

Para a garantia da integralidade e da autenticidade da prova, duas medidas precisam ser imediatamente tomadas assim que se toma conhecimento da prática de ilícito: a) a coleta adequada da prova eletrônica; e b) a preservação dos dados referentes à prática de crime.

Assim que recebida a notícia da infração, é necessária a coleta da prova eletrônica (por ex.: post em rede social, site, link em mensageiro instantâneo, etc.), o procurador ou promotor deve encaminhar a notícia ao setor pericial do órgão do MPE (no MPF, às ASSPAs locais), e que dá apoio aos procuradores/promotores, em questões relacionadas às investigações na internet[18]. Ela deverá coletar adequadamente a prova utilizando ferramentas forenses (ex. Verifact, no MPF/PREs), que atestem que o material corresponde, exatamente, ao publicado, mediante a extração do código *hash*, iniciando-se, a partir daí, a cadeia de custódia.

Ao mesmo tempo, deve ser requisitado ao provedor de aplicação de internet, responsável por aquele serviço (que mantém a rede social, que hospeda o *site* etc.), a preservação dos dados

[18] ASSPA – Assessoria de Pesquisa e Análise, presente em todas as Procuradorias da República e Procuradorias Regionais da República, integrante da estrutura da Secretaria de Perícia, Pesquisa e Análise (SPPEA), da PGR.

cadastrais e dos *logs* (registros) de acesso referente ao ilícito, nos termos do art. 15, § 2º do MCI.

A notificação do provedor de aplicação de internet, responsável pelo serviço, para preservar os registros de acesso às aplicações, pode ser feita pelo membro do MP ou autoridade policial, sem ordem judicial, porque se está apenas solicitando que a empresa preserve os registros de acesso àquela aplicação, que poderá, posteriormente, identificar o IP utilizado para postá-la e acessá-la, mediante o envio de uma ordem judicial.

Alguns provedores de aplicações mantêm canais específicos (portais na própria Internet) para pedidos de preservação e para envio de ordens judiciais através de endereços de *e-mail* destinados às equipes montadas para responder às autoridades, criados especialmente para responder às autoridades. Em tópicos próprios, serão informados os canais de acessos dos principais provedores de aplicação, utilizados no Brasil.

Para os provedores de aplicações, que prestam serviços no País e aqui mantêm escritório, mas que não possuem um canal específico para encaminhamento de pedidos e ordens de autoridades, basta enviar um ofício físico, no qual se requer a preservação da página ou do perfil investigado.

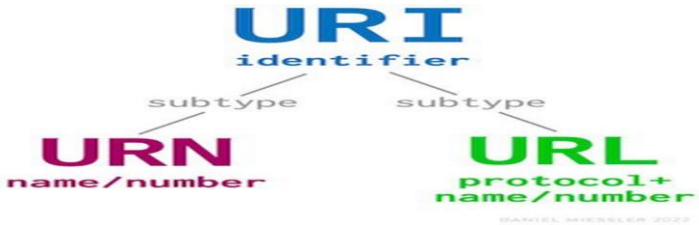
No caso de provedores de aplicações, que prestam serviços no País e aqui não mantêm representação, é possível utilizar a rede 24/7 da Polícia Federal (que atende tanto às autoridades federais como estaduais) para solicitar a preservação dos dados, por meio do endereço de e-mail cybercrime_brazil_24x7@dpf.gov.br. Para evitar a necessidade de uma cooperação internacional para obtenção de registros e dados de usuários, a Resolução TSE nº 23610/2019 sobre propaganda eleitoral, mesmo com as eventuais alterações ou acréscimos da Resolução TSE nº 23.732/2024, mantém a disposição de que seja informado no Registro de Candidatura do Candidato (RCC) ou no Documento de Registro dos Atos Partidários (DRAP) todas as contas dos partidos e candidatos (as) em provedores de aplicação de internet, justamente, para que sejam alcançadas pela Justiça Eleitoral (Res TSE nº 23610/2019, art. 28, § 1º). Assim como os provedores de aplicação à internet devem informar seus endereços eletrônicos de contato como de mensageria instantânea ou e-mail (Res TSE nº 23.672/2021, art. 10) para recebimento de ofícios, notificações e intimações. Tudo porque a celeridade do processo eleitoral não comporta o trâmite de eventual pedido de cooperação jurídica internacional, que não se cumpre em menos de seis meses, demorando em média um ano ou mais, quando se trata da obtenção de dados ou conteúdo digital.

É importante a correta identificação por meio do endereço na *web*, a **URL[19] ou URI[20] ou**

[19] URL (Uniform Resource Locator) é a forma padronizada de representação de diferentes documentos, mídias e serviços de rede na Internet, que identifica de forma completa cada documento com um endereço único. Ex. www.uol.com.br/serviços.php.

[20] URI – Uniforme Resource Identifier (Identificador de Recursos Uniforme), identifica certo conteúdo na internet, mas lcoalizadores também identificam certo conteúdo na internet, e as URLs e URNs são subconjuntos do

URN[21] ou ID[22] do perfil, de um grupo; de um vídeo etc.[23], a fim de que a preservação seja feita corretamente, tanto do conteúdo quanto dos dados cadastrais e dados associados a essa página ou perfil, os chamados metadados. Em tópico próprio, será informado como reconhecer a URL ou ID dos principais provedores de aplicação.



A URI (Uniforme Resource Identifier, ou seja, Identificador de Recursos Uniforme) identifica certo conteúdo na internet, mas localizadores como a URL também identificam certo conteúdo na internet de forma mais detalhada. Mas as URLs e URNs são subconjuntos do conjunto de URIs. Ex.: www.prerj.mpf.mp.br (identifica a página, mas sem o meio do protocolo – https:// - pelo qual também pode ser acessado e integra uma URL.

A URL (Uniforme Resource Locator, ou seja, Localizador Recursos Uniforme) é o padrão mais utilizado e citado como de uso preferencial em artigos da Resolução TSE nº 23610/2019, como o art. 38, § 4º (no caso de remoção de conteúdo que deve ser identificado pela sua URL, se não for possível pela URI ou URN). É uma combinação única de letras, números e/ou caracteres, que localiza certo conteúdo na internet de forma precisa e com o endereço completo. Ex.: https://www.prerj.mpf.mp.br/denuncia-de-ilicitos-na-internet.

URN (Uniforme Resource Name, ou seja, Nomes de Recursos Uniforme) é um recurso de internet com um nome estático. Ex.: prerj.mpf.mp.br.

E os metadados são os dados muito importantes para a investigação pois, se corretamente analisados e associados, podem trazer informações relevantes acerca da autoria do ilícito.

---

conjunto de URIs. EX.: www.prerj.mp.f.mp.br (identifica a página, mas sem o meio do protocolo <https://> pelo qual também pode ser acessado, como indica a URL).

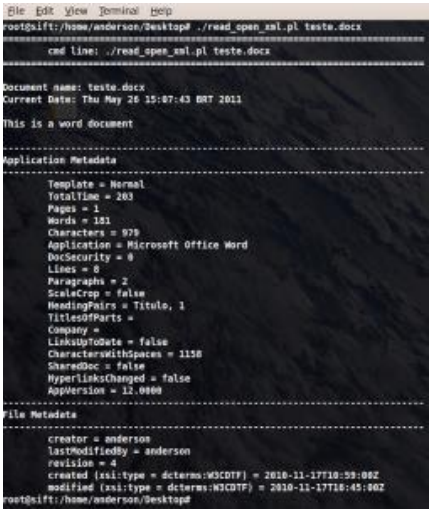
21 URN – Uniforme Resource Name, é um recurso da internet comum nome estático. Ex.: prerj.mpf.mp.br.

22 ID (Identificação ou user name), que é a identificação do usuário ou mais conhecido como Código de Usuário.

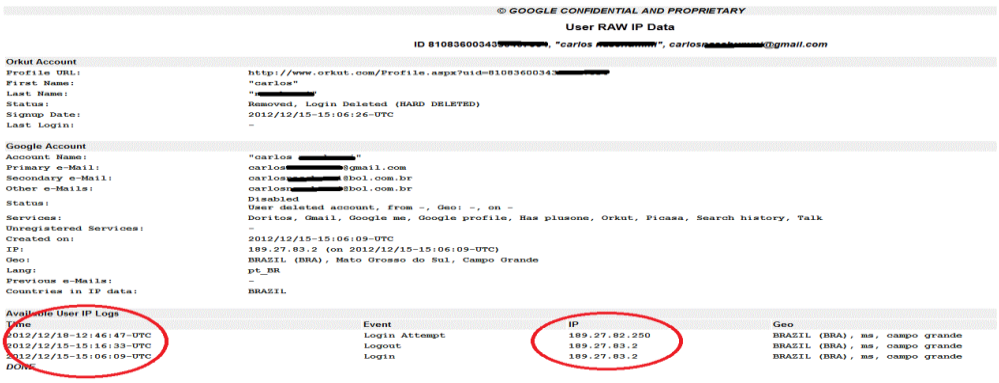
23 No caso de denunciante usar Facebook, veja o exemplo de uma URL de perfil: www.facebook.com/barackobama; se o uso do Facebook foi pelo celular, precisa clicar no menu do aplicativo (3 pontinhos) e escolher a opção "copiar a URL". Às vezes, ao invés do nome, pode aparecer o ID, veja o exemplo de URL de um GRUPO com ID: https://www.facebook.com/groups/982034701835686/. Exemplo de URL com vídeo no Facebook: www.facebook.com/BBB18RedeGlobo2018/videos/199872690605072/
No Youtube, podemos identificar URLs de CANAL: https://www.youtube.com/channel/UClu474HMt895mVxZdlIHXEA
Ou a URL de um vídeo específico: https://www.youtube.com/whatch/v=2y-5hfZWADI

Metadados de uma imagem: dados de GPS de onde a imagem foi tirada; qual o tipo de máquina; data e hora.

Metadados de documento: data e hora da criação do documento e última modificação.



Metadados de comunicação: data e hora em que o usuário se comunicou com outros usuários e IPs utilizados; localização do usuário enquanto utiliza o serviço.



Muitas vezes, o conteúdo investigado ainda está disponível na *web*, podendo ser coletado por um técnico em informática ou agente treinado para tal, que pode certificar a coleta da prova

por meio da geração do código hash[24], devendo ser um agente público.

É muito importante que a cadeia de custódia da prova não seja quebrada, de forma que sua integridade se mantenha, garantindo sua autenticidade. De acordo com o Marco Civil da Internet, os provedores de aplicação à internet, que prestam serviços no Brasil, devem reter os registros de acesso às suas aplicações por seis meses. Porém, quando recebemos a notícia de um ilícito, não sabemos exatamente quanto tempo de retenção resta, de forma que sempre deve ser pedida a preservação dos dados e do conteúdo pretendido até que se consiga a ordem judicial para sua obtenção.

VIII.3) Passos da investigação: pedido de retirada de conteúdo

Como regra geral, o MCI apenas permite a retirada de conteúdo mediante ordem judicial, que analisará a natureza do conteúdo, reputando-o ilícito ou não, de forma que os provedores de aplicações de internet não serão responsabilizados pelo conteúdo gerado por terceiros, ao qual dão suporte, sem que haja ordem judicial específica determinando a remoção desse conteúdo, nos termos do art. 19 do MCI. Esse dispositivo foi reproduzido na Resolução TSE nº 23.610/2019, art. 38.

A Resolução TSE nº 23.610/2019, art. 7º, § 1º, foi expressa em não admitir o exercício do poder de polícia da propaganda quando se tratar de controle de conteúdo postado na Internet. Nesses casos, será sempre necessária a provocação do juízo por parte de candidato, Partido ou MPE. Permanece o poder de polícia do juízo da propaganda nos casos em que a irregularidade não estiver no conteúdo, mas na forma ou meio da veiculação.

Entretanto, há três exceções que permitem a retirada de conteúdo imediatamente, sem ordem judicial, mediante contato direto com o provedor.

A primeira exceção diz respeito ao descumprimento de normas contidas nos termos de uso dos provedores de aplicação/conteúdo. Vários provedores, incluindo Facebook, Google e Twitter, possuem provimentos específicos, em seus termos de uso, para exclusão de conteúdo danoso, inclusive aquele com informações deturpadas.

A segunda exceção refere-se à prática de crime: quando a plataforma ou o serviço são utilizados para a prática de crime, é possível pedir diretamente ao provedor responsável a exclusão

[24] A função hash é um algoritmo matemático para a criptografia, na qual ocorre uma transformação do dado (como um arquivo, senha ou informações) em um conjunto alfanumérico com comprimento fixo de caracteres." Disponível em https://www.voitto.com.br/blog/artigo/o-que-e-hash-e-como-funciona/amp. Acesso em: 6 mai. 2022.

do conteúdo criminoso. Em regra, a utilização dos serviços para a prática de crime viola os termos de serviço dos provedores, o que permite a exclusão rápida.

A terceira e última exceção é legal e está prevista no art. 21 do MCI, que permite a exclusão de conteúdo de caráter sexual publicado sem a permissão do participante após notificação do interessado, sem a necessidade de ordem judicial.

Importante: o pedido de exclusão de conteúdo, inclusive criminoso, deve ser sempre acompanhado de pedido de preservação dos dados referentes à página ou publicação, de modo que a prova não se perca. Assim, verificado conteúdo ilícito, o promotor deve pedir a preservação dos dados, como mencionado no item anterior, e depois, ou concomitantemente, a exclusão do conteúdo, mas jamais a exclusão antes de assegurada a preservação.

VIII.4) Passos da investigação: pedido de afastamento do sigilo de dados telemáticos junto ao provedor de aplicações de internet

Após o pedido de preservação e/ou de retirada de conteúdo nocivo, deve ser requerido judicialmente o **afastamento de sigilo de dados telemáticos, nos casos criminais** e **nos casos cíveis**, com base no artigo 10, §§ 1º e 2º c/c art. 22, ambos do MCI (Res. TSE 23.610/2019, arts. 39 e 40).

O primeiro pedido de quebra deve ser direcionado ao provedor de aplicação à internet, que mantém o serviço/aplicação onde foi publicado o conteúdo ilícito. Ele deve ser instruído com a prova colhida na forma mencionada nos itens anteriores, bem como a indicação clara da página/postagem investigada, com a indicação do endereço URL, URN e /ou URI.

O pedido de afastamento deve requerer que o juízo respectivo requisite do provedor de aplicação à internet responsável pelo serviço as informações de IP de criação, data e hora dos registros de postagem (*uploads*) e acessos, ao perfil/página. Também deve ser requerido que o provedor encaminhe outras informações relacionadas, como *e-mail*, nome cadastrado, *nickname* (apelido), contatos de pagamento (por ex.: número de cartão de crédito). Exemplo de uma resposta:

Em tópico próprio, constam modelos de medida cautelar de quebra de sigilo telemáticos, bem como os endereços dos principais provedores.

VIII.5) Passos da investigação: pedido de afastamento do sigilo de dados telemáticos junto ao provedor de conexão à internet

Com as informações recebidas do provedor de aplicações de internet, conforme o explanado no item anterior, incluindo o Internet Protocol – IP utilizado e a data e hora de utilização,

será possível identificar o provedor de conexão, que alocou aquele IP, e requisitar a ele as informações referentes ao usuário que se conectou na internet através desse IP na data e hora indicados (art. 10, § 3º, do MCI).

A identificação do provedor de conexão (as operadoras de telefonia ou telecomunicações, que prestam serviços disponibilizando aquele endereço de IP específico) é feita a partir de uma consulta no *site* http://registro.br ou o https//whois.icann.org (informa os endereços de IPs no exterior).

A requisição, por se tratar de meros dados cadastrais, pode ser feita diretamente ao provedor de conexão identificado, de acordo com o art. 10, § 3º, do MCI. Entretanto, ainda há questionamentos sobre a necessidade ou não de intervenção judicial, sendo conveniente que o pedido seja feito ao Juízo, de modo a afastar qualquer futura alegação de nulidade. Em tópicos próprios, constam modelos de ofício com a requisição de dados cadastrais aos provedores de conexão, bem como os endereços dos principais provedores.

O endereço de IP utilizado identifica o dispositivo informático, seja ele um terminal de computador, celular, *tablet*, etc. Não significa necessariamente que o titular dos dados cadastrais, cliente daquela operadora, é o autor do fato, que foi o usuário que se está investigando. Esse cliente identificado pode ter emprestado seu sinal de *wifi* para um amigo, ou mesmo partilhar o mesmo sinal com vizinhos (fato comum em comunidades), ou ser utilizado por qualquer outra pessoa que com ele resida ou visite. Por isso, serão necessárias outras diligências para a confirmação da autoria.

VIII.6) Passos da investigação: medida cautelar de busca e apreensão

Com a identificação do endereço de onde partiram as imagens ou mensagens investigadas, a providência seguinte, no caso de investigação criminal, é a busca e apreensão no local para confirmação da materialidade e individualização da autoria. A busca, autorizada judicialmente, permitirá apreender vestígios relacionados à prática do delito, incluindo eventual material e equipamentos empregados, que deverão ser submetidos a perícia.

Não há legislação específica para quando essa medida se destina à apuração de um ilícito praticado pela internet, por isso são utilizadas as normas referentes à busca e apreensão previstas no Código de Processo Penal (art. 240, § 1º, alínea "e" e "h").

Nada impede que a cautelar seja requerida no âmbito de um procedimento investigatório de natureza eleitoral, aplicando-se subsidiariamente às legislações processuais civil e penal.

Saliente-se que o mandado de busca e apreensão deve ser específico, elencando um rol amplo de possibilidades para a apreensão, a fim de se evitar dúvidas que possam vir a gerar

nulidades, incluindo diversos tipos de equipamentos (computadores, celulares, *tablets*, câmeras fotográficas, mídias de armazenamento etc.).

Importante: Em relação aos aparelhos celulares, que são hoje muito mais que meros telefones, mas sim computadores pessoais, que armazenam milhares de dados, a jurisprudência mudou. Em 2007, decisão do STF dizia bastar um mandado genérico para se ter acesso a todo o conteúdo de um celular apreendido. Em 2016, o STJ, no HC 51.531, decidiu ser necessária autorização específica para que os agentes de investigação tivessem acesso ao conteúdo do aparelho celular apreendido em uma prisão em flagrante. Recentemente, foi reconhecida a Repercussão Geral pelo Supremo Tribunal Federal, ao Agravo em Recurso Extraordinário ARE nº 1.042.075, em que se discute exatamente essa questão: de que para acesso ao aparelho celular apreendido, para conhecimento do registro das chamadas e da agenda de telefones, bem como das demais informações, é necessária prévia autorização judicial. Nesse quadro, de forma a evitar futura alegação de nulidade, é conveniente pedir autorização judicial para acesso de cada um dos equipamentos apreendidos, inclusive celulares e *tablets*.

Armazenamento na nuvem (*cloud computing*): armazenamento nas nuvens permite que arquivos sejam guardados em servidores remotos, instalados em local diverso de onde o equipamento deve ser apreendido. Inúmeros provedores oferecem serviços que permitem armazenamento de arquivos nas nuvens (Google, Microsoft, Apple, etc.). O armazenamento pode ocorrer em serviços destinados a isto, como Google Drive, ICloud, ou em outros serviços que oferecem espaço, como *e-mails*.

Normalmente, para acessar esses arquivos é necessário fornecer uma senha. Essa pode ser fornecida espontaneamente pelo investigado para acesso aos arquivos remotos, e nesse caso, o perito que estiver acompanhando o cumprimento da diligência de busca e apreensão, pode acessar e coletar esses arquivos e toda evidência digital relacionada a eles, de forma sincronizada.

Caso o dispositivo esteja desconectado com a nuvem, a perícia terá que obter a senha, utilizando programas de descriptografia. Muitos arquivos na nuvem não são criptografados. Uma alternativa para a obtenção de arquivos mantidos na nuvem caso não haja colaboração do investigado é a requisição direta ao provedor responsável pelo serviço. O pedido, neste caso, demanda autorização judicial e poderá englobar todos os arquivos e informações mantidos pelo provedor, desde que detalhados na autorização. Após a busca e apreensão, feita pela autoridade policial ou ministerial, visando identificar a autoria, caso residam mais de uma pessoa no local onde foi apreendido o dispositivo informático ou caso o sinal de Internet seja compartilhado com terceiros. Essa apuração será mais simples dependendo dos elementos colhidos durante a busca, como a identificação do dono do celular de onde partiram as publicações.

No entanto, quando **a investigação for cível**, identificado o usuário que divulgou a notícia, pelo provedor de aplicações de internet, que informou o IP, data e hora do usuário, e pelo provedor

de conexão, que informou os dados cadastrais do respectivo, que utilizou aquele IP, muitas vezes, **não há necessidade de busca e apreensão daquele arquivo, que já é público**. Basta a identificação do usuário do IP, que se conectou à internet, por determinado dispositivo, e fez a referida publicação. Mas caso haja negativa da autoria delitiva, somente a perícia no dispositivo informático apreendido poderá confirmá-la.

O TSE firmou com os principais provedores de aplicações de internet, que prestam serviços no País, como o grupo Meta (Facebook, Instagram e WhatsApp); Google; Twitter; TikTok, Kwai e Telegram, em 6/1/2022, Memorandos de Ajustamento[25], com prazo até 31/12/2022, que visavam ao enfrentamento à desinformação contra o processo eleitoral, no qual os provedores se comprometeram a oferecer cursos de capacitação para os TREs, criar canais de denúncias em suas plataformas e oferecer informações oficiais confiáveis sobre o processo eleitoral e temas relacionados; além de se comprometerem a deletar perfis falsos; promoverem campanhas para mitigar o impacto das fake news ao processo eleitoral brasileiro; combaterem o uso de robôs e colaborarem com as autoridades. Em menor extensão, com o Telegram, firmado em 25/3/2022.

É necessário, outrossim, o constante desenvolvimento e aperfeiçoamento de ferramentas já existentes na própria aplicação, que identifiquem os robôs (bots), muito utilizados para propagar desinformação em seus serviços, e a identificação de usuários que descumprem os próprios Termos de Serviços das plataformas.

VIII.7) Ilícito eleitoral em sites

Temos visto inúmeras páginas na *web* – *sites* – falsos, se fazendo passar pela página de alguém, algum estabelecimento ou instituição.

Os mensageiros eletrônicos e as demais redes sociais propagam *links* que levam a essas páginas através de postagens também falsas.

O ideal é que tais postagens sejam retiradas das redes sociais, porém, devido à dimensão da Internet e à rápida difusão dessas mensagens, nem sempre isso é possível, sendo necessário retirar/desabilitar o conteúdo do *site* para que não fique mais disponível a quem acessá-lo.

Assim que recebida a notícia da infração, sendo necessária a coleta da prova eletrônica, isto é, a prova da existência da página, o PRE ou promotor deve encaminhar a notícia à ASSPA ou setor pericial do MP, que deverá coletar adequadamente a prova utilizando ferramentas forenses que atestem que o material corresponde, exatamente, ao publicado, iniciando-se, a partir

[25] Disponível em: https://www.tse.jus.br/imprensa/noticias-tse/2022/Fevereiro/tse-e-plataformas-digitais assinam-acordo-nesta-terca-feira-15. Acesso em: 20 mar, 2022.

daí, a cadeia de custódia. Essa extração gerará um cálculo hash. A técnica para fazer essa extração de maneira adequada, deve ser realizada pelo técnico ou analista pericial.

Além da preservação da prova, a próxima providência será a identificação de onde o *site* está hospedado. Em geral, os criminosos utilizam um serviço de hospedagem, como GoDaddy, UOL ou Worldpress.

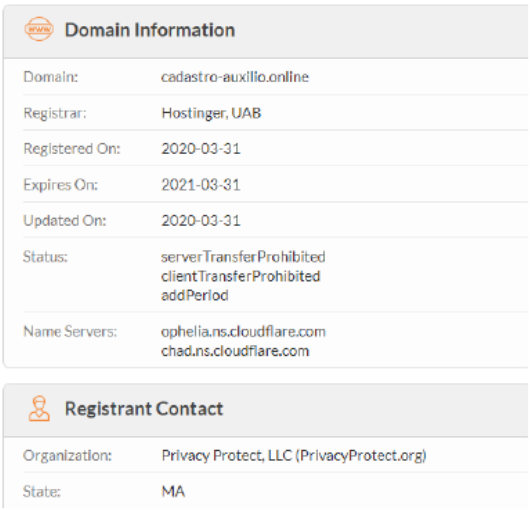
O serviço de hospedagem, em que o *site* malicioso está albergado, em tese, tem como informar os dados da pessoa que criou o *site* malicioso, o IP de criação e os *logs* de acesso ao *site*. O problema é que, em geral, os criminosos se utilizam também de um serviço de anonimização, isto é, se valem dos serviços de uma empresa de privacidade *on-line* para que ela registre o *site* na empresa de hospedagem no lugar do real proprietário do domínio, como forma de dificultar a sua identificação. Essa empresa, que registrou o *site* como seu, é que possui a informação do real proprietário (dados cadastrais, inclusive financeiros).

Para identificar o provedor de hospedagem e eventual provedor de anonimização, devem ser consultados os serviços https://www.registro.br/ (para endereços nacionais) ou no http://whois.icann.org (para endereços no exterior), nos termos do item VII.2 acima.

Veja um exemplo de um *site* fraudulento, que simulava um endereço oficial do Governo Federal para angariar dados e inocular códigos maliciosos, antes acessível pelo endereço eletrônico https://cadastroauxilio.online/Beneficio/?AuxilioEmergencial:

Após pesquisa realizada em http://whois.icann.org (ou https://lookup.icann.org/lookup), foi possível constatar que a empresa, que hospeda o *site* malicioso, está oculta e somente pode ser identificada se entrarmos em contato com a empresa *Cloudflare*, que consta como *name server*, a Hostinger aparece como o Registrador e a Privacy Protect LLC, que oferece serviços de privacidade, está no lugar do Registrante (ver quadro abaixo). A empresa *Cloudflare* é a que tem a informação acerca da hospedagem do *site* malicioso e a quem deve ser questionado quem hospeda o *site*. Uma vez sabendo quem é o provedor de hospedagem, deve ser direcionado o

pedido de preservação de registros de criação do *site* e *logs* de acesso (IPs, data e hora) e o pedido de remoção do *site* malicioso da Internet. A empresa Privacy Protect é a que aparece como responsável pelo *site* malicioso, a Registrante deve ser interpelada para preservar os dados do real usuário (dados cadastrais, inclusive financeiros) para futuro encaminhamento, após obtenção de ordem judicial para este fim. Outra providência pode ser contatar a Hostinger, que no caso é a Registradora, para que seja retirado o domínio malicioso do ar.



Domain Information

Domain:	cadastro-auxilio.online
Registrar:	Hostinger, UAB
Registered On:	2020-03-31
Expires On:	2021-03-31
Updated On:	2020-03-31
Status:	serverTransferProhibited clientTransferProhibited addPeriod
Name Servers:	ophelia.ns.cloudflare.com chad.ns.cloudflare.com

Registrant Contact

Organization:	Privacy Protect, LLC (PrivacyProtect.org)
State:	MA

Caso as empresas responsáveis pela hospedagem e anonimização sejam brasileiras ou tenham filial no Brasil, os pedidos de preservação devem ser endereçados a elas diretamente nos termos do item VII.2 acima.

Relembre-se que para a empresa responsável pela hospedagem deve também ser direcionado o pedido de remoção do *site* malicioso, frente à possibilidade de que o provedor verifique violação dos seus termos de serviço e retire espontaneamente o *site* da Internet.

Posteriormente, o PRE/Promotor Eleitoral pode ajuizar a medida cautelar de quebra de sigilo telemático, com o pedido para a ordem judicial de remoção do *site*. Caso a empresa a ser demandada não tenha vínculo com o Brasil, duas medidas podem ser tomadas simultaneamente. Essas empresas costumam possuir uma aba ou *email* para reportar abusos, o que pode ser feito diretamente a fim de avisar a empresa sobre o conteúdo ilícito, já pedindo preservação dos dados e a remoção do *site* ilícito, reforçando sobre a necessidade de não haver a notificação do responsável pelo *site* a fim de não prejudicar a investigação.

Concomitantemente, deve-se pedir o auxílio da Polícia Federal através do *e-mail* cybercrime_brazil_24x7@dpf.gov.br, também pedindo preservação dos dados e a remoção do *site* malicioso.

Após, deve-se realizar o ajuizamento de pedido judicial de quebra de sigilo telemático do *site* a fim de instruir o pedido de cooperação internacional para obtenção formal das informações

relativas ao *site* investigado.

Relembre-se que para todas as medidas extra e judiciais o *site* deve ser identificado com o seu endereço eletrônico (URL) completo.

VIII.8) Ilícito eleitoral pelo Facebook e Instagram

Recebida representação de que houve a veiculação, no Facebook ou Instagram, de mensagem com conteúdo ilícito, a primeira providência é adoção de medidas de preservação dos registros relacionados a esta mensagem e do usuário que a emitiu, como mencionado no item VII.2.

Para tal finalidade, é importante que se identifique a conta do perfil que se pretende investigar (v. https://www.facebook.com/safety/groups/law/guidelines/). As contas do Facebook podem ser identificadas pelo: a) URLs das contas com o número de identificação de usuário (http://www.facebook.com/profile.php? id=1000000XXXXXXXX) ou com o nome de usuário (http://www.facebook.com/nomedeusuario) do perfil do Facebook, b) endereço de *e mail* e c) o número de telefone (+55, DDD, número).

Para a localização do endereço eletrônico do perfil investigado (URL), no computador, ao acessar a página do perfil, a URL é exibida na barra de endereços do navegador.

No celular, o acesso à URL do perfil é obtido após o clique no menu e a seleção de "copiar link". Após clicar em "copiar link", deve-se "colar" essa informação em qualquer arquivo de texto.

Obtidas as informações em relação à conta investigada, acesse o Sistema do Facebook de Solicitação On-Line para Autoridades, localizado em https://www.facebook.com/records, e siga as instruções para a preservação da conta. Para preservação da conta, o procedimento é o mesmo tanto se o fato em apuração for ilícito eleitoral civil como criminal.

Ao mesmo tempo em que se busca a preservação dos dados junto ao Facebook, é necessária a coleta adequada da prova, com todos os cuidados forenses para que seja mantida íntegra e preservada, dando-se início à cadeia de custódia. Para tanto, as informações necessárias para acesso à publicação devem ser encaminhadas de imediato à ASSPA local ou ao setor especializado na sede do MP, para extração do cálculo *hash*, nos termos mencionados no item VII.2. A ASSPA ou o setor de TI do MP terá condições técnicas de fazer essa extração de maneira adequada.

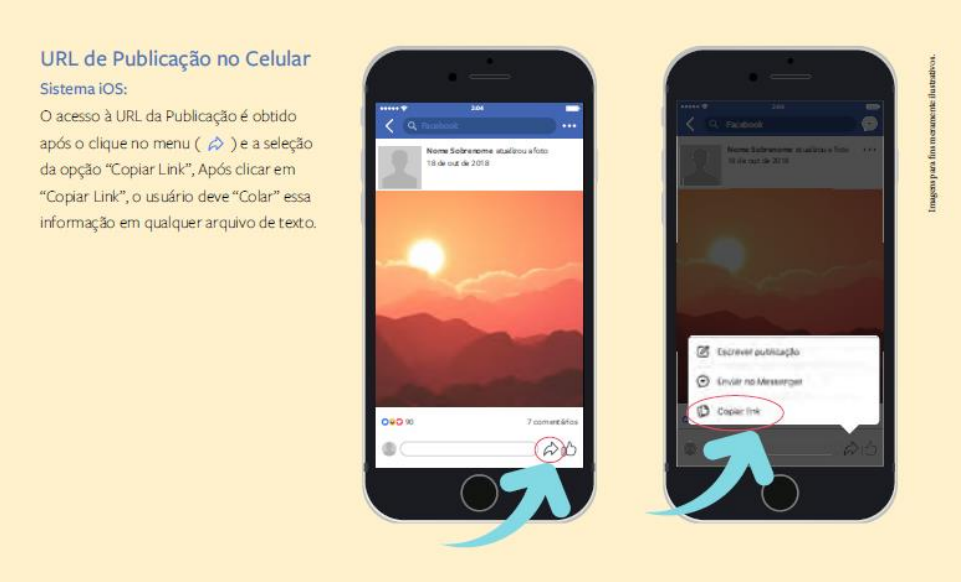
Realizado o pedido de preservação e colheita da prova, caso se considere necessária a retirada do conteúdo do provedor, é importante que se obtenha a URL específica da publicação ou comentário, que se pretende remover. A retirada de conteúdo, como exposto acima, precisa limitar-se especificamente à URL infratora, sob pena de ser retirado também conteúdo lícito (quando, por exemplo, se solicita a retirada de uma página inteira, que contém conteúdo lícito e ilícito).

No Facebook, cada perfil, página, evento ou grupo possui uma URL própria e genérica que, por sua vez, é mais ampla e diferente das URLs mais específicas das publicações ou comentários neles existentes. Em uma página, grupo ou evento, determinada publicação poderá ter sido feita por usuários diferentes que tenham poderes sobre aquele ambiente (administrador, que pode ser distinto do criador), motivo pelo qual é importante que se identifique a URL específica da publicação tida como ilícita.

No computador, para identificação da URL específica de uma publicação ou comentário, clique na respectiva data ou hora de disponibilização, que a URL aparecerá na barra de endereços do navegador, conforme imagem a seguir:

No celular, o acesso à URL da publicação é obtido após o clique no menu e a seleção da

opção copiar link. Após clicar em "copiar link", deve-se "colar" essa informação em qualquer arquivo de texto.26



A retirada de conteúdo, como mencionado no item VII.3, somente pode ser feita sem ordem judicial em determinadas hipóteses. Nesses casos, depois de identificada a URL específica, como mencionado acima, pode ser feito o pedido de retirada diretamente ao Facebook, por meio de *e-mail* enviado ao endereço records@facebook.com, com o *link* do conteúdo a ser retirado.

Após a preservação da prova, e a retirada do conteúdo, caso seja necessário, o próximo passo é o ajuizamento de medida cautelar de afastamento de sigilo telemático para obtenção dos registros de acesso e uploads (postagens) àquela aplicação, cujo modelo encontra-se em tópico próprio (item VII.5), seguindo-se os demais passos expostos nos itens VII.6 e VII.7.

Importante: o Facebook notifica os usuários quanto a pedidos de informação referentes a seus dados. Por isso, caso o sigilo seja indispensável para a investigação, é necessário indicar à empresa que o pedido não poderá ser informado ao usuário.

Durante o período eleitoral, os ofícios e ordens judiciais devem ser enviadas para os endereços: eleicoesfacebook@tozzinifreire.com.br

Em casos criminais, reitere-se que o meio de comunicação ideal para a entrega de ofícios ao Facebook é a plataforma https://www.facebook.com/records. Por fim, nos ofícios, deve constar o endereço da matriz do grupo Meta Plataforms (Facebook/Instagram/WhatsApp/Messenger):

META PLATAFORMS, INC.
1601 Willow Road,
Menlo Park, CA 94025,

26 Imagem obtida em: www.tre-rj.jus.br/site/eleicoes/2018/arquivos/cartilha_localizacao_especificacao_conteudo.pdf (página já excluída).

California,
United States of America
A/C do Facebook/Instagram Brasil
Rua Leopoldo Couto de Magalhães Junior, 700, 5º andar
Bairro Itaim Bibi
São Paulo -SP
CEP 04542-000

VIII.9) Ilícito eleitoral pelo WhatsApp

Na hipótese de veiculação de mensagens com conteúdo ilícito pelo aplicativo WhatsApp, o pedido de preservação de dados deve ser realizado pelo sistema de Solicitação On-Line para Autoridades, localizado no https://www.whatsapp.com/records, bastando seguir as instruções.

Para esta finalidade, é necessário que se tenha a conta a ser investigada que será identificada pelo número do telefone do usuário (+55-DDD-número).

Sem prejuízo, deve ser feita a coleta da prova nos termos indicados no item VII.2, com a remessa das informações à ASSPA ou ao setor de TI.

Importante: as mensagens de WhatsApp podem conter dois tipos diferentes de meios de propagação. O primeiro é o envio do arquivo, ou mensagem, no próprio sistema do aplicativo. Nesses casos, deve ser seguido o roteiro indicado abaixo neste item para colheita da mensagem e investigação da origem. O segundo é o envio de *link* que remete a outro *site* na Internet, que é o que efetivamente contém o conteúdo ilícito. Neste caso, não basta ser excluída a mensagem, pois o *site* continuará funcionando, devendo ser seguido o roteiro indicado no item VII.7.

Após o pedido de preservação e a coleta da prova, o próximo passo é o ajuizamento da medida cautelar de quebra de sigilo de dados do provedor de aplicação (item VII.4), pela qual é possível solicitar diversas informações dos usuários, como abaixo especificado:

- dados de perfil (foto, nome, número de telefone, sistema operacional, data da criação da conta, versão do WhatsApp instalado, e endereço de *e-mail*, se fornecido) - esses dados também podem ser obtidos sem ordem judicial;
- informação dos grupos onde o investigado participa, incluindo os participantes;
- grupos onde o usuário é administrador;
- última conexão com data, hora e IP, se disponível;
- indicação de *e-mail* que foi utilizado para *backup* de mídia e mensagens, se disponível;
- histórico de mudança de números; e
- agenda de contatos.

Importante: as comunicações realizadas através do WhatsApp utilizam criptografia ponta-a-

ponta. Isso significa que a empresa não possui as mensagens e nem é possível interceptá-las. É possível, porém, ajuizar medida de interceptação telemática visando obter os dados das comunicações, mas não o conteúdo. Nesses casos, é possível solicitar o envio de:

- extratos de mensagens, consistente nas informações de remetente, destinatário, data e hora da mensagem;

- tipo da mensagem; e

- IP da conta alvo, se disponível.

Pode ser solicitado que tais informações sejam repassadas a cada 24 horas, contadas da data de implementação da medida até os 15 (quinze) dias seguintes a esta, nos termos da Lei 9246/96 (Lei de Interceptação Telefônica e Telemática).

No período eleitoral, quaisquer intimações devem ser enviadas para waeleitoral@mattosfilho.com.br.

Repise-se que, nos casos criminais, os ofícios devem ser encaminhados pelo sistema de Solicitação On-Line para Autoridades, localizado no https:// www.whatsapp.com/records:

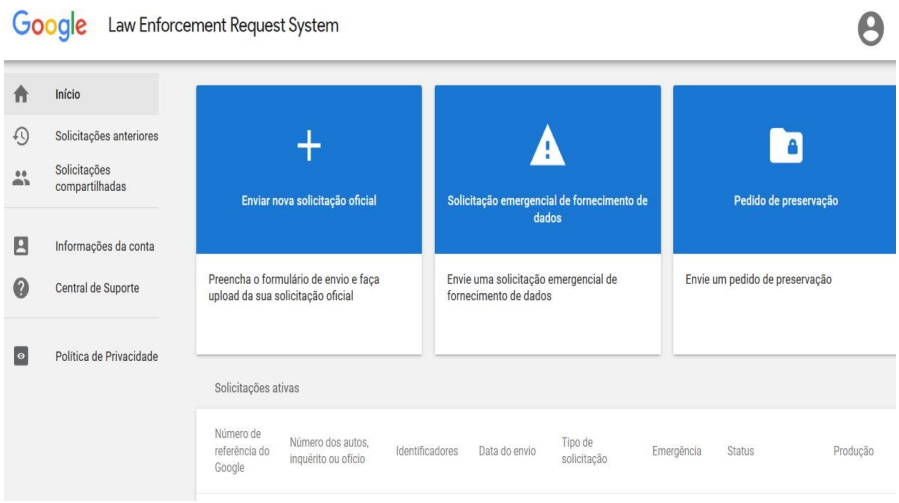
Por fim, nos ofícios, deve constar o endereço do WhatsApp LLC, como segue:

WhatsApp LLC
1601 Willow Road, Menlo Park, CA 94025,
California, United States
A/C do WhatsApp LLC
Rua Leopoldo Couto de Magalhães Junior, 700, 5º andar,
Bairro Itaim Bibi, São Paulo-SP
CEP 04542-000

VIII.10) Ilícito eleitoral pelo Youtube

Na hipótese de veiculação de conteúdo ilícito pelo Youtube, o pedido de preservação de dados deve ser realizado pelo sistema de Law Enforcement Request System da Google, acessível pela URL http://lers.google.com, na qual será necessária a criação de conta.

A preservação de dados ou encaminhamento de ofícios também poderá ser realizada pelos *e-mails*: lis-latam@google.com e juridicobrasil@google.com.



Como nos casos anteriores, concomitantemente ao pedido de preservação, é necessário coletar a prova por meio de ferramentas forenses, conforme descrito no item VII.2, encaminhando-se à ASSPA ou ao setor de TI da sede do MP.

Também é possível solicitar a retirada do conteúdo nocivo, nos termos descritos no item VII.3. O *link* para remover conteúdo do YouTube caso viole seus Termos de Serviço: https://www.youtube.com/reportingtool/legal.

Após, deve ser providenciado o ajuizamento de medida cautelar de quebra de sigilo telemático, nos termos descritos no item VII.4, para obter as seguintes informações, entre outras:
- *logs* de acesso (contendo IP, data, hora e fuso horário GMT) de criação do canal e dos acessos em período a ser indicado;
- endereços eletrônicos e outros dados eventualmente armazenados do criador da página; e
- dados da conta Google, incluindo informações de localização, dados armazenados do Google Maps, histórico de pesquisa do Google, imagens no Google Photos, dados no Google Drive, etc.

Recomenda-se que o ofício seja enviado pelo Sistema de Law Enforcement Request System da Google, acessível pela URL http://lers.google.com e tenha o seguinte endereçamento:

Google Brasil Internet Ltda.

Avenida Brigadeiro Faria Lima, 3477, 18º andar
São Paulo - SP
CEP 04538-133

VIII.11) Ilícito eleitoral pelo X (ex-Twitter)

Na hipótese de veiculação de conteúdo ilícito pelo Twitter, o pedido de preservação de dados que até o início de 2022 era realizado pelo sistema on line https://legalrequests.twitter.com, esse portal foi descontinuado e o pedido de preservação e os demais devem ser enviados por meio físico (informado ao final).

O pedido de preservação deve conter a identificação do perfil infringente, com as seguintes informações (v. https://help.twitter.com/pt/rules-and-policies/twitter-law enforcement-support#6): o nome do usuário e o URL do perfil do Twitter envolvido (por exemplo, https://twitter.com/twittersafety (@twittersafety); e/ou o número de identificação do usuário ou UID exclusivo e público da conta no Twitter ou um nome de usuário e URL do Periscope (por exemplo, @twittersafety e https://periscope.tv/twittersafety). Para localizar um UID do Twitter ou o nome de usuário do Periscope, consulte https://help.twitter.com/pt/rules-and-policies/twitter-law-enforcement
support#5.7.

Realizado o pedido de preservação, a notícia de fato deve ser encaminhada à ASSPA ou ao setor de TI do MP para este realizar a preservação das informações trazidas na notícia de fato, nos termos descritos no item VII.2.

Caso seja necessária a retirada do conteúdo, nos termos do descrito no item VII.3, seguir orientações publicadas em https://help.twitter.com/pt/rules-and-policies/twitter-law enforcement-support#16.5.

Após a preservação, e a retirada, se necessária, o próximo passo é o ajuizamento de Medida Cautelar de Afastamento de Sigilo Telemático, nos termos descritos no item VII.4, em que podem ser pleiteadas diversas informações sobre o usuário, tais como:

- *Logs* de acesso (IP, data, horário e fuso horário) do período indicado (referente à publicação da mensagem);

- nome, sobrenome, senha, *email* e nome de usuário;

- localização, foto da conta e do fundo;

- número de celular para recebimento de SMS e catálogo de endereços;

- *tweets*, as contas seguidas, *tweets* favoritos;

- coordenadas exatas da localização dos *tweets*;

- endereços de IP, data/hora/fuso, navegador utilizado, domínio referentes, páginas

visitadas, operadora do dispositivo móvel;

- dispositivo móvel, Ids de aplicativos e termos de busca; e

- links visitados e quantidade de vezes que foi clicado.

Importante constar no requerimento que o ofício deve ser enviado para o seguinte endereço:

Twitter Brasil Rede de Informação Ltda. (TWITTER BRASIL)
Av. Brigadeiro Faria Lima, 4055, 5º andar, salas 05/119, Itaim-Bibi, São Paulo-São Paulo
CEP 04538-133

Importante: o X (ex-Twitter) notifica usuários sobre as solicitações de informação da conta, motivo pelo qual é importante que, em qualquer pedido, inclusive o de preservação, conste o requerimento para que o usuário não seja notificado, com a indicação de que a ciência será prejudicial à investigação. Deve ser apontado, também e na medida do possível, o prazo em que essa comunicação não poderá ser feita.

Por fim, cabe ressaltar que as operadoras do Twitter atribuem o "selo azul de verificação" às contas de interesse público, ou seja, as operadoras do Twitter analisam os dados fornecidos pelos titulares e confirmam que estes são autênticos e que efetivamente pertencem à pessoa ou à marca que representam (v. https://help.twitter.com/pt/managing your-account/twitter-verified-accounts). Tal informação pode ajudar a verificar se o *tweet* investigado partiu realmente do titular da conta. Atualmente, essas contas verificadas são vendidas, então a confiabilidade sobre essa verificação é relativa.

IX) Modelo de peça de medida cautelar de quebra de sigilo telemático para servidor de hospedagem e privacidade de sites ilícitos

EXCELENTÍSSIMO SR. DESEMBARGADOR ELEITORAL RELATOR
OU JUIZ ELEITORAL DA ___ ZONA ELEITORAL

SIGILOSO

Procedimento nº

A PROCURADORIA REGIONAL ELEITORAL ou MINISTÉRIO PÚBLICO ELEITORAL, pelo (a) Procurador (a) Regional Eleitoral ou Promotor (a) de Justiça Eleitoral infra-assinado(a), com fulcro em suas atribuições constitucionais e legais, vem à presença de Vossa Excelência requerer, com fulcro no artigo 5º, inciso XII, da Constituição Federal e no artigo 10, § 1º, da Lei nº 12.965/14 (Res TSE nº 23.671/2019, art. 39), MEDIDA CAUTELAR DE QUEBRA DE DADOS TELEMÁTICOS, pelos motivos de fato e direito abaixo expostos:

I – Histórico

O procedimento, em epígrafe, foi instaurado para apurar a possível prática do ilícito eleitoral tipificado no artigo XX da .

Conforme consta na notícia, o *site* [indicar URL] simula ser um *site* oficial do Governo Estadual, com o fim de angariar dados dos usuários e inocular códigos maliciosos, conforme se nota pelas imagens abaixo:

[Incluir imagens da captura de tela do site]

Frente a tal informação, solicitou-se a preservação dos registros referentes ao mencionado *site*, tanto para o provedor de hospedagem como para o serviço de anonimização (Id. x), bem como solicitou-se à Assessoria de Pesquisa e Análise (ASSPA) ou ao setor de Tecnologia e Informação do MP, realizasse a colheita da prova, com extração do cálculo *hash*, o que foi cumprido, conforme Id. x.

Dessa forma, revela-se imperiosa, para a elucidação do delito penal sob investigação, a quebra de sigilo de dados telemáticos do responsável pelo site [indicar URL], de modo a viabilizar sua identificação e reunir elementos probatórios acerca da prática criminosa investigada.

1.2) Diferenças entre Serviço de Hospedagem e de Anonimização

Para melhor entendimento do pleito ministerial, faz-se necessário o conhecimento acerca da diferença entre serviço de hospedagem e de anonimização de *sites*. Os *sites* são disponibilizados na internet, através do servidor de hospedagem. Em geral, os criminosos se utilizam de um serviço de hospedagem, como GoDaddy, UOL ou worldpress.

Assim, o serviço de hospedagem em que o *site* está albergado, em tese, tem como informar os dados da pessoa que criou o *site*, o IP de criação e os *logs* de acesso ao *site*. O problema é que, em geral, os criminosos se utilizam também de um serviço de anonimização, isto é, se valem dos serviços de uma empresa de privacidade *on-line* para que

ela registre o *site* na empresa de hospedagem no lugar do real proprietário do domínio, como forma de dificultar a sua identificação.

Essa empresa que registrou o *site* como seu é que possui a informação do real proprietário (dados cadastrais, inclusive financeiros).

Para identificar o provedor de hospedagem e eventual provedor de anonimização, devem ser consultados os serviços https://www.registro.br/ (para endereços nacionais) e no http://whois.icann.org (para endereços no exterior).

Após pesquisa realizada em http://whois.icann.org (ou https://lookup.icann.org/lookup), foi possível constatar que a empresa que hospeda o *site* investigado [indicar URL] é a empresa X e a que oferece serviços de privacidade é a empresa Y.

De tal forma, a empresa X é a que hospeda o *site* malicioso e é quem possui os registros de criação do *site* e *logs* de acesso (IPs, data e hora). Por sua vez, a empresa Y é a que aparece como responsável pelo *site* malicioso no cadastro da empresa X de hospedagem e, portanto, deve ser interpelada para informar os dados do real responsável (dados cadastrais, inclusive financeiros) pelo site.

II) Direito

II.a) Ocorrência do ilícito eleitoral previsto no Art. X ....

Conforme visto no item I, o *site* [indicar URL] simula ser um *site* oficial do Governo Estadual, com o fim de angariar dados dos usuários e inocular códigos maliciosos, conforme se nota pelas imagens acima expostas.
[Descrição de detalhes do caso]

Assim evidencia-se que o responsável pelo mencionado *site* [detalhar a tipificação].

II.b) Competência da Justiça Eleitoral

O artigo tal , inciso da Constituição da República determina que a Justiça Eleitoral será competente para julgar ....

No caso concreto, a publicação menciona, expressamente, ...

II.c) Requisitos para a concessão da Medida Cautelar

Como é cediço, o direito à inviolabilidade da vida privada e da intimidade, previsto no art. 5º, incs. X e XII da Constituição Federal não se reveste de caráter absoluto, podendo e devendo ser relativizado quando indispensável para investigação criminal.

Nesse sentido, a Lei nº 12.965/14, conhecida como Marco Civil da Internet, veio regulamentar especificamente o acesso aos registros de conexão ou de registros de acesso a aplicações de internet para viabilizar a investigação de fatos delitivos, reproduzido na Resolução TSE nº 23.610/2019, art. 40, *in verbis*:

> Art.40. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial, em caráter incidental ou autônomo, requerer ao juiz eleitoral que ordene ao responsável pela guarda o fornecimento dos dados constantes do art. 39 desta Resolução. § 1º. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade (Lei nº 12965/2014, art.22).
> I - fundados indícios da ocorrência do ilícito de natureza eleitoral;
> II - justificativa motivada da utilidade dos dados solicitados para fins de investigação ou instrução probatória; e
> III - período ao qual se referem os registros;

IV - a identificação do endereço da postagem ou conta em questão (URL ou, caso inexistente, URI ou URN), observados, nos termos do art. 19 da Lei nº 12.965/2014, o âmbito e os limites técnicos de cada provedor de aplicação de internet.

Tomando-se por base os parâmetros estabelecidos na Lei nº 12.965/14, *in casu*, e na Resolução TSE nº 23.610/2019, consideram-se preenchidos os requisitos para o afastamento do sigilo telemático.

Como visto, há indícios razoáveis da prática da conduta ilícita tipificada no art. XX do

Necessário, neste ponto, identificar a autoria, partindo-se da individualização dos responsáveis pela publicação do conteúdo.

Ademais, a medida é necessária para a investigação dos fatos, já que possibilitará a coleta de elementos probatórios para a identificação da autoria do ilícito eleitoral. Por fim, quanto à delimitação temporal exigida pelo legislador, tal requisito restou cumprido, já que se pretende a obtenção dos registros referentes ao período da criação do perfil investigado, bem como da publicação com conteúdo ilícito.

Assim sendo, estão presentes os requisitos necessários à quebra de sigilo telemático. Como visto no item 1.2 desta peça, a empresa que hospeda o *site* investigado [indicar URL] é a empresa X e a que oferece serviços de privacidade é a empresa Y. Outrossim, tendo em vista que a mensagem veicula conteúdo ilícito, é imprescindível seja determinada a sua remoção da plataforma virtual, até mesmo para cessar os efeitos nocivos no meio social.

III) Pedido

Ante o exposto, o MINISTÉRIO PÚBLICO ELEITORAL requer seja deferida a quebra de sigilo de dados telemáticos acima pleiteada, e pleiteia o que segue:

a) seja oficiada a empresa X, situada no endereço XXX, para que:

- forneça os dados de cadastros do responsável pelo *site* [indicar URL], - forneça os *Logs* de criação do mencionado *site* (IP, data, hora e fuso horário); - forneça os *Logs* de acesso ao site do período XX (Data em que se teve a notícia do funcionamento do *site*) até o recebimento do presente.
- remova o *site* [indicar URL] da Internet;
- não comunique ao responsável pelo site a presente medida, tendo em vista que o sigilo é necessário ao bom êxito das investigações; e que a resposta seja encaminhada com código *hash*.

b) seja oficiada a empresa Y, situada no endereço XXX, para que:

- forneça os dados cadastrais referente ao responsável pelo site [indicar URL]; -forneça os dados financeiros referente ao responsável pelo site (INDICAR URL), com a indicação da forma de pagamento, conta bancária, etc;
- não comunique ao ao responsável pelo *site* a presente medida, tendo em vista que o sigilo é necessário ao bom êxito das investigações e que a resposta seja encaminhada com código *hash*.

Com o objetivo de assegurar o prosseguimento das investigações, requer o MINISTÉRIO PÚBLICO ELEITORAL a DECRETAÇÃO DO SIGILO ABSOLUTO DOS PRESENTES AUTOS.

X) Modelo de peça de medida cautelar de quebra de sigilo telemático ao Facebook

EXCELENTÍSSIMO SR. DESEMBARGADOR ELEITORALRELATOR OU JUIZ ELEITORAL DA __ ZONA ELEITORAL

SIGILOSO

Procedimento nº

A PROCURADORIA REGIONAL ELEITORAL ou MINISTÉRIO PÚBLICO ELEITORAL, pelo (a) Procurador(a) Regional Eleitoral ou pelo(a)Promotor (a) de Justiça Eleitoral infra-assinado(a), com fulcro em suas atribuições constitucionais e legais, vem à presença de Vossa Excelência requerer, com fulcro no artigo 5º, inciso XII, da Constituição Federal e no artigo 10, § 1º, da Lei 12.965/14 e artigo 39, da Resolução TSE nº 23610/2019, MEDIDA CAUTELAR DE AFASTAMENTO DE DADOS TELEMÁTICOS, pelos motivos de fato e direito abaixo expostos:

I – Histórico

O procedimento, em epígrafe, foi instaurado para apurar a possível prática do ilícito eleitoral tipificado no art. XXX do Código Eleitoral (ou da LC 64/1990) . Conforme consta na notícia, o usuário do Facebook denominado XXX, com endereço eletrônico (URL - rodapé: URL (Uniform Resource Locator) é a forma padronizada de representação de diferentes documentos, mídias e serviços de rede na Internet, que identifica de forma completa cada documento com um endereço único. Ex. http://www.uol.com.br/serviços.php.) no http://www.facebook.com/profile.php?id=1000000XXXXXXXX, publicou, em página do referido provedor de aplicação, no dia X, a seguinte mensagem, acessível na url www.facebook.com/xxxx):

[Reproduzir aqui a publicação ilícita]

Frente à tal informação, solicitou-se a preservação dos registros referentes à conta do perfil de XXX perante o Facebook (Id. x), bem como solicitou-se junto à ASSPA ou setor de TI do MPE realizasse a colheita da prova, com extração do cálculo *hash*, o que foi cumprido, conforme Id. X.

A captura de tela da referida mensagem encontra-se no Id. X e, pela sua leitura, é possível notar que esta veicula conteúdo ilícito, subsumível à conduta típica prevista no art. XXX do .

Dessa forma, revela-se imperiosa, para a elucidação do delito penal sob investigação, a quebra de sigilo de dados telemáticos do usuário do perfil ou página X, de modo a viabilizar sua identificação e reunir elementos probatórios acerca da prática criminosa investigada.

II) Direito

II.a) Ocorrência do ilícito eleitoral previsto no art. XXX do Código Eleitoral (ou LC 64/1990 ou propaganda eleitoral irregular)

[Descrição dos fatos tais como apurados e tipificação]

II.b) Competência da Justiça Eleitoral

O artigo , inciso , da

No caso concreto, a publicação menciona, expressamente, [identificar os pontos concretos que justificam a competência eleitoral, como a utilização de programas, mensagens e logos da Prefeitura Municipal/do candidato ....].

II.c) Requisitos para a quebra de sigilo telemático

Como é sabido, o direito à inviolabilidade da vida privada e da intimidade, previsto no art. 5º, incs. X e XII da Constituição Federal não se reveste de caráter absoluto, podendo e devendo ser relativizado quando indispensável para investigação eleitoral.

Nesse sentido, o artigo 22 da Lei 12.965/14, conhecida como "Marco Civil da Internet", veio regulamentar especificamente o acesso aos registros de conexão ou de registros de acesso a aplicações de internet para viabilizar a investigação do ilícito eleitoral, reproduzido na Resolução 23.610/2019, art.40, *in verbis*:

> Art. 40. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de dados constantes do art. 39 desta Resolução.
> § 1º. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
> I - fundados indícios da ocorrência do ilícito de natureza eleitoral;
> II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
> III - período ao qual se referem os registros;
> IV - a identificação do endereço da postagem ou conta em questão (URL ou, caso inexistente, URI ou URN), observados, nos termos do art. 19 da Lei nº 12.965/2014, o âmbito e os limites técnicos de cada provedor de aplicação de internet.

Tomando-se por base os parâmetros estabelecidos na Lei nº 12.965/14, *in casu*, previstos na Res. TSE nº 23.610/2019, consideram-se preenchidos os requisitos para o afastamento do sigilo telemático.

Como visto, há indícios razoáveis da prática do ilícito eleitoral de abuso de poder ... previsto no art.22 da LC 64/90 (ou crime do CE). Necessário, neste ponto, identificar a autoria, partindo-se da individualização dos responsáveis pela publicação do conteúdo.

Ademais, a medida é necessária para a investigação dos fatos, já que possibilitará a colheita de elementos probatórios para a identificação da autoria do ilícito eleitoral. Por fim, quanto à delimitação temporal exigida pelo legislador, tal requisito resto u cumprido, já que se pretende a obtenção dos registros referentes ao período da criação do perfil investigado, bem como da publicação com conteúdo ilícito. Assim sendo, estão presentes os requisitos necessários à quebra de sigilo telemático.

Outrossim, considerando que a mensagem veicula conteúdo ilícito, é imprescindível seja determinada a sua remoção da plataforma virtual, até mesmo para cessar os efeitos nocivos no meio social.

III) Pedido

Ante o exposto, o MINISTÉRIO PÚBLICO ELEITORAL requer seja deferida a quebra de sigilo de dados telemáticos acima pleiteada, com a expedição de ofício à empresa META PLATAFORMS, INC, sediada em 1601 Willow Road, Menlo Park, CA 94025, United States of America, a/c FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA., CNPJ 13.347.016/0001-17, sediada na Av. Brigadeiro Faria Lima, 3732, 5º Andar, Itaim Bibi, CEP 04538-132, São Paulo-SP[27] para que:

a) informe os dados cadastrais do usuário do perfil X [indicar URLs das contas com o número de identificação de usuário (ex: http://www.facebook.com/profile.php?id=1000000XXXXXXXX) e/ou com o nome de usuário (ex:http://www.facebook.com/nomedeusuario) do perfil do Facebook e/ou b) endereço de email e/ou c) o número de telefone (+55, DDD, número)]; inclusive nome visível, endereços eletrônicos e telefone vinculados à conta;
b) informe o e-mail ou número de terminal telefônico utilizado para a validação da criação da conta referente ao mencionado perfil;
c) informe os logs de acesso (contendo IP, data, hora e fuso horário) de criação do mencionado perfil;
d) informe os logs de acesso (contendo IP, data, hora e fuso horário) para a veiculação da mensagem referente à URL [indicar URL específica da publicação];
e) informe os logs de acesso (contendo IP, data, hora e fuso horário) do período de XX até a data da assinatura da ordem;
f) remova o conteúdo da publicação referente à URL [indicar URL específica da publicação], bem como os compartilhamentos desta mensagem;
g) não comunique ao usuário da conta investigada a presente medida, tendo em vista que o sigilo é necessário ao bom êxito das investigações.
h) que a resposta seja encaminhada com código *hash*.

Com o objetivo de assegurar o prosseguimento das investigações, requer o Ministério Público Federal a DECRETAÇÃO DO SIGILO ABSOLUTO DOS PRESENTES AUTOS.

[27] Para encaminhamento do ofício por meio eletrônico, deve-se acessar o site: https://www.facebook.com/records. ou email fornecido pelo provedor para fins de atendimento de ordens judiciais.

XI) Modelo de ofício para preservação de registros e remoção de site ilícito para serviço de hospedagem

OFÍCIO nº Localidade, data de 2024.

URGENTE/SIGILOSO

Ao Diretor(a)
UOL - Universo On Line S/A
Rua Barão de Limeira, 458, Centro- São Paulo - CEP 01202 (ofício encaminhado pelo email intimauol@uolinc.com)

REF: REQUISIÇÃO DE PRESERVAÇÃO DE DADOS E PEDIDO DE REMOÇÃO DE SITE ILÍCITO
PROCEDIMENTO Nº

Senhor(a) Diretor (a),

A PROCURADORIA REGIONAL ELEITORAL ou O MINISTÉRIO PÚBLICO ELEITORAL, pelo(a) Promotor(a) de Justiça Eleitoral abaixo subscrito(a), comunica que foi instaurado o procedimento, em epígrafe, com o fim de investigar o *site* hospedado no endereço eletrônico:

[INDICAR A URL COMPLETA DO SITE].

O mencionado *site* simula ser um site oficial para (ex. angariar dados dos eleitores e inocular códigos maliciosos).

Assim, para instrução do procedimento supra identificado, com fundamento no art. 15, § 2º da Lei nº 12.965/2014 (Marco Civil da Internet) e art. 39 da Resolução TSE nº 23.610/2019, requisita-se a preservação dos seguintes dados referentes ao mencionado *site*:

- Dados de cadastros do responsável pelo site, inclusive informações financeiras; - *logs* de criação do *site* (IP, data, hora e fuso horário);
-*logs* de acesso ao *site* do período XX (Data em que se teve a notícia do funcionamento do site) até o recebimento do presente.

Outrossim, tendo em vista que, através do mencionado *site*, é realizada atividade ilícita eleitoral, o que provavelmente contraria as normas de serviço desta empresa, solicita-se a remoção do *site* (indicar) da rede de Internet.

Outrossim, informo que, dentro do prazo legal, será realizado o ajuizamento de Medida Cautelar de Quebra de Sigilo Telemático para obtenção de ordem judicial para o envio dos registros e remoção do site, cuja preservação ora é solicitada.

Por fim, solicito que o presente pedido não seja informado ao usuário da conta, tendo em vista que o sigilo é necessário ao bom êxito das investigações.

XII) Modelo de ofício para preservação de registros e remoção de site ilícito para serviço de privacidade

OFÍCIO nº Localidade, data de 2024.

URGENTE/SIGILOSO

Ao Diretor(a)

REF: PEDIDO DE PRESERVAÇÃO DE DADOS
PROCEDIMENTO Nº

Senhor(a) Diretor (a),

Cumprimentando-o, para instrução do procedimento supra identificado, com fundamento no art. 13, § 2º e art. 15, § 2º da Lei nº 12.965/2014 (Marco Civil da Internet) e art. 39 da Resolução TSE 23.610/2019, venho por meio deste requisitar a preservação de dados cadastrais (inclusive dados financeiros) referentes ao *site* abaixo indicado, no período de XX (data da informação de funcionamento do *site*) até o momento do recebimento do presente ofício:

[URL DO SITE INVESTIGADO]

Outrossim, informo que, dentro do prazo legal, será realizado o ajuizamento de Medida Cautelar de Quebra de Sigilo Telemático para obtenção de ordem judicial para o envio dos registros (inclusive financeiro), cuja preservação ora é solicitada.

Por fim, solicito que o presente pedido não seja informado ao usuário da conta, tendo em vista que o sigilo é necessário ao bom êxito das investigações.

Atenciosamente,

XIII) Modelo de ofício de requisição de dados cadastrais e de preservação para provedor de conexão (Claro S/A)

OFÍCIO nº Localidade, data de 2024.

URGENTE/SIGILOSO

Ao (À) Ilmo. (a) Senhor (a)
Diretor da
CLARO S/A, CNPJ nº 40.432.544/0001-47
Rua Verbo Divino, nº1.356, Chácara Santo Antônio, São Paulo/SP,
CEP 04.719-002 (*email* de encaminhamento: oficios.doc@claro.com.br)

Referência: Requisição de Dados Cadastrais e Preservação de Conta
Procedimento nº

Senhor(a) Diretor (a),

Cumprimentando-o(a), o MINISTÉRIO PÚBLICO ELEITORAL, por seu Promotor (a) Eleitoral infra-assinado(a), visando a instrução do procedimento, em epígrafe, instaurado para investigação de XX, requisita a Vossa Senhoria, com fundamento no art. 10, § 3º, da Lei nº 12.965/2014 (Marco Civil da Internet) e art. 39 da Resolução TSE 23.610/2019, o fornecimento, no prazo de [de 24 horas a 5 dias], dos dados cadastrais disponíveis do usuário vinculado à seguinte conexão:

- [indicação do IP, com DATA e HORÁRIO GMT].

Outrossim, solicito que sejam preservados os dados do mencionado usuário, referente ao período XX.

Solicito, ainda, que a resposta ao ofício: a) tenha caráter sigiloso, b) indique o número do procedimento em epígrafe e do presente ofício; c) seja encaminhada, em meio informatizado, com código *hash*, em arquivos que possibilitem a migração de informações para os autos do processo sem redigitação, nos termos do art. 7º, § 2º, da Resolução nº 181/2017-CNMP e d) seja enviada ao e-mail eletrônico XX.

Por fim, solicito que o presente pedido não seja informado ao usuário, posto que o sigilo é necessário ao bom êxito das investigações.

Atenciosamente,

XIV) Ofício de solicitação de remoção de conteúdo a provedor de aplicação (Facebook)

OFÍCIO n. Localidade, data de 2022. URGENTE/SIGILOSO

A
META PLATAFORMS, INC.
1601 Willow Road, Menlo Park, CA 94025, United States of America
A/C FACEBOOK/INSTAGRAM BRASIL
Rua Av. Brigadeiro Faria Lima, 3732, 5º Andar, Itaim Bibi, São Paulo-SP,
CEP 04538-132 (encaminhado pelo e-mail records@fb.com)

REF: PEDIDO DE REMOÇÃO DE CONTEÚDO
PROCEDIMENTO Nº

Senhor(a) Diretor (a),

Comunico a Vossa Senhoria que o MINISTÉRIO PÚBLICO ELEITORAL, por intermédio do(a) Promotor(a) de Justiça Eleitoral, que esta subscreve, recebeu a informação de que o usuário abaixo indicado, por meio de conteúdo publicado na rede social FACEBOOK e acessível na URL descrita a seguir, praticou conduta XX e, portanto, possivelmente violou normas contidas nos termos de uso desse provedor de aplicação.

Assim sendo, solicito a imediata adoção das providências necessárias à remoção do conteúdo indicado na URL abaixo, bem como da preservação dos dados referentes à página do perfil que segue:

- Identificação do conteúdo: www.facebook.xxx.
- Identificação da conta: http://www.facebook.com/profile.php? id=1000000XXXXXXXX OU http://www.facebook.com/username OU endereço de e-mail OU número de telefone no formato (+55, DDD, número).

Por fim, solicito que o presente pedido não seja informado ao usuário, posto que o sigilo é necessário ao bom êxito das investigações.

Atenciosamente,

XV) Ofício de solicitação de preservação de dados a provedor de aplicação/conexão

OFÍCIO nº Localidade, data de 2024.

URGENTE/SIGILOSO

Ao Diretor(a)
Globo Comunicações e Participações SA
Rua Marquês de São Vicente, 30 – sala 106
Cep: 22451-040 - Gávea- RJ
E-mail:

Referência: **PEDIDO DE PRESERVAÇÃO DE DADOS**
Procedimento nº

Senhor(a) Diretor (a),

Cumprimentando-o(a), o MINISTÉRIO PÚBLICO ELEITORAL, por meio de seu Promotor(a) eleitoral infra-assinado(a), visando a instrução do procedimento, em epígrafe, com fundamento no art. 13, § 2º e art. 15, § 2º da Lei nº 12.965/2014 (Marco Civil da Internet), requisita a preservação de dados referentes a conta abaixo indicada, no período de XX (data da publicação) até o momento do recebimento do presente ofício:

[Indicação dos dados de individualização da conta]

Outrossim, informa que, dentro do prazo legal, será realizado o ajuizamento de Medida Cautelar de Quebra de Sigilo Telemático para obtenção de ordem judicial para o envio dos registros, cuja preservação ora é solicitada.

Por fim, solicita que o presente pedido não seja informado ao usuário da conta, tendo em vista que o sigilo é necessário ao bom êxito das investigações.

Atenciosamente,

XVI) *Email* para a Polícia Federal como ponto de contato da rede 24X7

cybercrime_brazil_24x7@dpf.gov.br

De: PRE/Promotor Eleitoral
Para: cybercrime_brazil_24x7@dpf.gov.br

Prezada Sra. Delegada de Polícia Federal,
Chefe do SRCC

Ref.: Notícia de Fato nº 1.34.001.00XXXX/2022-00

Solicito os bons préstimos dessa Unidade para providenciar pedido de preservação de dados cadastrais, inclusive financeiros de pagamento do serviço (conta bancária, cartão de crédito ou relativos a carteira virtual, se o caso), dados de criação (IP, data e hora) e *logs* de acesso do site malicioso www.XXXJJJJ.com (INDICAR URL) que simula ser um *site* oficial do candidato/Partido/Prefeitura tal, com o fim de angariar dados dos usuários e inocular códigos maliciosos, conduta descrita no artigo XX, do Código Eleitoral (ou no art. 22 da LC 64/90)e que está hospedado pelo provedor (indicar nome da empresa provedora de hospedagem de sites) no país (indicar o país).

Ressalto a importância de que o usuário não seja notificado do pedido de preservação, até que seja obtida a devida ordem judicial de quebra de sigilo de dados telemáticos e enviado e cumprido o pedido de cooperação internacional para obtenção das informações cuja preservação ora se requer.

Aguardo a informação acerca dos dados que já puderem ser disponibilizados desde logo.

Atenciosamente,

XVI) Fontes

Barreto. Alessandro Gonçalves; Brasil, Beatriz Silveira. *Manual de Investigação Cibernética: À luz do Marco Civil da Internet*. Brasport.

Guia Prático sobre Combate à Desinformação e Investigação na Internet, do GACC da 2ª CCR do MPF.

Aulas EAD da ESMPU sobre Investigação de Crimes Cibernéticos, de Fernanda Domingos.

https://portal.nucciber.mpba.mp.br/.

https://www.tse.jus.br/imprensa/noticias-tse/2022/Fevereiro/tse-e-plataformas-digitais assinam-acordo-nesta-terca-feira-15.

https://www.tse.jus.br/eleicoes/sistema-de-alertas

https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf

https://cartilha.cert.br/fasciculos/verificacao-duas-etapas/fasciculo-verificacao-duas etapas.pdf

XVII) Endereços de contato dos provedores

Para obter o anexo com a lista de provedores, solicite à vice-PGE.