MPCE
Ministério Público
do Estado do Ceará

CENTRO DE APOIO OPERACIONAL ELEITORAL – CAOPEL

Ofício Circular nº 0030/2026/CAOPEL

Fortaleza/CE, 10 de junho de 2026

A Sua Excelência o(a) Senhor(a)
PROMOTOR(A) ELEITORAL

Referente: **Protocolo nº 02.2026.00030118-8**
Assunto: Encaminha Ofício Circular nº 26/2026-AEBBPGE

Senhor(a) Promotor(a) Eleitoral,

Cumprimentando-o(a) cordialmente, encaminhamos a Vossa Excelência o Ofício-Circular em epígrafe, oriundo da Procuradoria-Geral Eleitoral, contendo o "Guia prático sobre Desinformação e Investigação na Internet" e, ainda, o material utilizado em palestra proferida pela Procuradora Regional da República Neide Mara Cavalcanti Cardoso de Oliveira, sobre o tema "Ilícitos Eleitorais na internet: como investigar?".

Atenciosamente,

Igor Pereira Pinheiro
Promotor de Justiça
Coordenador do CAOPEL

Monia Dantas de Macedo
Promotora de Justiça
Coordenadora Auxiliar do CAOPEL

João Batista Fontenele Neto
Promotor de Justiça
Coordenador Auxiliar do CAOPEL

MINISTÉRIO PÚBLICO ELEITORAL
PROCURADORIA-GERAL ELEITORAL

OFÍCIO CIRCULAR Nº 26/2026 - AEBB/PGE

Brasília, 2 de junho de 2026.

A Sua Excelência o(a) Senhor(a)
PROCURADOR(A) REGIONAL ELEITORAL

Assunto: **Eleições 2026: guia prático sobre Desinformação e Investigação na Internet. Material utilizado na palestra "*Ilícitos Eleitorais na Internet: como investigar?*".**

Senhor(a) Procurador(a) Regional Eleitoral,

1. Cumprimentando(a), encaminho a Vossa Excelência o "*Guia prático sobre Desinformação e Investigação na Internet*" atualizado pelas Procuradoras Regionais da República Neide Mara Cavalcanti Cardoso de Oliveira e Fernanda Teixeira Souza Domingos, coordenadoras do Grupo de Trabalho sobre Desinformação na Internet, Interferência Cibernética na Democracia e Influência nas Eleições (GTDIE).

2. Encaminho, ainda, o material utilizado em palestra proferida pela Procuradora Regional da República Neide Mara Cavalcanti Cardoso de Oliveira, sobre o tema "*Ilícitos Eleitorais na internet: como investigar?*", no contexto da capacitação realizada para membros e servidores do Ministério Público Eleitoral em parceria com o Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio), no dia 27 de maio de 2026.

3. Considerando a relevância do tema, solicito a V. Exa. que providencie o compartilhamento do material com os Promotores Eleitorais de sua circunscrição.

Atenciosamente,

ALEXANDRE ESPINOSA BRAVO BARBOSA

Vice-Procurador-Geral Eleitoral

Ministério Público *nas* ELEIÇÕES 2026

Ministério Público *nas*
ELEIÇÕES 2026

ILÍCITOS ELEITORAIS NA INTERNET: COMO INVESTIGAR?

Ministério Público Eleitoral

Ministério Público *nas*
ELEIÇÕES 2026

1.Acesso à internet (provs. conexão e aplicação)

2. Marco Civil da Internet e Res.TSE 23610/2019

3. Remoção de Conteúdo

4. Investigação para identificar o usuário

4.1 Desinformação/Investigação em site

4.2 Desinformação/Investigação no Face/Insta

4.3 Desinformação/Investigação no WhatsApp

4.4 Desinformação/Investigação no Youtube

4.5 Desinformação/Investigação no X

5. Estratégia contra Desinformação - PGE

Ministério Público nas ELEIÇÕES 2026

1. Acesso à internet

Toda conexão à rede é feita por meio de um modem, ligado a um **provedor de conexão à internet** (CLARO/NET, Oi TELEMAR, TIM, VIVO, etc).

Para que o usuário possa ser “encontrado”, o provedor lhe atribui um **número de protocolo exclusivo**, pelo período de conexão.

IP = número do protocolo

Ministério Público nas ELEIÇÕES 2026

1.1 Provedores de conexão à internet

Transição do IPv4 para

- endereços IPv4 – esgotamento em 12/2014, sem a implementação total do IPv6;
- situações ocorrem em que há a alocação de um endereço de IP para mais de um usuário durante a transição do IPv4 para o IPv6 (uso da técnica CG-NAT44 = IP nateado);
- grande dificuldade na identificação de usuários infratores;
  - **necessidade do pedido da porta lógica (ou de origem) de acesso aos provedores de conexão e aos de aplicação de internet (art. 9º-G, §2º, III, Res. TSE nº 23.610/19 incluído pela Res 23732/24)**
- recém aprovado o Decreto nº 12975, de 20/5/26, que obriga a guarda da porta lógica (ou de origem) para os provedores de conexão e de aplicação à internet (art.15-A, §§ 1º e 2º,MCI)

1.2 Provedores de aplicação de internet

SERVIÇOS MAIS COMUNS PRESTADOS NA INTERNET
permitem a inserção de postagens na internet

- **world wide web** – www (site, blog, fotoblog)
- **e-mail (@**gmail, hotmail, terra)
- **formação de redes e comunidades virtuais** (Facebook, Instagram, X – ex-Twitter, TikTok)
- **troca instantânea de mensagens** (Whatsapp,Telegram)
- **hospedagem e compartilhamento de arquivos** (redes P2P: eMule, Aresgalaxy, Gnutella, Gigatribe)
- **voip** (voz sobre IP)
- **chat** (salas de bate-papo)
- **fóruns de discussão** (Yahoo groups)
- **serviços de streaming** (YouTube, Globoplay)
- **e-commerce** (Mercado Livre, Amazon)

Ministério Público nas ELEIÇÕES 2026

2. Marco Civil da Internet e Res. TSE 23610/19

Define termos técnicos, direitos e garantias dos usuários, e diretrizes do Poder Público.

art. 5º – Conceitos básicos:

- **endereço de protocolo de internet (endereço IP):** o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais (inc.III); (art.37, VI, Res. TSE 23610/19)
- **registro de conexão:** o 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 (inc. VI, MCI e art.37, inc. VII, Res. TSE 23610/19).

-**registro de acesso a aplicações de internet:** o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP (inc. VIII, MCI, e art.37, VIII, Res. TSE 23610/19).

2. Marco Civil da Internet e Res. TSE 23610/19

- estabelece que as informações dos provedores de conexão e de aplicação à internet somente poderão ser obtidas por ordem judicial (art. 10, § 1º, MCI, e art. 39, da Res. TSE 23610/2019);

- provedores com representação no Brasil ou prestando serviços no País devem cumprir a legislação nacional (art.11, § 2º, MCI e art.40, § 2ª, da Res.TSE 23610/2019).

2. Marco Civil da Internet – Lei nº 12.965/14

art. 11º – estabelece aplicação da legislação brasileira para as operações de coleta, armazenamento, guarda e tratamento de registros realizados em território nacional, sendo obrigatoriamente respeitados os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º - pelo menos um dos terminais localizados no Brasil,

§ 2º - mesmo a 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.

2. Marco Civil da Internet – Lei nº 12.965/14

PROVEDORES SEM REPRESENTAÇÃO NO BRASIL

1.Provedores **sem representação** no Brasil, mas que oferecem seus serviços ao público em território nacional, devem cumprir a legislação brasileira:

- ***Targeting Test:***
  - serviço oferecido em português;
  - publicidade voltada para o público em território nacional;
  - vendas na moeda nacional.

2. **Provedores que NÃO oferecem seus serviços ao público no Brasil**, mas que são utilizados a partir do território nacional: para obtenção dos dados, a menos que eles estejam acessíveis às autoridades nacionais (art. 240 CPP e arts. 842 e ss do CPC), necessário o pedido de cooperação internacional (MLAT). **Res. TSE 23610/19, art. 28.**

2. Marco Civil da Internet – Lei nº 12.965/14

PRAZOS DE RETENÇÃO:

- **registros de acesso às aplicações de internet**: 6 meses (arts.15 e 15-A);
- **registros de conexão**: 1 ano (arts. 13 e 15-A).

PEDIDO DE PRESERVAÇÃO por PRAZO SUPERIOR: pode ser feito pelo MP, polícia ou autoridade administrativa.

Registros armazenados são apenas de metadados:
IP, porta, data e hora GMT (não são criptografados)

2. Marco Civil da Internet – Lei nº 12.965/14

CONTEÚDO: não há obrigação de guarda, mas fornecimento somente por ordem judicial. Pode ser feito pedido de preservação também.

Conteúdo armazenado – art. 7, inc. III, do MCI (CPP, art. 240, alíneas *f* e *h* e CPC, arts. 842 e 843).

Conteúdo *online* - fluxo (tempo real) – art. 7, inc. II, do MCI (na forma da Lei nº 9296/96).

2. Marco Civil da Internet – Lei nº 12.965/14

SANÇÕES do ART. 12: descumprimento (arts. 10 e 11, MCI)

I - ADVERTÊNCIA COM INDICAÇÃO DE PRAZO PARA ADOÇÃO DE MEDIDAS CORRETIVAS;

II - MULTA ATÉ 10% DO FATURAMENTO DO GRUPO ECONÔMICO NO BRASIL - condição econômica do infrator + princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção; (Res. TSE nº 23610/19, art. 27-A, § 8º)

III - SUSPENSÃO TEMPORÁRIA DAS ATIVIDADES – que envolvam os atos previstos no art. 11;

IV - PROIBIÇÃO DE EXERCÍCIO DAS ATIVIDADES - que envolvam os atos previstos no art. 11

APLICAÇÃO SEM PREJUÍZO DAS DEMAIS SANÇÕES CÍVEIS, CRIMINAIS OU ADMINISTRATIVAS CABÍVEIS.

3. Remoção de Conteúdo

REMOÇÃO DE CONTEÚDO DA INTERNET
PODER DE POLÍCIA

Res. 23.610/2019, art. 7º. O juízo eleitoral com atribuições fixadas na forma do art. 8º desta Resolução somente poderá determinar a imediata retirada de conteúdo na internet que, em sua forma ou meio de veiculação, esteja em desacordo com o disposto nesta Resolução.

§ 1º Caso a irregularidade constatada na internet se refira ao teor da propaganda, não será admitido o exercício do poder de polícia, nos termos do art. 19 da Lei nº 12.965/2014 (que prever que o provedor deve ser intimado por ordem judicial).

Ex.: disparo em massa no WhatsApp – meio ilegal de veiculação; impulsionamento de propaganda eleitoral negativa de adversário – forma ilegal de veiculação.

Ministério Público nas ELEIÇÕES 2026

3. Remoção de Conteúdo

Uma das novidades da nova Resolução TSE nº 23.755/2026 foi a alteração da responsabilidade civil dos provedores de aplicação à internet sobre o conteúdo de informações falsas ou sem comprovação técnica que descredibilizem a integridade do sistema eletrônico de votação; que incite crime contra o Estado Democrático de Direito; que fomente a subversão da ordem constitucional ou ruptura da normalidade institucional democrática; ou configure violência política contra a mulher (art. 326-B, CE), tornando-os responsáveis pela remoção desse tipo de conteúdo, independente de ordem judicial, ao incluir o § 4º-A, 4º-B e 4º- C, no art. 28, da Res. TSE nº 23.610/2019.

O usuário responsável pela publicação deve ser comunicado pelo provedor dos motivos e pode requerer judicialmente o restabelecimento da publicação (§4º- C, art. 28).

Ministério Público nas ELEIÇÕES 2026

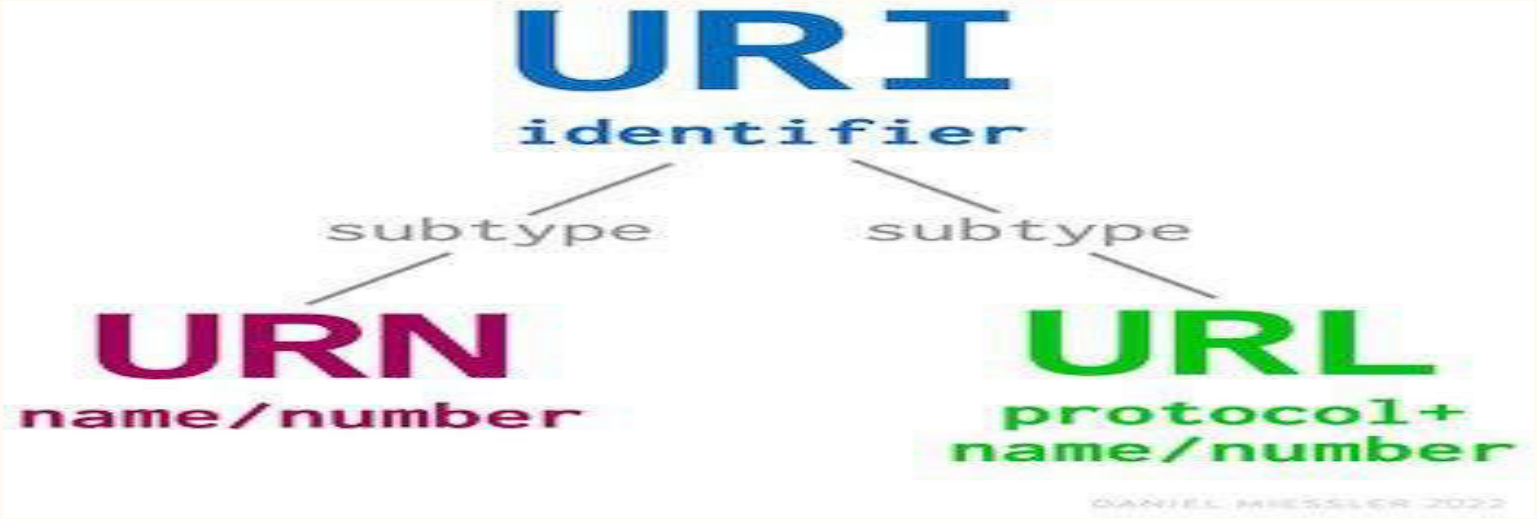
3. Remoção de Conteúdo

A nova Res. do TSE nº 23755/2026 incluiu o **art. 38-A, na Res. TSE 23.610/2019** ao prever que o juízo eleitoral, em processo com ampla defesa e contraditório (§ 1º), remova perfil com usuário falso, apócrifo ou que não exista no mundo real (automatizado ou robo), cuja publicação seja crime eleitoral ou desinformação sobre a integridadede do processo eleitoral, cujas publicações configurem reiterada prática assim reconhecida pela Justiça Eleitoral.

E permitiu ao provedor de aplicação à internet a remoção desse mesmo conteúdo, independente de ordem judicial, desde que o perfil seja falso, automatizado ou robo no **§ 2º, do Art. 38-A, da Res. TSE 23.610/2019**. Exclui a hipótese de perfil aprócrifo (anônimo).

3. Remoção de Conteúdo

Res. TSE 23.610/2019, art. 38, § 4º. A ordem judicial que determinar a remoção de conteúdo divulgado na internet fixará prazo razoável para o cumprimento, não inferior a 24 h, e deverá conter, sob pena de nulidade, a URL e, caso inexistente esta, a URI ou a URN do conteúdo específico, 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.



Ministério Público nas ELEIÇÕES 2026

3. Remoção de Conteúdo

URI - Uniforme Resource Identifier (Identificador de Recurso Uniforme), combinação única de letras, números e/ou caracteres, que identifica certo conteúdo na internet, por meio da página. A URL e URN são subconjuntos do conjunto de URIs.
Ex: **www.prerj.mpf.mp.br (identifica a página, mas sem o meio em que ele se localiza, que é o protocolo – https://)**

URL - Uniforme Resource Locator (Localizador de Recurso Uniforme), que localiza certo conteúdo na internet de forma precisa,padrão). Ex: **https://www.prerj.mpf.mp.br/denuncia-de-ilícitos-na-internet (endereço mais completo)**

URN – Uniforme Resource Name (Nome de Recurso Uniforme), identifica um nome estático. Ex: **prerj.mpf.mp.br**

4. Identificação do usuário

IDENTIFICAÇÃO DO USUÁRIO

Res. TSE nº 23.610/2019, art. 39. O provedor responsável pela guarda somente será obrigado a disponibilizar os registros de conexão e de acesso a aplicações de internet, de forma autônoma ou associados a dados cadastrais, a dados pessoais ou a outras informações disponíveis que possam contribuir para a identificação do usuário, mediante ordem judicial, na forma prevista nesta Seção (**MCI, art.10, caput e § 1º**).

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 (**MCI, art. 22**).

4. Identificação do usuário

IDENTIFICAÇÃO DO USUÁRIO

Res. TSE nº 23610/2019, art. 40.

§ 2º A ausência de identificação imediata do usuário responsável pela divulgação do conteúdo não constitui circunstância suficiente para o deferimento liminar do pedido de quebra de sigilo de dados.

§ 4º Nos casos previstos no caput deste artigo, os provedores indicados no art. 39 desta Resolução podem ser oficiados para cumprir determinações judiciais, sem que sejam incluídos no polo passivo das demandas, nos termos do § 1º-B do art. 17 da resolução deste Tribunal que regula representações, reclamações e direito de resposta.

Ministério Público nas ELEIÇÕES 2026

4.1Investigação para identificar o usuário

VISÃO GERAL DO PROCEDIMENTO

identificação do meio empregado

identificação dos responsáveis pelo serviço
preservação de dados

quebra de sigilo de dados telemáticos: IP

quebra de sigilo de dados telemáticos: conexão

comprovação da autoria e da materialidade

Ministério Público nas ELEIÇÕES 2026

4.1 Investigação para identificar o usuário

USUÁRIO → INTERNET → APLICAÇÕES DA INTERNET

PROVEDOR DE CONEXÃO:

TIM vivo Claro Brasil

PROVEDOR DE APLICAÇÃO
ou
PROVEDOR DE CONTEÚDO

Google

WhatsApp

mercado livre

Ministério Público nas ELEIÇÕES 2026

4.1 Investigação para identificar o usuário

- ✓**comunicação instantânea** (Whatsapp,Telegram…)?
- ✓**redes de relacionamentos** (Facebook, Instagram, X, TikTok)?
- ✓**página da web** (blogs, fotologs, sites)?
- ✓**e-mail** (@ gmail, hotmail, globo, terra...)?
- ✓**fóruns de discussão** (yahoo groups...)?
- ✓**sala de bate-papo** (chats)?

4.1 Investigação para identificar o usuário

1. IDENTIFICAÇÃO DOS RESPONSÁVEIS PELO SERVIÇO

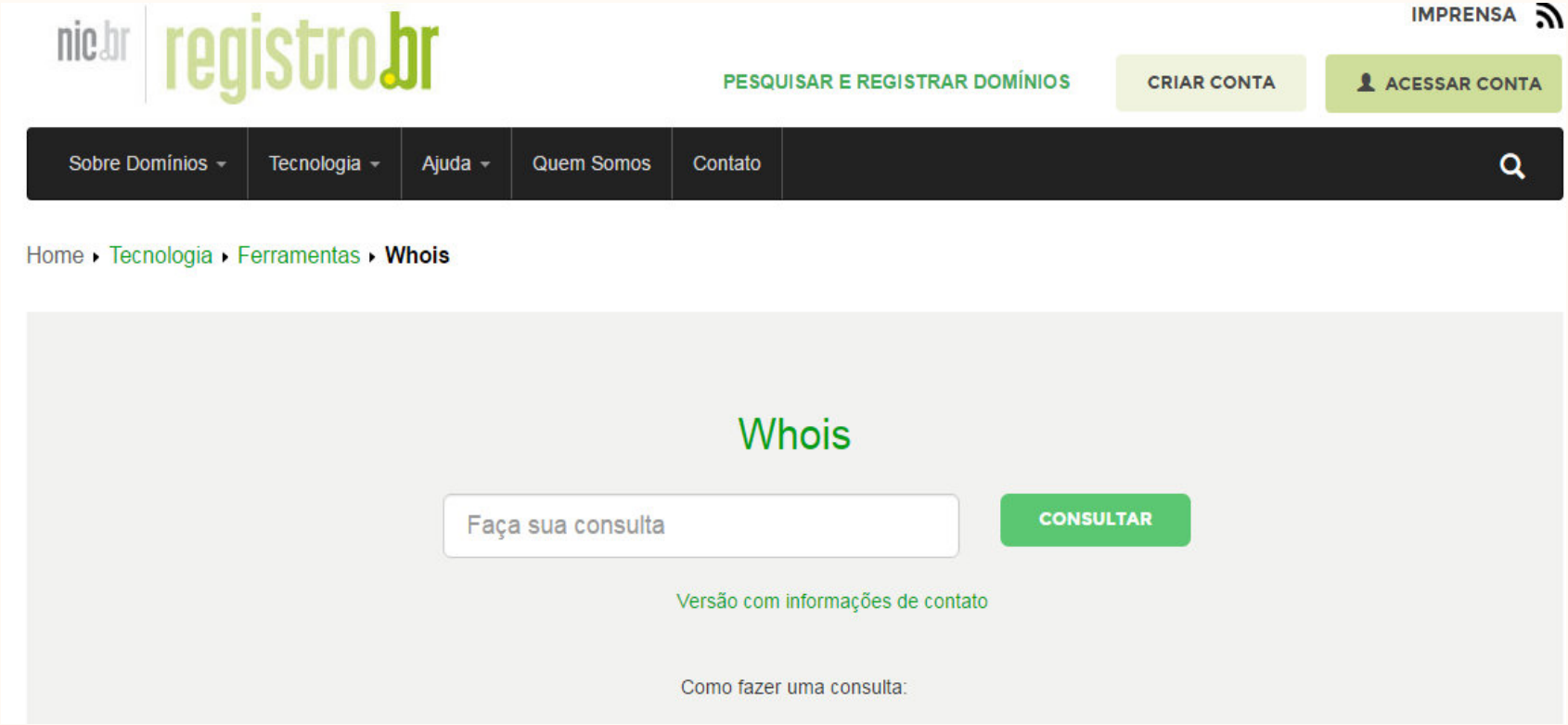
- Endereços nacionais (.br) → https://registro.br

- Endereços estrangeiros→ http://whois.icann.org

Ministério Público nas ELEIÇÕES 2026

4.1 Investigação para identificar o usuário

1. IDENTIFICAÇÃO DOS RESPONSÁVEIS PELO SERVIÇO



4.1 Investigação para identificar o usuário

2. PRESERVAÇÃO DAS PROVAS (cadeia de custódia)

Salvar e garantir integridade dos dados:

- Evidência/Prova Digital: volátil
- Autenticidade: **garantir que a evidência digital veio mesmo de onde se alega (certificar gerando um código *hash*, código aritmético que confere uma impressão digital única do arquivo)**
- Integridade: **garantir que o manuseio da prova não a altera**

4.1 Investigação para identificar o usuário

2. PRESERVAÇÃO DAS PROVAS (cadeia de custódia)

✓notificar provedor para preservar registros de acesso à aplicação de internet e *logs* de postagens (*uploads*) e acessos (sempre avisar que **não notifique** o usuário dos dados);

✓obrigação dos provedores de retenção (salvo conteúdo) e preservação por período superior;

✓ os principais provedores de aplicações de internet disponibilizam portais para realização desse pedido de preservação.

4.1 Investigação para identificar o usuário

3. QUEBRA DE SIGILO DE DADOS TELEMÁTICOS (IP)

•**pedido judicial** para obtenção dos registros de acesso à aplicação de internet e *logs* de postagens (*uploads*) e acessos (Art. 15, MCI), indagando:

•endereço IP;
•data, horário e referência GMT da conexão;
•porta lógica;
•dados como *email*, nome cadastrado, *nickname* (pode ser usado em outros aplicativos).

✓se não houver vínculo do provedor com o Brasil, necessário recorrer à cooperação jurídica internacional.

4.1 Investigação para identificar o usuário

3. QUEBRA DE SIGILO DE DADOS TELEMÁTICOS (IP)

User RAW IP Data

ID 810836003439[redacted], "carlos [redacted]", carlos[redacted]@gmail.com

Orkut Account

Profile URL:	http://www.orkut.com/Profile.aspx?uid=81083600343[redacted]
First Name:	"carlos"
Last Name:	"[redacted]"
Status:	Removed, Login Deleted (HARD DELETED)
Signup Date:	2012/12/15-15:06:26-UTC
Last Login:	-

Google Account

Account Name:	"carlos [redacted]"
Primary e-Mail:	carlos[redacted]@gmail.com
Secondary e-Mail:	carlos[redacted]@bol.com.br
Other e-Mails:	carlosn[redacted]@bol.com.br
Status:	Disabled User deleted account, from -, Geo: -, on -
Services:	Doritos, Gmail, Google me, Google profile, Has plusone, Orkut, Picasa, Search history, Talk
Unregistered Services:	-
Created on:	2012/12/15-15:06:09-UTC
IP:	189.27.83.2 (on 2012/12/15-15:06:09-UTC)
Geo:	BRAZIL (BRA), Mato Grosso do Sul, Campo Grande
Lang:	pt_BR
Previous e-Mails:	-
Countries in IP data:	BRAZIL

Available User IP Logs

Time	Event	IP	Geo
2012/12/18-12:46:47-UTC	Login Attempt	189.27.82.250	BRAZIL (BRA), ms, campo grande
2012/12/15-15:16:33-UTC	Logout	189.27.83.2	BRAZIL (BRA), ms, campo grande
2012/12/15-15:06:09-UTC	Login	189.27.83.2	BRAZIL (BRA), ms, campo grande

DONE

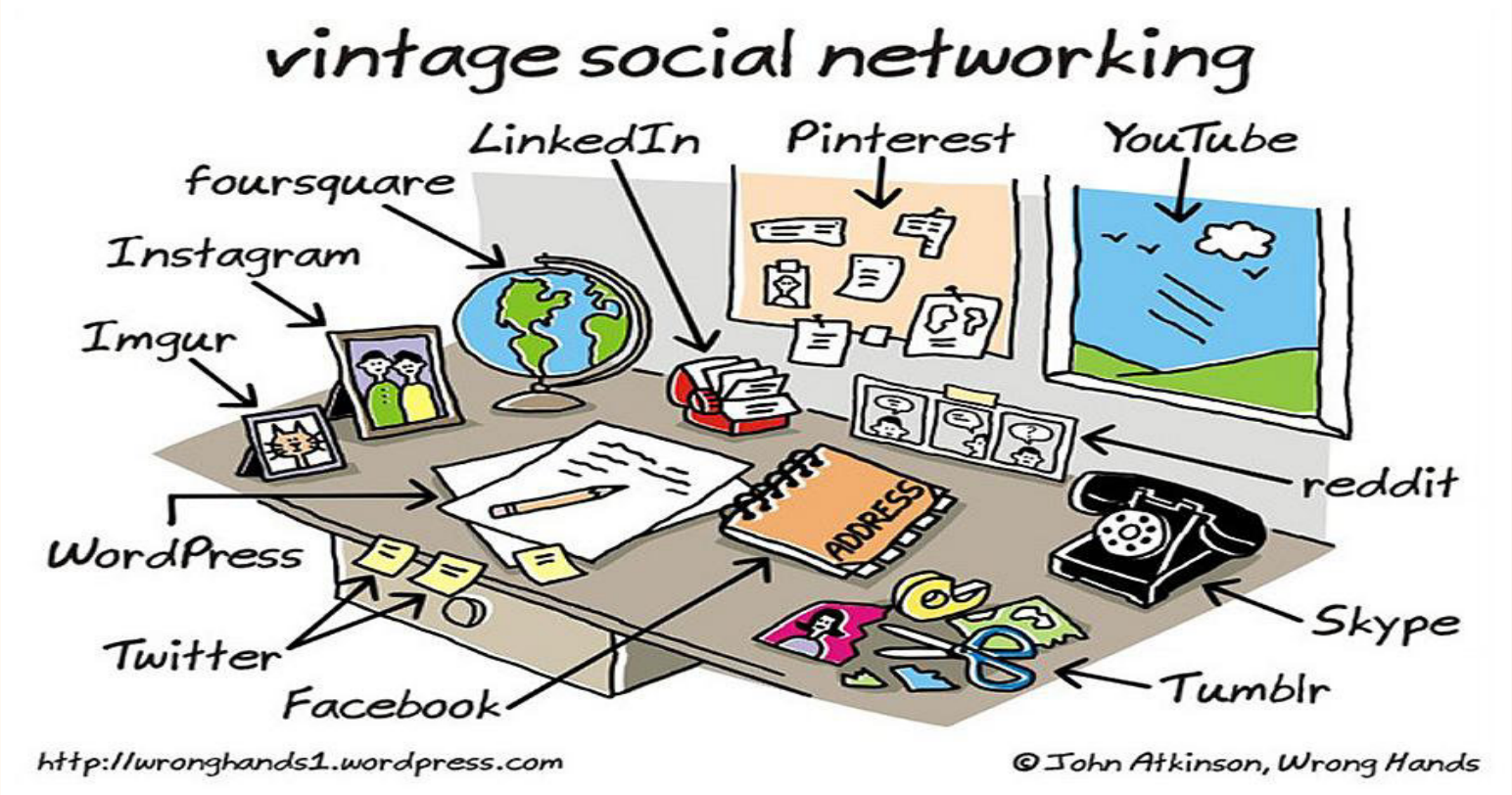
4. QUEBRA DE SIGILO DE DADOS TELEMÁTICOS (DADOS CADASTRAIS DO USUÁRIO)

Visa identificar a máquina de onde o fato foi praticado, a partir do IP fornecido (Art. 13, MCI)

- ✓em geral, a expedição de ofício é para concessionária de telefonia ou portal (PORTALJUD-Telefônica, Vivo).
- ✓pedido e ofício devem fazer referência obrigatória a:
  - endereço IP (indicado pelo prov. de aplicação);
  - data, horário e referência GMT da conexão;
  - porta lógica (Art. 9º-G, §2º, III, Res. TSE nº 23.610/19 incluído Res 23732/24)
- ✓endereços: www.registro.br

5. COMPROVAÇÃO DA MATERIALIDADE E DA AUTORIA – BUSCA E APREENSÃO

Especificidades na Obtenção de Provas Digitais – cuidados na coleta e preservação

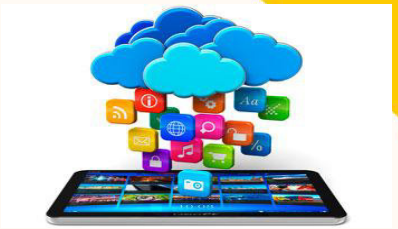


5. COMPROVAÇÃO DA MATERIALIDADE E DA AUTORIA – BUSCA E APREENSÃO

- ✓ Precedida de ordem de missão policial.
- ✓ Busca e apreensão do terminal (autorização para acesso aos dados e arquivos), pen drives, HD externo.
- ✓ oitiva do assinante da conexão - no local (STF - RECLAMAÇÃO 33.711:ouvir sem advertir sobre o direito ao silêncio).
- ✓ **Celulares:** STF **2007**, bastava mandado genérico. STJ **2016** HC 51.531/ REsp 1.727.266/SC, j.05/06/2018 - autorização específica para conteúdo do celular no flagrante (dados e conversas). **STF Repercussão Geral ARE1.042.075/24.11.17, Rel. Min. Dias Toffolli -** acesso a agenda e a histórico de ligações deve ter prévia ordem judicial - tema de repercussão geral (mérito pendente).

4.1 Investigação para identificar o usuário

Armazenamento na Nuvem



a) sincronização com a nuvem – busca e apreensão a partir do local do terminal (senha);

b) pedido de apreensão virtual para a empresa que presta o serviço de *cloud computing.* O conteúdo armazenado na nuvem nem sempre é criptografado (*backup* nos serviços do Google Drive, iCloud etc).

Garantir a cadeia de custódia:

laudo pericial no computador e demais materiais apreendidos/ no local, agente técnico especializado/*software,* que verifica *hashes.*

4.1.1 Investigação em site

Link de sites com postagens falsas

1º passo – preservação com a coleta da prova (prova a existência da página). Setor pericial/técnico colerá adequadamente a prova para que se ateste que a evidência noticiada corresponde ao publicado. Essa extração gerará um código *hash* da URL (Uniforme Resource Locator - combinação única de letras, números e/ou caracteres, que localiza certo conteúdo único na internet)

2º passo – identificação de onde o *site* está hospedado.
O serviço de hospedagem (exs.: GoDaddy, UOL ou WordPress), em geral, informa os dados da pessoa que criou o *site* malicioso, o IP de criação e os *logs* de acesso ao *site*.

4.1.1 Investigação em site

Link de sites com postagens falsas

Serviço de anonimização – uma empresa de privacidade *on-line*, que registra o *site* na empresa de hospedagem, no lugar do real proprietário daquele domínio. Essa empresa possui os dados do real proprietário (dados cadastrais e financeiros).

Para consulta dos provedores de hospedagem e anonimização – https://registro.br (nacionais) ou https://Whois.icann.org (estrangeiros).

Sem vínculo com o Br - aba ou *e-mail* para reportar abusos – pode avisar a empresa sobre o conteúdo ilícito, pedindo a **preservação dos dados e a remoção do *site***. Pedir auxílio à PF, por meio do *e-mail* cybercrime_brazil_24x7@dpf.gov.br

4.1.1 Investigação em site

Link de sites com postagens falsas

3º passo – pedido de preservação de registros de criação do *site* e *logs* de acesso (IPs, data e hora) e de remoção do *site* malicioso

A empresa de hospedagem, ou anonimização, deve ser oficiada para preservar os dados do real usuário (dados do IP de criação da conta e *logs* de acesso, e dados cadastrais, inclusive financeiros) para posterior ordem judicial para envio dos dados.

4º passo – decisão judicial de quebra de sigilo telemático

Sem vínculo do provedor de hospedagem e/ou anonimização no Brasil - procedimento de cooperação jurídica internacional.

4.1.2 Investigação no Facebook e Instagram

1º passo – pedido de preservação no portal **https//: www.facebook.com/records. Hash e print da página.**

Precisa da **identificação correta da URL** do perfil que se pretende investigar.

As URLs das contas podem ser investigadas com:

a) o número de identificação do usuário (http://www.facebook.com/profile.php?id=1000000XXXXXXXX) ou o nome de usuário do perfil do Facebook, (http://www.facebook.com/nomedeusuario);
b) endereço de *e-mail* e
c) número de telefone (+55, DDD, número).

4.1.2 Investigação no Facebook e Instagram

Para localizar a URL:

No **computador**, ao acessar o **perfil**, a URL é exibida na barra de endereços do navegador. Se específica de uma **publicação ou comentário**: clique na respectiva data ou hora de disponibilização, que a URL aparecerá 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.

Ministério Público nas ELEIÇÕES 2026

4.1.2 Investigação no Facebook e Instagram

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.

Portal FACEBOOK para autoridades

- cadastro prévio (*e-mail* institucional)
- recebimento de link por e-mail
- acesso limitado por 1 hora
- solicitação de preservação de dados do Facebook e Instagram

Ministério Público nas ELEIÇÕES 2026

4.1.2 Investigação no Facebook e Instagram

HTTP://WWW.FACEBOOK.COM/RECORDS

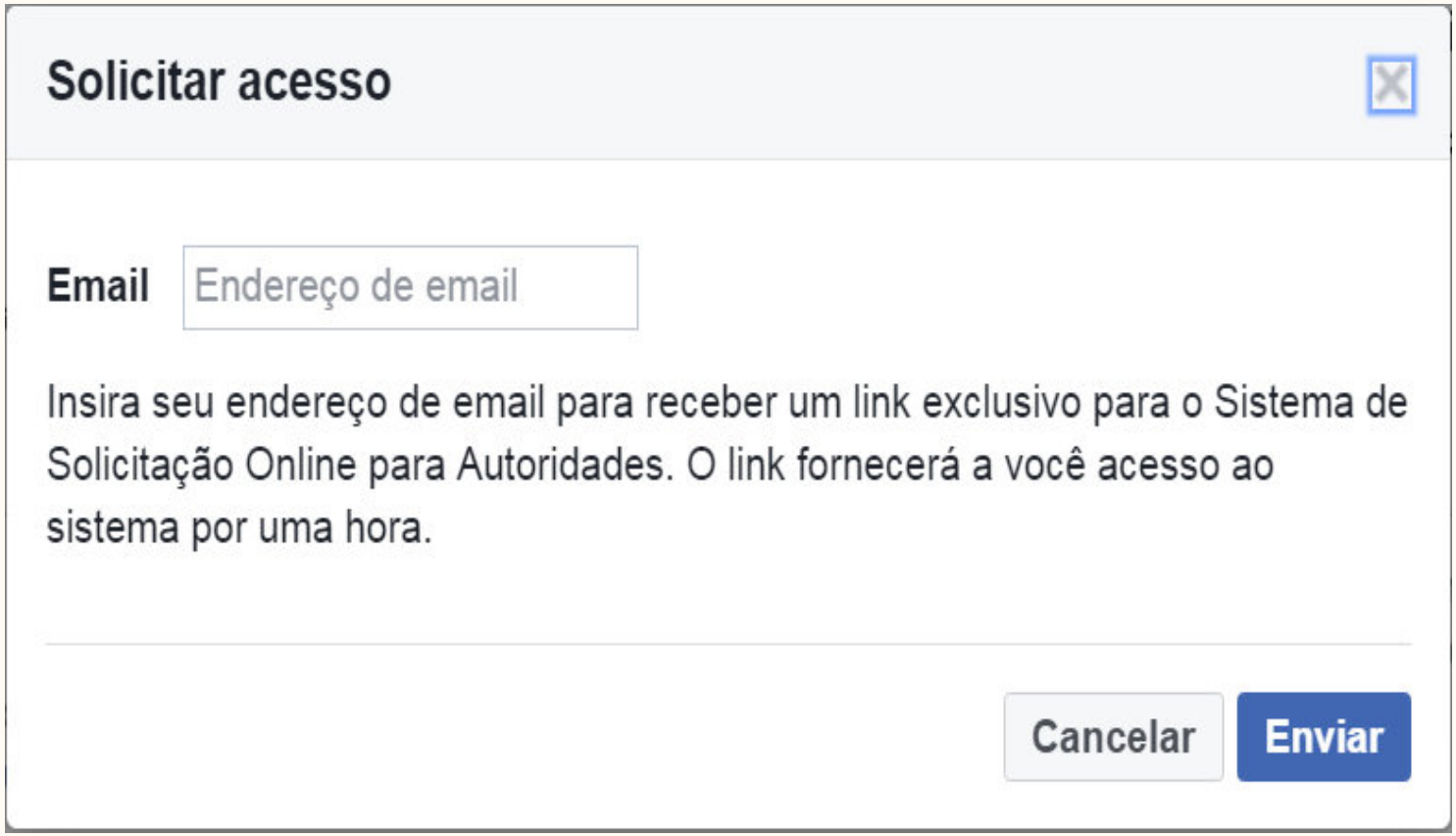
(ACESSO EXCLUSIVO PARA AUTORIDADES)

Ministério Público nas ELEIÇÕES 2026

4.1.2 Investigação no Facebook e Instagram

HTTP://WWW.FACEBOOK.COM/RECORDS

(ACESSO EXCLUSIVO PARA AUTORIDADES)

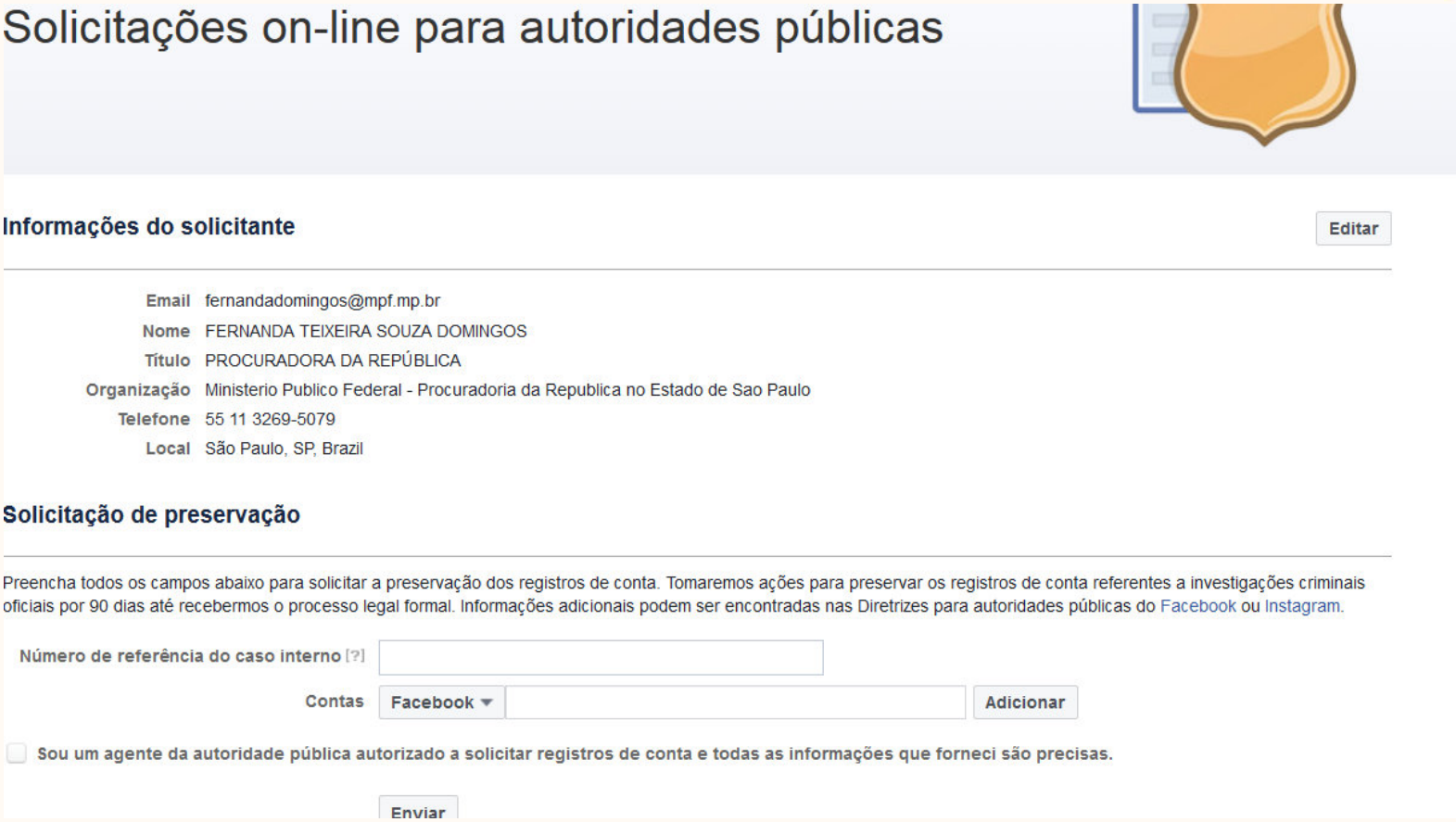


Ministério Público nas
ELEIÇÕES 2026

4.1.2 Investigação no Facebook e Instagram

HTTP://WWW.FACEBOOK.COM/RECORDS

(ACESSO EXCLUSIVO PARA AUTORIDADES)



Ministério Público nas ELEIÇÕES 2026

4.1.2 Investigação no Facebook e Instagram

O Sistema de Solicitação On-Line para Autoridades, localizado em **facebook.com/records**, está à disposição das Autoridades Policiais ou do Ministério Público para o envio, rastreamento e processamento de solicitações. Como proceder:

1) Acesse www.facebook.com/records;
2) Clique no item "*Sou um agente autorizado da autoridade política e esta é uma solicitação oficial*";
3) Clique em "*Solicitar acesso*";
4) Digite o seu endereço de **e-mail institucional** (exemplo: endereços terminados em gov.br, jus.br ou mp.br);
5) No e-mail cadastrado, você receberá uma mensagem com um link onde poderá submeter o pedido de acesso a registros. O link ficará disponível por uma hora.
6) Clique no link do e-mail recebido;
7) Clique em "*Solicitação de registros*" no topo da página;
8) Assegure-se de que as suas informações estão corretas. Se necessário, clique em "*editar*" para alterá-las;
9) Insira os dados solicitados;
10) "Número de referência do caso interno": n° IPL, proc ou PIC.

4.1.2 Investigação no Facebook e Instagram

2º passo - coleta adequada da prova - início à cadeia de custódia. As informações necessárias para acesso à publicação devem ser encaminhadas de imediato ao setor próprio para a extração do cálculo *hash;*

3º passo - se necessário, **pedido de retirada do conteúdo,** se ferir os termos de uso; diretamente ao Facebook (*e-mail* para records@facebook.com, com o *link* do conteúdo a ser retirado). – obter a URL específica da postagem que se quer remover, sob pena de ser retirado também conteúdo lícito;

4º passo – decisão cautelar de quebra de sigilo telemático para obtenção dos registros de acesso à aplicação e de *upload* e acessos, e, se necessário, **decisão judicial de retirada do conteúdo.** Ofícios pelo portal.

Ministério Público nas
ELEIÇÕES 2026

4.1.3 Investigação no WhatsApp

Ministério Público nas ELEIÇÕES 2026

4.1.3 Investigação no WhatsApp

Dois meios diferentes de propagação:

1) Envio de arquivo ou mensagem no aplicativo – **Preservação no Portal www.whatsapp.com/records** e investigação padrão.

2) Envio de ***link*** que remete a outro *site* na internet, onde efetivamente está o conteúdo ilícito. Não basta excluir a mensagem, porque o *link* continuará funcionando – investigação tem que seguir o padrão do item sobre **Desinformação em *sites*.**

É necessário informar o telefone do usuário.

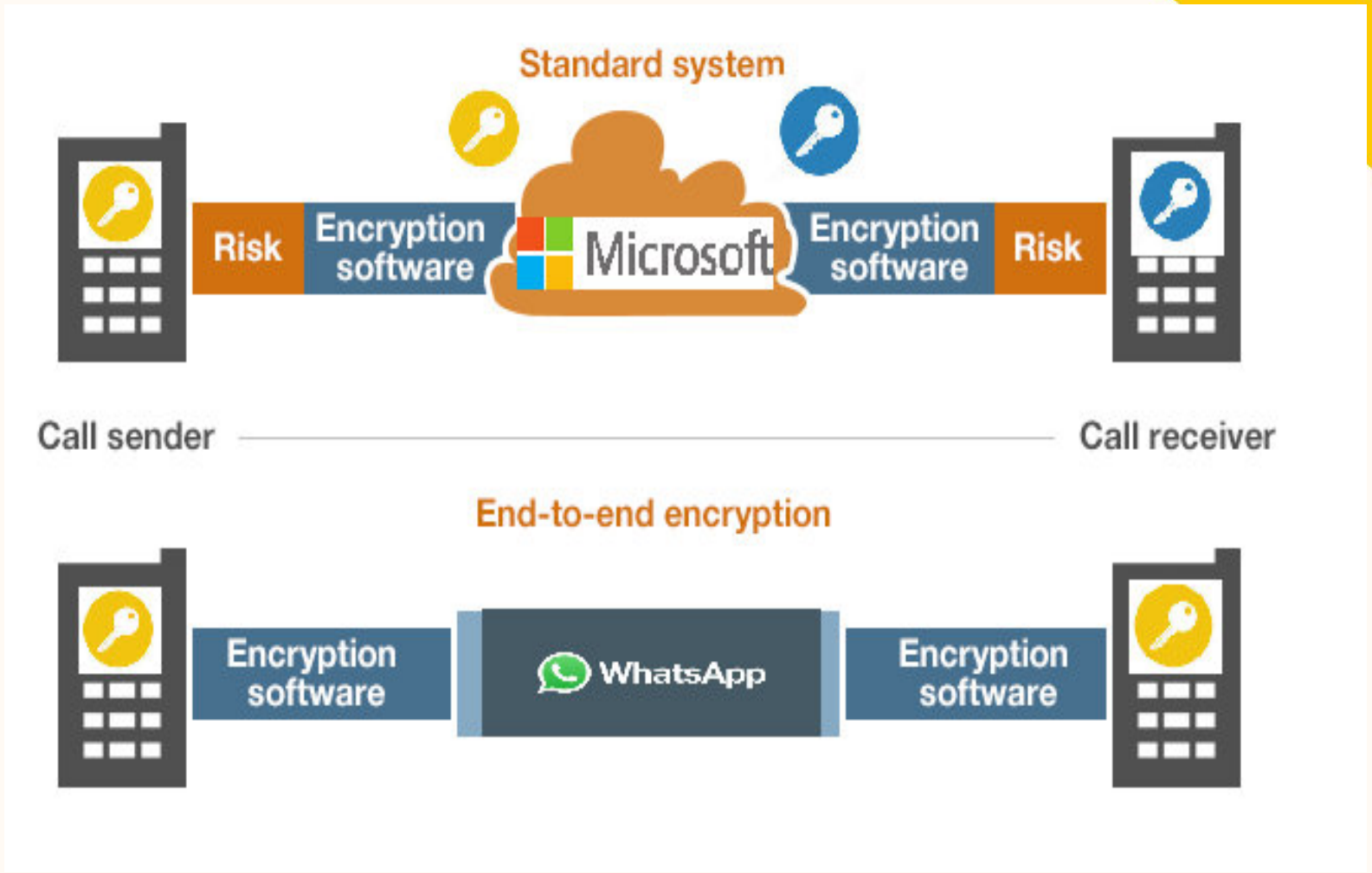
Ministério Público nas ELEIÇÕES 2026

4.1.3 Investigação no WhatsApp

Portal - HTTP://WWW.WHATSAPP.COM/RECORDS

Ministério Público nas
ELEIÇÕES 2026

4.1.3 Investigação no WhatsApp



Ministério Público nas ELEIÇÕES 2026

4.1.3 Investigação no WhatsApp

WHATSAPP - dados que podem ser solicitados (por ofício, via o portal www.whatsapp.com/records)

COM mandado judicial

(Medida cautelar)

- Informações de grupos (nomes e ID), de quais o investigado é administrador, participa e dos participantes
- Mudanças de números
- Agenda de Contatos
- Última conexão com IP, porta, data, hora

SEM mandado judicial

(Dados de Perfil):

- Nome
- Foto
- Telefone
- Modelo do Aparelho
- Versão do aplicativo
- *status* da conexão
- endereço de *e-mail*
- Informações do cliente WEB.

Ministério Público nas ELEIÇÕES 2026

4.1.3 Investigação no WhatsApp

Comunicação pelo WhatsApp, por utilizar Criptografia ponta-a-ponta, não se pode obter o conteúdo, mas, por medida cautelar de interceptação telemática, é possível obter os dados das comunicações:

1) **Extratos de mensagens: informações de remetente, destinatário, data e hora da mensagem;**
2) **tipo de mensagem;**
3) **IP da conta alvo, se disponível.**

Pode ser pedido que as informações sejam entregues a cada 24 h, a partir da implantação da medida até 15 dias seguintes.

Ministério Público nas ELEIÇÕES 2026

4.1.4 Investigação no Youtube

1ºpasso - pedido de preservação de dados pelo sistema *on-line* de Law Enforcement Request System da Google acessível pelo **portal http://lers.google.com**, na qual será necessária a criação de conta **(pedir que o usuário não seja notificado pelo prazo x).**
Ex. de uma URL de um vídeo específico:
https://www.youtube.com/whatch/v=2y-5hfZWADI

2º passo - coletar a evidência digital noticiada por meio de ferramentas forenses para extração do código hash;

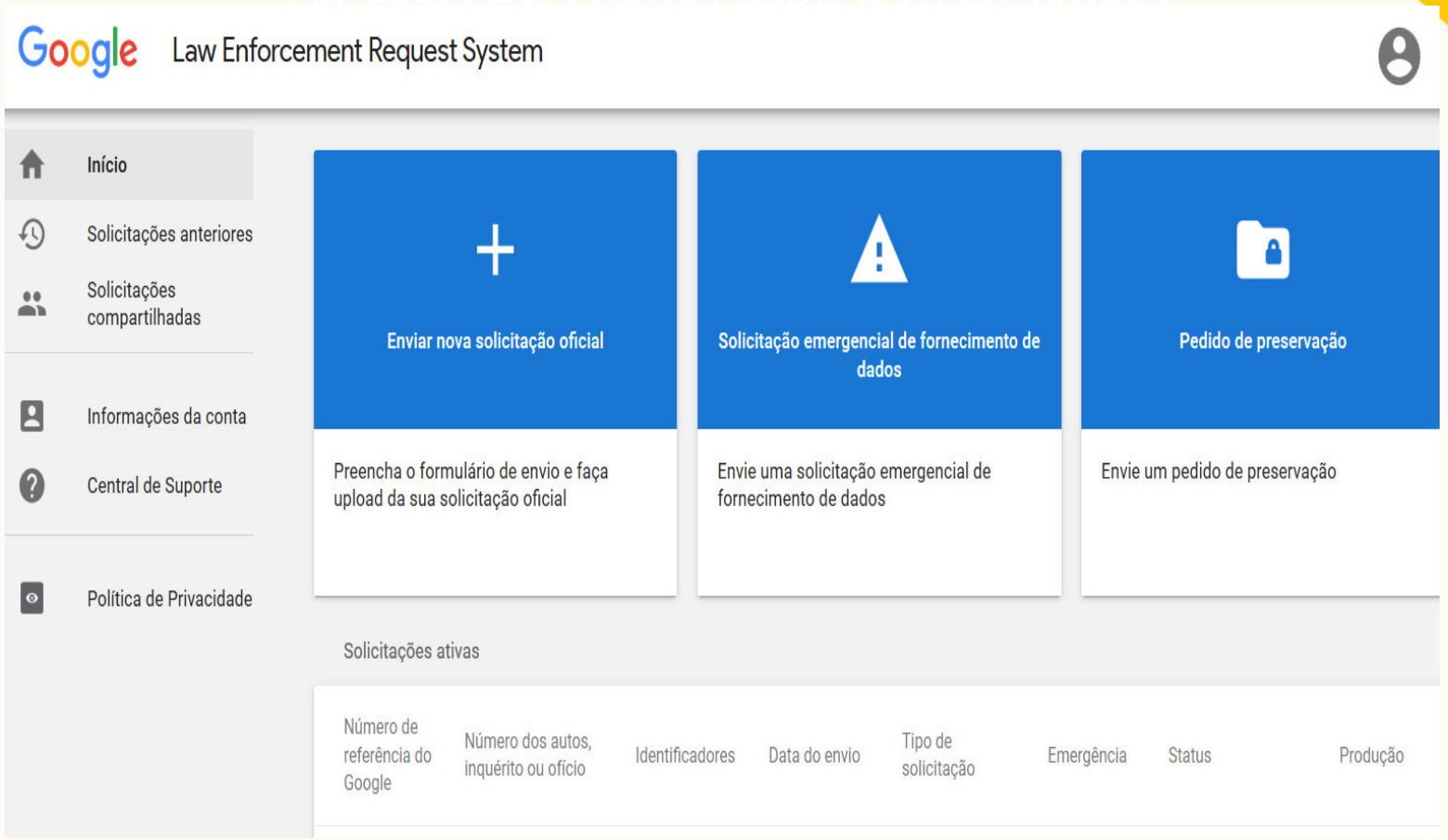
3º passo – pedido de retirada do conteúdo nocivo, caso viole seus Termos de Serviço: https://www.youtube.com/reportingtool/legal;

Ministério Público nas
ELEIÇÕES 2026

4.1.4 Investigação no Youtube

http://lers.google.com

(ACESSO EXCLUSIVO PARA AUTORIDADES)



Ministério Público nas ELEIÇÕES 2026

4.1.4 Investigação no Youtube

4º passo – decisão cautelar de quebra de sigilo telemático, e, se necessário, decisão judicial de retirada do conteúdo; para obtenção das seguintes informações, entre outras:

- *logs* de acesso (IP, porta, 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 armazenadas no Google Photos, dados armazenados no Google Drive, etc.

Oficios podem ser enviados também pelos *e-mails*: lis-latam@google.com e juridicobrasil@google.com

Ministério Público nas ELEIÇÕES 2026

4.1.5 Investigação no X

1º passo - pedido de preservação de dados era pelo sistema *on-line* https://legalrequests.twitter.com. **Infelizmente, em 2022, foi descontinuado o portal. Pedido de preservação e todos os demais devem ser para o email do X** (para o eleitoral o prov indica endereço distinto).

Deve conter a identificação do perfil infringente:
a) **nome do usuário e o URL do perfil do Twitter** envolvido (por exemplo, https://twitter.com/twittersafety (@twittersafety);
b) o **número de identificação do usuário ou UID exclusiva e pública da conta no Twitter** ou um **nome de usuário e URL do Periscope** (ex: @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#.

Ministério Público nas ELEIÇÕES 2026

4.1.5 Investigação no X

2º passo - coletar a evidência por meio de ferramentas forenses e extração do hash;

3º passo - retirada do conteúdo, se necessária. Seguir as orientações publicadas em https://help.x.com/pt/rules-and-policies/x-law- enforcement-support#;

4º passo – decisão cautelar de afastamento de sigilo telemático, e, se necessário, decisão judicial de retirada do conteúdo.

Ministério Público nas ELEIÇÕES 2026

4.1.5 Investigação no X

Informações que podem ser obtidas sobre o usuário:

- *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
- nº 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

Ministério Público nas ELEIÇÕES 2026

4.1.5 Investigação no X

Atribuíam o “selo azul de verificação” às contas de interesse público. Analisavam os dados fornecidos pelos titulares e confirmavam que esses eram autênticos e que efetivamente pertenciam à pessoa ou à marca que representavam (v.https://help.x.com/pt/managing-your- account/twitter-verified-accounts).Tal informação podia ajudar a verificar se o tweet investigado partiu realmente do titular da conta.

Atualmente, essas contas verificadas são pagas, e o serviço chama-se **PREMIUM X**, então a confiabilidade sobre essa verificação é relativa.

Ministério Público nas ELEIÇÕES 2026

5. Estratégia de Enfrentamento à Desinformação da PGE

Procuradoria Geral Eleitoral/2ª Câmara Criminal - PGR criaram:

Grupo de Trabalho sobre Desinformação na Internet, interferência cibernética na Democracia e influência nas Eleições (Portaria PGE/2ª CCR nº 1, de 21/10/2025).

Parceria: Instituto de Tecnologia e Sociedade do Rio (ITS-Rio) para **capacitação de membros do MPE e servidores** e,

Monitoramento de programas de IA dos principais provedores usados no País sobre as campanhas pres/gov/sen para verificar se foram respeitados padrões aceitáveis ou não nas respostas, com relatórios mensais ao GT de Desinformação na internet.

Monitoramento de notícias jornalísticas sobre desinformação eleitoral na internet e envio para o GT distribuir as notícias para as PREs com atribuição.

Ministério Público *nas*
ELEIÇÕES 2026

CONTATO

Neide Cardoso de Oliveira **neidec@mpf.mp.br**

Procuradora Regional da República

Coordenadora do Grupo de Trabalho de Desinformação na Internet, interferência cibernética na Democracia e processo eleitoral (GTDIE)

Obrigada !

Ministério Público *nas*
ELEIÇÕES 2026

Guia Prático sobre Investigação e Desinformação 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

Secretária de Cooperação Jurídica Internacional
AnaMara Osório Silva

Ouvidor-Geral do Ministério Público Federal
Brasilino Pereira dos Santos

Corregedor-Geral do Ministério Público Federal
Elton Ghersel

Secretário-Geral
Eliana Peres Torelly de Carvalho

GRUPO DE TRABALHO SOBRE DESINFORMAÇÃO NA INTERNET, INTERFERÊNCIA CIBERNÉTICA NA DEMOCRACIA E INFLUÊNCIA NAS ELEIÇÕES

Procuradora Regional da República
Neide M. C. Cardoso de Oliveira

Procuradora Regional da República
Fernanda Domingos Teixeira

Eleições 2026:
Guia prático sobre investigação e desinformação na internet

Realização

Grupo de Trabalho sobre Desinformação na Internet, interferência cibernética na Democracia e influência nas Eleições (baseado no *Guia prático de investigação na internet e Covid-19,* do GACC-2021)

Autoras

Neide M. C. Cardoso de Oliveira

Procuradora Regional da República na 2ª Região. Coordenadora do Grupo de Trabalho sobre Desinformação na Internet, interferência cibernética na Democracia e influência nas Eleições (GTDIE). Coordenadora adjunta do Grupo de Atuação Especial sobre Crimes Cibernéticos da 2ª Câmara Criminal (GACCTI) da 2ª Câmara Criminal da PGR. 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.

Fernanda Teixeira Souza Domingos

Procuradora Regional da República na 3ª Região. Coordenadora-adjunta do Grupo de Trabalho Grupo de Trabalho sobre Desinformação na Internet, interferência cibernética na Democracia e influência nas Eleições. Coordenadora do Grupo de Atuação Especial sobre Crimes Cibernéticos e Crimes mediante o uso de Tecnologias da Informação (GACCTI) da 2ª Câmara Criminal da PGR. Graduada em Direito pela Universidade do Estado de São Paulo (USP). Mestrado em Direito Internacional e em Direito da Internet e Sistemas da Informação pela Universidade de Estrasburgo, França.

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 propaganda eleitoral), no 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, a 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[3] no mundo. Assim, cada região do globo recebeu um lote de IPs (Internet Protocol) para gerir.

No Brasil, o Núcleo de Informação e Coordenação do .br (NIC.br)[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, artigo 37, inciso 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 executivodo 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 identificada, 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 informavam que vários (centenas/milhares) clientes seus utilizaram o mesmo número de IP, na data e horário requisitados.

Todo esse problema acabou com a recém publicação do Decreto nº 12975, de 20/5/26[5], que alterou o Decreto nº 8771/2016, que regulamenta o Marco Civil da Internet, e agora prevê a obrigatoriedade de guarda da porta lógica para os provedores de conexão e de aplicação, como mais um dado a ser armazenado da mesma forma que o IP, data e hora.

Indico *links*[6] de vídeos explicativos produzidos pelo NIC.br, que dão uma explicação didática sobre o funcionamento da internet.

---

[5] Art. 15-A. O dever de guarda de registros de endereço IP pelos provedores de conexão e pelos provedores de aplicações deinternet, previsto nos art. 13 e art. 15 da Lei nº 12.965, de 23 de abril de 2014, abrangerá a porta lógica de origem associada sempre que necessário para a identificação inequívoca do terminal de origem ou do próximo enlace de rede. § 1º O dever de guarda da porta lógica de origem independerá de prévia requisição e recairá autonomamente sobre cada provedor. § 2º O fornecimento da porta lógica de origem e dos dados a ela vinculados observará o disposto nos art. 10 e art. 22 da Lei nº 12.965, de 23 de abril de 2014. (NR)

[6] 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 internet 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[7] 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,

desde que providenciem o ingresso do pedido de autorização judicial para o acesso aos dados no

[7] 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 públicobrasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

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)**[8]**,** 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**[9]**:** 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**[10]**:** 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, o 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. Além disso, o Decreto n° 11.491/2023, que internalizou a Convenção de Budapeste sobre os Crimes Cibernéticos no ordenamento jurídico brasileiro traz um conceito mais amplo de dados cadastrais, estatuindo serem todas as informações em poder do provedor de serviços referentes ao assinante de seus serviços,

---

[8] 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.

[9] Res. TSE 23.610/2019, Art. 37, inc. VI.

[10] Res. TSE 23.610/2019, Art. 37, inc. VIII.

excetuando-se dados de tráfego e de conteúdo, que possam determinar a identidade do assinante ou auxiliar nessa determinação.

> Artigo 18 – Ordem de exibição
> 1.(...)
> 2.(...)
> 3. Paras os fins deste Artigo, o termo "informações cadastrais do assinante" indica qualquer informação mantida em forma eletrônica ou em qualquer outra, que esteja em poder do provedor de serviço e que seja relativa a assinantes de seus serviços, com exceção dos dados de tráfego e do conteúdo da comunicação, e por meio da qual se possa determinar:
> a. o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas para esse fim e a época do serviço;
> b. a identidade do assinante, o domicílio ou o endereço postal, o telefone e outros números de contato e informações sobre pagamento e cobrança, que estejam disponíveis de acordo com o contrato de prestação de serviço.
> c. quaisquer outras informações sobre o local da instalação do equipamento de comunicação disponível com base no contrato de prestação de serviço.

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 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 (MCI) 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, inc. 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 ao 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

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), e 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) 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 da aplicação Facebook, do provedor de aplicação Meta, que acabou sendo incorporada a 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 (paga). Suas características:

> 1) é um serviço oferecido na internet (atualmente pelas redes sociais Facebook e Instagram, ambos do provedor Meta), incluindo a priorização em serviços de busca na internet (art.28, § 7º-A da Res.TSE 23610/19);
> 2) só pode ser contratado exclusivamente por partidos, federações, coligações, candidata(o)s e seus representantes (art. 29, caput, da Res. TSE 23610/19);
> 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, art. 29, Res TSE 23610/19);
> 4) só pode ser contratado para promover ou beneficiar candidatura (vedada a propaganda negativa - art.28, § 7º-A da Res.TSE 23610/19).

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).

VI) Detecção de Desinformação eleitoral

O conceito de desinformação abrange a notícia notoriamente falsa (*fakenews*) ou a gravemente descontextualizada no tempo ou no espaço, nesse caso, a notícia que não é totalmente falsa, mas não corresponde exatamente à data em que ela está sendo publicada (no tempo) ou ao contexto da publicação (espaço). Por isso a importância da checagem sobre qualquer notícia. E a propagação de desinformação, em especial a eleitoral, aproveita-se da ignorância, do comodismo, da falta de tempo, das emoções do destinatário e da rivalidade política. Ela possibilita a manipulação do debate político. E no ambiente digital é difícil distinguir o que é propaganda, notícia ou opinião. A notícia falsa é formada por um conteúdo que visa *enganar o leitor usando estratégias para ocultar sua intenção. Isso significa que elas imitam a forma de uma notícia jornalística, inclusive em sua linguagem, mas seu conteúdo não guarda qualquer relação com os fatos e sua produção não implica em nenhum cuidado jornalístico*[11].

Boatos diversos – a checagem de informações sobre qualquer notícia passa por duas etapas: uma

[11] "*Internet, Democracia e Eleições – Guia prático para gestores públicos e usuários*", Núcleo de Informação e Coordenação do Ponto BR (NIC.br), São Paulo: Comitê Gestor da Internet no Brasil, 2018, p. 36.

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, deve-se 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.

O crime de desinformação eleitoral é previsto no Código Eleitoral de 1965, no artigo 323, mas existe no ordenamento jurídico brasileiro desde 1950, como leciona o jurista Luiz Carlos Gonçalves[12] e a redação do *caput* foi alterada e inclui-se dois parágrafos, pela Lei 14.192/2021, justamente para prever a sanção pela prática de desinformação em ambientes digitais e quando envolve menosprezo ou discriminação de gênero, cor, raça ou etnia, *in verbis*:

> Art. 323. Divulgar, na propaganda eleitoral ou durante período de campanha eleitoral, fatos que sabe inverídicos em relação a partidos ou a candidatos e capazes de exercer influência perante o eleitorado: (Redação dada pela Lei nº 14.192, de 2021)
> Pena - detenção de dois meses a um ano, ou pagamento de 120 a 150 dias-multa.
> Parágrafo único. Revogado. (Redação dada pela Lei nº 14.192, de 2021)
>
> § 1º Nas mesmas penas incorre quem produz, oferece ou vende vídeo com conteúdo inverídico acerca de partidos ou candidatos. (Incluído pela Lei nº 14.192, de 2021)
>
> § 2º Aumenta-se a pena de 1/3 (um terço) até metade se o crime: (Incluído pela Lei nº 14.192, de 2021)
> I - é cometido por meio da imprensa, rádio ou televisão, ou por meio da internet ou de rede social, ou é transmitido em tempo real; (Incluído pela Lei nº 14.192, de 2021)
> II - envolve menosprezo ou discriminação à condição de mulher ou à sua cor, raça ou etnia. (Incluído pela Lei nº 14.192, de 2021)

A Resolução TSE nº 23.732/2024 previu como dever do provedor de aplicação de internet, que veicule conteúdo político eleitoral (atualmente somente a Meta, por meio de suas redes sociais, Instagram e Facebook, oferece tais serviços, como já dito, a Google excluiu essa possibilidade no pleito de 2024), a adoção de medidas para impedir ou diminuir a circulação de fatos notoriamente inverídicos ou descontextualizados que atinjam a integridade do processo eleitoral e previu uma série de medidas[13].

---

[12] GONÇALVES, Luiz Carlos dos Santos. Investigação e processo dos crimes eleitorais e conexos. São Paulo: SaraivJur, 2022. p. 108.

[13] Art. 9º-D. É dever do provedor de aplicação de internet, que permita a veiculação de conteúdo político-eleitoral, a adoção e a publicização de medidas para impedir ou diminuir a circulação de fatos notoriamente inverídicos ou

O conteúdo do artigo eleitoral criminal sobre desinformação foi incluído na Resolução TSE nº 23610, em seus artigos 9º-E, caput, inciso II (além de outros crimes taxativamente citados nos demais incisos)[14] e 9º-F, *in verbis*:

> Art. 9º-E. Os provedores de aplicação serão solidariamente responsáveis, civil e administrativamente, quando não promoverem a indisponibilização imediata de conteúdos e contas, durante o período eleitoral, nos seguintes casos de risco: (Incluído pela Resolução nº 23.732/2024)
>
> I – (...)
> II – de divulgação ou compartilhamento de fatos notoriamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos; (Incluído pela Resolução nº 23.732/2024)
> III – (...)
> IV – (...).

Em 2024, o Tribunal Superior Eleitoral (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[15].

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/

gravemente descontextualizados que possam atingir a integridade do processo eleitoral, incluindo: (Incluído pela Resolução nº 23.732/2024) I - a elaboração e a aplicação de termos de uso e de políticas de conteúdo compatíveis com esse objetivo; (Incluído pela Resolução nº 23.732/2024) II - a implementação de instrumentos eficazes de notificação e de canais de denúncia, acessíveis às pessoas usuárias e a instituições e entidades públicas e privadas; (Incluído pela Resolução nº 23.732/2024); III – o planejamento e a execução de ações corretivas e preventivas, incluindo o aprimoramento de seus sistemas de recomendação de conteúdo; (Incluído pela Resolução nº 23.732/2024); IV - a transparência dos resultados alcançados pelas ações mencionadas no inciso III do caput deste artigo; (Incluído pela Resolução nº 23.732/2024); V – a elaboração, em ano eleitoral, de avaliação de impacto de seus serviços sobre a integridade do processo eleitoral, a fim de implementar medidas eficazes e proporcionais para mitigar os riscos identificados, incluindo quanto à violência política de gênero, e a implementação das medidas previstas neste artigo. (Incluído pela Resolução nº 23.732/2024); VI – o aprimoramento de suas capacidades tecnológicas e operacionais, com priorização de ferramentas e funcionalidades que contribuam para o alcance do objetivo previsto no caput deste artigo. (Incluído pela Resolução nº 23.732/2024). § 1º É vedado ao provedor de aplicação, que comercialize qualquer modalidade de impulsionamento de conteúdo, inclusive sob a forma de priorização de resultado de busca, disponibilizar esse serviço para veiculação de fato notoriamente inverídico ou gravemente descontextualizado que possa atingir a integridade do processo eleitoral. (Incluído pela Resolução nº 23.732/2024)

[14] I – de condutas, informações e atos antidemocráticos caracterizadores de violação aos artigos 296, parágrafo único; 359-L, 359- M, 359-N, 359-P e 359-R do Código Penal; (Incluído pela Resolução nº 23.732/2024); II – (...); III – de grave ameaça, direta e imediata, de violência ou incitação à violência contra a integridade física de membros e servidores da Justiça eleitoral e Ministério Público eleitoral ou contra a infraestrutura física do Poder Judiciário para restringir ou impedir o exercício dos poderes constitucionais ou a abolição violenta do Estado Democrático de Direito; (Incluído pela Resolução nº 23.732/2024); IV – de comportamento ou discurso de ódio, inclusive promoção de racismo, homofobia, ideologias nazistas, fascistas ou odiosas contra uma pessoa ou grupo por preconceito de origem, raça, sexo, cor, idade, religião e quaisquer outras formas de discriminação; (Incluído pela Resolução nº 23.732/2024)

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

- Agência Estado: https://politica.estadao.com.br/blogs/estadao-verifica/
- Grupo Globo: https://g1.globo.com/fato-ou-fake/

Além disso, a aplicação 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 a cartilha produzida pelo NIC.br: 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, e também, no período eleitoral como o 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. Se não houver 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 aplicativos, evite fornecer dados e permissões desnecessários.

A nova Resolução 23755/2026 incluiu o artigo 38-A na Resolução nº 23.610/2019, para permitir a remoção de perfil falso, apócrifo (anônimo) ou de cuja pessoa não exista no mundo real (automatizado ou robo) que reiteradamente publique(m) desinformação que possa(m) atingir a integridade do processo eleitoral assim reconhecidos pela Justiça Eleitoral, *in verbis*:

> Art. 38-A. A remoção de perfil será feita quando se tratar de usuário comprovadamente falso, apócrifo ou vinculado a pessoa que sequer exista fora do universo digital (perfil automatizado ou robô), cujas publicações configurem a reiterada prática: (Incluído pela Resolução nº 23.755/2026)

> I - de crime eleitoral; (Incluído pela Resolução nº 23.755/2026)
> II - de publicação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam atingir a integridade do processo eleitoral, que tenham sido assim reconhecidos pela Justiça Eleitoral. (Incluído pela Resolução nº 23.755/2026)
> § 1º As determinações de remoção de perfil serão aplicadas em processo judicial em que seja assegurada a ampla defesa e o contraditório. (Incluído pela Resolução nº 23.755/2026)
> § 2º É permitida a exclusão pelos provedores de aplicação apenas nas hipóteses de perfis falsos, automatizados ou robô. (Incluído pela Resolução nº 23.755/2026)

Outra grande novidade introduzida, pela nova Resolução TSE nº 23.755/2026 na Resolução TSE nº 23.610/2019, foi a alteração da responsabilidade civil dos provedores de aplicação sobre o conteúdo de informações falsas ou sem comprovação técnica que descredibilizem a integridade do sistema eletrônico de votação e a publicação de fatos que configurem crimes ali indicados em seus serviços, tornando-os responsáveis pela remoção desse tipo de conteúdo, independente de ordem judicial. Observe-se a diferença entre o § 4º em sua redação original, mantido para os conteúdos impulsionados para os provedores que o comercializam no período eleitoral, e a dos novos § 4º-A e B, do artigo 28, *in verbis*:

> § 4º O provedor de aplicação de internet que possibilite o impulsionamento pago de conteúdos deverá contar com canal de comunicação com suas usuárias e seus usuários e somente poderá ser responsabilizado por danos decorrentes do conteúdo impulsionado se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente pela Justiça Eleitoral (Lei nº 9.504/1997, art. 57-B, § 4º) .
>
> § 4º-A. O disposto no § 4º não se aplica quando o conteúdo veicular: (Incluído pela Resolução nº 23.755/2026)
>
> I - informações falsas ou sem comprovação técnica que descredibilizem a integridade do sistema eletrônico de votação; (Incluído pela Resolução nº 23.755/2026)
>
> II - incitação de crimes contra o Estado Democrático de Direito; (Incluído pela Resolução nº 23.755/2026)
>
> III - publicações que fomentem a subversão da ordem constitucional ou a ruptura da normalidade institucional democrática; (Incluído pela Resolução nº 23.755/2026)
>
> IV - violência política contra a mulher. (Incluído pela Resolução nº 23.755/2026)
>
> § 4º-B. Nas hipóteses previstas no § 4º-A, o provedor de aplicação de internet deve adotar as providências necessárias para tornar indisponível o conteúdo ilícito, independentemente de determinação judicial, garantindo, em qualquer caso, a comunicação ao usuário dos motivos que levaram à exclusão da publicação e a possibilidade de recorrer da moderação. (Incluído pela Resolução nº 23.755/2026)

Sem prejuízo do responsável pela publicação requerer judicialmente o restabelecimento da

publicação se provar sua licitude, o que requer a manutenção de um canal de moderação pelo provedor de aplicação, *in verbis*:

> § 4º-C. O responsável pela publicação do conteúdo removido pelo provedor de aplicações de internet também poderá requerer judicialmente o seu restabelecimento, mediante demonstração da ausência de ilicitude. (Incluído pela Resolução nº 23.755/2026)

VII) Uso de Inteligência Artificial na Propaganda eleitoral

A Inteligência Artifical (IA) é a área da tecnologia que cria sistemas e máquinas capazes de imitar habilidades humanas, como aprender com dados, reconhecer imagens e voz, entender linguagem e tomar decisões ou resolver problemas. Ao invés de apenas seguir ordens programadas, a IA utiliza dados e algoritmos para detectar padrões e evoluir. Ela automatiza tarefas complexas e gera conteúdos (texto, imagens), sendo comum em chatbots e análise de dados. Por exemplo: assistentes virtuais (como Siri, Alexa ou ChatGPT); recomendações da Netflix ou Spotify; carros que dirigem sozinhos; filtros de rosto em redes sociais etc (Adriana Schimaburkuro[16]).

O TSE, por meio da Resolução nº 23.732/2024, 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, identificado como "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 popularmente denominada *deepfake*[17]. Cabe transcrever os respectivos artigos que alteraram a 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 qual tecnologia foi utilizada. (Incluído pela Resolução nº 23.732/2024, com redação dada pela Resolução nº 23755/2026)

---

16 Definição da Coordenadora do Núcleo Técnico de Combate a Crimes Cibernéticos da PRSP.

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

> (...)
> § 3º O uso de chatbots, avatares e conteúdos sintéticos como artifício para intermediar a comunicação de campanha com pessoas naturais submete-se ao disposto no caput deste artigo, vedada qualquer simulação de interlocução com a pessoa candidata ou outra pessoa real. (Incluído pela Resolução nº 23.732/2024)
> (...)
> 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. (Incluído pela Resolução nº 23.732/2024)
> § 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. (Incluído pela Resolução nº 23.732/2024)

E a nova Resolução TSE nº 23.755/2026 alterou a Resolução TSE 23.610/2019, para incluir o art.9ª-I, que prevê a possibilidade de o juízo eleitoral inverter o ônus da prova nas representações cujo objeto seja propaganda eleitoral com uso de conteúdo sintético gerado por inteligência artificial ou tecnologia equivalente e o art. 9º-J, que permite aos Tribunais Eleitorais firmar acordos de cooperação com a academia e a sociedade civil para auxiliarem em processos relacionados à eleição. Mas a principal alteração consistiu na inclusão de vedações aos provedores de aplicação de internet que ofertem sistemas de IA ou tecnologia equivalente, de determinados tipos de "alimentação" dos programas de IA, no **artigo 28, § 1º-C**:

> § 1º-C. É vedado aos provedores de aplicação que ofertem sistemas de inteligência artificial ou por tecnologia equivalente, ainda que solicitado pela(o) usuária(o):
>
> I - ranquear, recomendar, sugerir ou priorizar candidatas(os), campanhas, partidos políticos, federações ou coligações;
> II - emitir opiniões, indicar preferência eleitoral, recomendar voto ou realizar qualquer forma de favorecimento ou desfavorecimento político-eleitoral, de maneira direta ou indireta, inclusive por meio de respostas automatizadas;
> III - criar ou promover alterações em fotografia, vídeo ou outro registro audiovisual que contenha cena de sexo, nudez ou pornografia envolvendo candidata ou candidato;
> IV - formular publicidade eleitoral que represente ato de violência política contra a mulher.

A Procuradoria Geral Eleitoral (PGE) junto com a 2ª Câmara de Coordenação Criminal (2ªCCR) da PGR criou o primeiro grupo bicameral, o denominado "Grupo de Trabalho sobre Desinformação na Internet, interferência cibernética na Democracia e influência nas Eleições" (GTDIE) [18], que incluiu em seu Plano de Trabalho, por meio do Termo de Mútua Cooperação firmado pela PGR com o Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS-Rio), desenvolver a atividade de monitoramento desses provedores de aplicação que oferecem serviços de

[18] Portaria PGE/2ª CCR nº 1, de 21/10/2025.

IA para analisar a partir de premissas padronizadas como a IA responderá ao eleitor que a consultar sobre candidatos e suas campanhas no pleito de 2026. Relatórios que serão produzidos mensalmente e enviados ao respectivo Grupo para análise e eventual atuação junto aos respectivos provedores.

A nova Resolução também introduziu mais três incisos (V, VI e VII)[19] no já citado art. 9º-E para prever a responsabilidade solidária dos provedores no uso de conteúdo sintético ou tecnologia equivalente, em desacordo com as regras previstas na Resolução 23610/2019 (inc. V); aquelas publicações que reproduzam outras já indisponibilizadas pela Justiça eleitoral (inc. VI), independente de nova ordem judicial e de publicação que envolva conteúdo de violência política de gênero (inc. VII), que é crime tipificado no artigo 326-B, do Código Eleitoral. Assim como incluiu dois parágrafos (1º e 2º) no referido artigo para possibilitar o Juízo eleitoral comunicar demais provedores sobre aquele conteúdo (inc. VI)[20] para que não haja sua disseminação assim como determina (§ 2º) que criem solução específica que permita aos autores eleitorais denunciar conteúdos ilícitos listados no art. 9-E.

VIII) 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-mail(s)* ou mensagem(s) recebida(s) e ou enviada (s); postagem(ns) em redes sociais; 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.

---

[19] Art. 9º-E. (...) V - de divulgação ou compartilhamento de conteúdo sintético gerado ou modificado por inteligência artificial ou por tecnologia equivalente, em desacordo com as regras de rotulagem ou incidente nas vedações previstas nesta Resolução; (Redação dada pela Resolução nº 23.755/2026); VI - de publicações que reproduzam, no todo ou em parte, conteúdo idêntico ou substancialmente equivalente àquele que já tenha sido objeto de ordem de indisponibilização pela Justiça Eleitoral, no exercício do poder de polícia ou no âmbito de ações eleitorais, quando os provedores de aplicação, cientes da decisão, deixarem de promover sua indisponibilização imediata, independentemente de nova ordem judicial específica. (Incluído pela Resolução nº 23.755/2026); VII - de violência política contra a mulher. (Incluído pela Resolução nº 23.755/2026)

[20] § 1º O Juízo competente poderá, de ofício ou a requerimento do autor da representação, determinar a cientificação dos demais provedores de aplicação para que atuem preventivamente contra a disseminação dos conteúdos referidos no inciso VI deste artigo. e § 2º Os provedores de aplicação devem implementar solução específica que permita às candidatas, aos candidatos, aos partidos políticos, às federações e às coligações denunciarem a infringência do disposto neste artigo. (Incluídos pela Resolução nº 23.755/2026)

VIII.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, e pode assim determinar seu grau de confiabilidade.

Como esclarecido em estudo específico sobre o assunto, 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.

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.*[21]

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 ga rantir 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.

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.

---

[21] 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.

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 eletrônicos (digitais). 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 vontadedo 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.*

Trata-se de uma visão moderna e evolutiva do tradicional conceito de documento – simples escrito em papel – tendo em vista o avanço da tecnologia[22].

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.

---

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

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

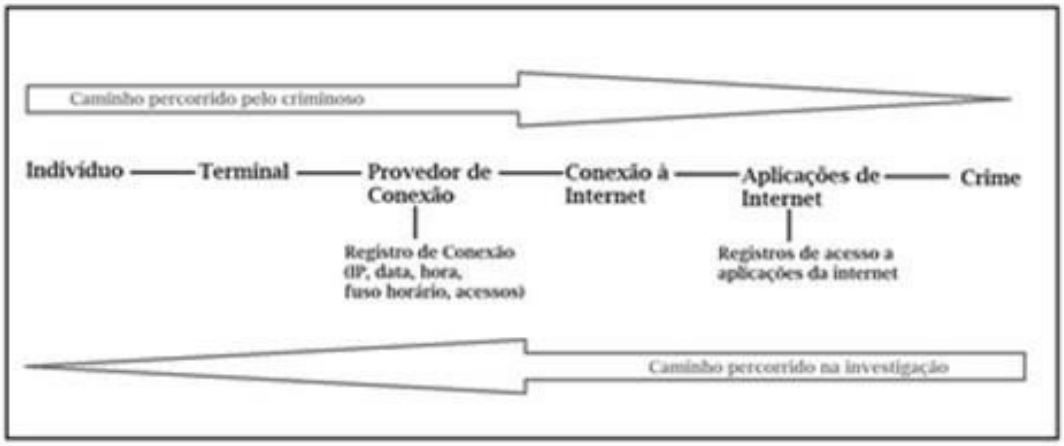
A manipulação da prova digital deve ser adequada também visando a obtenção de metadados, pois esses a permeiam, devem ser coletados na perícia e serem fornecidos também pelos provedores de aplicações de internet.

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.

IX) 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[23] [14]:

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



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. Essa 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

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[24]. 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, além do dado da porta de origem ou porta lógica.

Em uma breve síntese, recebida uma denúncia de publicação de desinformação eleitoral ou qualquer outro ilícito eleitoral, 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 dado(s) do(s) registro(s) de acesso e *log(s)* de *upload* (postagem) e de acesso do usuário junto ao respectivo provedor de aplicação identificado. Os grandes provedores costumam disponibilizar portais[25] para as autoridades

---

[24] 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, era preciso fazer um cruzamento de dados a partir de vários acessos com Ips diferentes para se identificar o usuário buscado, o que não será mais necessário com a recém alteração do Decreto que regulamentou o MCI e prevê a obrigatoriedade da guarda do dado da porta de origem ou lógica pelos provedores de conexão e de aplicação e seu fornecimento mediante ordem judicial.

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

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 no mesmo sítio do NIC.br[26] (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 dados cadastrais do cliente titular do serviço de conexão à internet. Essa informação, que independe de ordem judicial, 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.

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

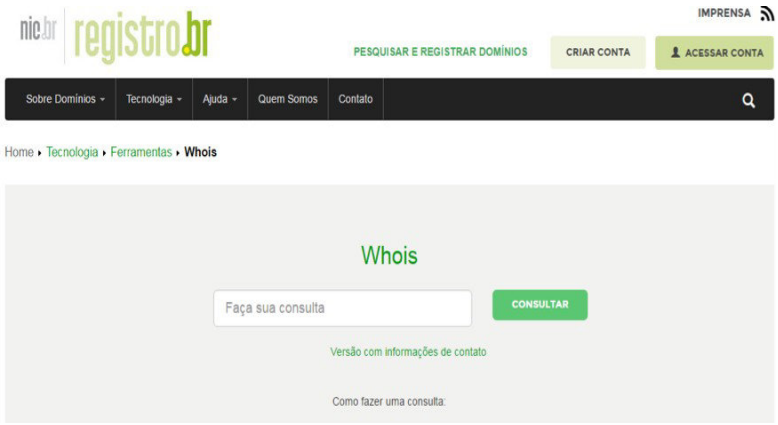
Ao se tentar identificar o autor de um ilícito na internet, o que pode ser requerido pela parte ao Juízo, em processo cível ou criminal, conforme prevê o art. 22 do MCI, reproduzido no art. 40 da Resolução TSE nº 23.610/2019, é busca conhecer a materialidade reportada, a localização geográfica do conteúdo hospedado e finalmente identificar o usuário 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 ilícitos criminais, 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, X, Tiktok etc); troca de mensagens instantâneas (WhatsApp, Telegram, Signal etc); email (@gmail, hotmail, terra etc); páginas na word wide

[26] http://registro.br (para endereços nacionais).

web - www (*sites*, *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* (Netflix, YouTube, Globoplay, Amazonetc) 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), esse último com muitas limitações em relação aos provedores europeus em razão da Lei de Proteção de dados europeia (GRPD).



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

A evidência digital é um registro informático no dispositivo que deve se tornar uma prova digital quando se pode atribuir a esse registro a uma pessoa. E essa evidência digital pode estar armazenada em um dispositivo de computador ou transmitido por uma rede de computadores. Ela é extremamente volátil, pois o usuário pode a excluir tão rápido quanto a publicou na internet. Ela deve ser obtida de acordo com a lei e por um processo que garanta a integridade e autenticidade. Devemos garantir assim a sua autenticidade, ou seja, de que a informação foi veiculada exatamente onde e forma que se está noticiando que ela foi e para assegurar sua integridade, que o manuseio dela não a alterará.

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 daquela evidência digital para que ela se converta em uma prova eletrônica; e b) a preservação dos dados (de acesso e conteúdo) referentes à prática de crime.

Assim que recebida a notícia da infração, é necessária a coleta da evidência eletrônica (por ex.: post em rede social, site, mensagem instantânea etc.), o procurador ou promotor deve encaminhar a notícia ao setor pericial do órgão do MP (no MPF, às ASSPAs locais ou gabinete eleitoral), e que dá apoio aos procuradores/promotores, em questões relacionadas às investigações na internet[27]. Ela deverá coletar adequadamente a evidência utilizando ferramentas forenses (ex. Verifact, nas PREs), que atestem que o material corresponde, exatamente, ao publicado, mediante a extração do código *hash*, iniciando-se, a partir daí, a observância da cadeia de custódia da prova eletrônica para se usada em um processo.

É necessário também se obter o mais rápido possível a preservação dos dados de identificação do usuário (IP, data e hora, porta de origem, da publicação) e do próprio conteúdo daquela evidência diretamente ao provedor de aplicações.

Assim, simutaneamente, 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 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 (art. 10, §1°, do MCI, e art. 39, da Res. TSE nº 23610/19).

Alguns provedores de aplicações mantêm canais específicos (portais na própria internet) para pedidos de preservação e para envio de ordens judiciais por meio de endereços de *e-mail* destinados às equipes organizadas 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.

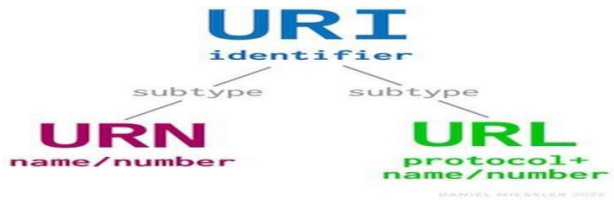
Para os provedores de aplicações, que prestam serviços no País e aqui mantêm escritório, mas que não possuem um canal específico para encaminhamento de pedidos e ordens de autoridades, basta enviar um ofício físico, no qual se requer a preservação da página ou do perfil investigado.

---

[27] Assessoria de Pesquisa e Análise (ASSPA) 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.

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 obrigatoriedade 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 (MLAT) 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[28].

É importante a correta identificação por meio do endereço na *web*, a **URL**[29] ou **URI**[30] ou **URN**[31] ou **ID**[32] do perfil, de um grupo; de um vídeo etc.[33], 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.



[28] Cenário que se pretende um dia alterar com a eventual ratificação pelo Brasil do 2º Protocolo sobre prova eletrônica à Convenção de Cibercrime (conhecida como Convenção de Budapeste), já ratificada pelo Brasil, em 2022.

[29] 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.

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

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

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

[33] 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

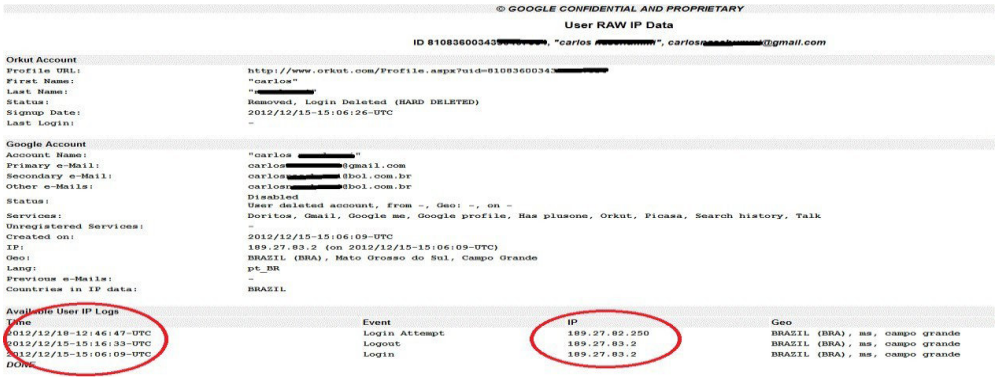
A URL (Uniforme Resource Locator, ou seja, Localizador Recursos Uniforme) é o padrão mais utilizado e citado como de uso preferencial no art. 38, § 4º , da Resolução TSE n º 23610/2019 (no caso de remoção de conteúdo esse deve ser identificado pela sua URL, se não for possível pela URI ou URN). É uma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

E os metadados são dados de registro de acesso à aplicação e são muito importantes para a investigação pois, se corretamente analisados e associados, podem trazer informações relevantes acerca da autoria de um ilícito. Eles não são criptografados em nenhuma aplicação (são dados). Exemplos:

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.



© GOOGLE CONFIDENTIAL AND PROPRIETARY

User RAW IP Data

ID 810836003431[redacted], "carlos [redacted]", carlos[redacted]@gmail.com

Orkut Account

Profile URL:	http://www.orkut.com/Profile.aspx?uid=810836003431[redacted]
First Name:	"carlos"
Last Name:	"[redacted]"
Status:	Removed, Login Deleted (HARD DELETED)
Signup Date:	2012/12/15-15:06:26-UTC
Last Login:	-

Google Account

Account Name:	"carlos [redacted]"
Primary e-Mail:	carlos[redacted]@gmail.com
Secondary e-Mail:	carlos[redacted]@bol.com.br
Other e-Mails:	carlos[redacted]@bol.com.br
Status:	Disabled User deleted account, from -, Geo: -, on -
Services:	Doritos, Gmail, Google me, Google profile, Has plusone, Orkut, Picasa, Search history, Talk
Unregistered Services:	-
Created on:	2012/12/15-15:06:09-UTC
IP:	189.27.83.2 (on 2012/12/15-15:06:09-UTC)
Geo:	BRAZIL (BRA), Mato Grosso do Sul, Campo Grande
Lang:	pt_BR
Previous e-Mails:	-
Countries in IP data:	BRAZIL

Available User IP Logs

Time	Event	IP	Geo
2012/12/10-12:46:47-UTC	Login Attempt	189.27.82.250	BRAZIL (BRA), ms, campo grande
2012/12/15-15:16:33-UTC	Logout	189.27.83.2	BRAZIL (BRA), ms, campo grande
2012/12/15-15:06:09-UTC	Login	189.27.83.2	BRAZIL (BRA), ms, campo grande

DONE

Muitas vezes, o conteúdo investigado ainda está disponível na *web,* podendo ser coletado por um perito ou técnico em informática ou agente treinado para tal, que pode certificar a coleta da prova por meio da geração do código *hash*[34], 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.

IX.3) Passos da investigação: pedido de remoção de conteúdo

Como regra geral, o MCI apenas permite a remoção de conteúdo mediante ordem judicial, cujo juiz 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

[34] "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.

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.

No entanto, recentes alterações legislativas como o ECA digital e a própria nova Res. do TSE nº 23755/2026 prevê para o juízo eleitoral (art.38-A da Res. TSE 23610/2019) à remoção de perfil falso, apócrifo, ou que não exista no munod real (automatizado uo robo), cujo conteúdo, após publicações reiteradas, seja relacionado a crime eleitoral e à desinformação sobre a integridade do processo eleitoral, nos termos do art. 38-A, § 1º; e prevê a mesma remoção pelo próprio provedor de aplicação à internet, independentemente de ordem judicial, desde que o perfil seja falso ou automatizado ou robo, conforme o art. 38ª-A, § 2º, da Res. TSE 23.610/2019[35] (exclui apenas o apócrifo).

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, existem 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 Meta (Facebook, Instagram, WhatsApp e Messenger), Google, TikTok, X, 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 na plataforma o serviço disponibilizado é utilizado para a prática de crime, é possível pedir diretamente ao provedor responsável a remoção de 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.

---

[35] Art. 38-A. A remoção de perfil será feita quando se tratar de usuário comprovadamente falso, apócrifo ou vinculado a pessoa que sequer exista fora do universo digital (perfil automatizado ou robô), cujas publicações configurem a reiterada prática: (Incluído pela Resolução nº 23.755/2026) I - de crime eleitoral; (Incluído pela Resolução nº 23.755/2026) II - de publicação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam atingir a integridade do processo eleitoral, que tenham sido assim reconhecidos pela Justiça Eleitoral. (Incluído pela Resolução nº 23.755/2026) § 1º As determinações de remoção de perfil serão aplicadas em processo judicial em que seja assegurada a ampla defesa e o contraditório. (Incluído pela Resolução nº 23.755/2026) § 2º É permitida a exclusão pelos provedores de aplicação apenas nas hipóteses de perfis falsos, automatizados ou robô. (Incluído pela Resolução nº 23.755/2026)

Agora, a partir da Res. TSE nº 23755/2026, art. 38, os provedores de aplicação têm a obrigação de excluir os conteúdos ali delimitados sempre que identificá-los em seus serviços, após reiteradas decisões da Justiça eleitoral, conforme explicado no item acima referente a "Desinformação eleitoral na internet".

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.

IX.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/perfil 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, assim como a porta de origem ou porta lógica. 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 afastamento de sigilo telemáticos, bem como os endereços dos principais provedores[36].

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

[36] Todas as informações aqui indicadas constam disponibilizadas pelos membros do Ministério Público Federal no portal e-evidence (ao lado do ícone do Único na página do MPF), que é organizado e alimentado pelos membros que integram o GACCTI da 2ª CCR.

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

será possível identificar o provedor de conexão à internet, que alocou aquele IP, e requisitar a ele as informações referentes aos dados cadastrais do usuário[37]que se conectou na internet por meio 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 .

A requisição, por se tratar de meros dados cadastrais (nome e endereço), pode ser feita diretamente ao provedor de conexão identificado, de acordo com o art. 10, § 3º, do MCI, sem necessidade de ordem judicial. Em tópicos próprios, constam modelos de ofício com a requisição de dados cadastrais aos provedores de conexão, bem como os endereços dos principais provedores[38].

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.

IX.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

37 Também denominados dados de assinante ou de subscritor.

38 Esses endereços não se aplicam ao período eleitoral quando os principais provedores utilizados no País indicam endereços próprios para respostas ao TSE com escritórios para responderem de forma mais ágil no período eleitoral.

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 apare lho celular apreendido, para conhecimento do registro das chamadas e da agenda de telefo nes, bem como das demais informações, é necessária prévia autorização judicial. Nesse qua dro, 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 cola boração 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, desde 2022, que prestam serviços no País, como o grupo Meta (Facebook, Instagram, WhatsApp e Messenger) Memorandos de Ajustamento[39] com os provedores Google; X (ex-Twitter); TikTok, Kwai e Telegram, 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.

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.

IX.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.

---

[39] 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.

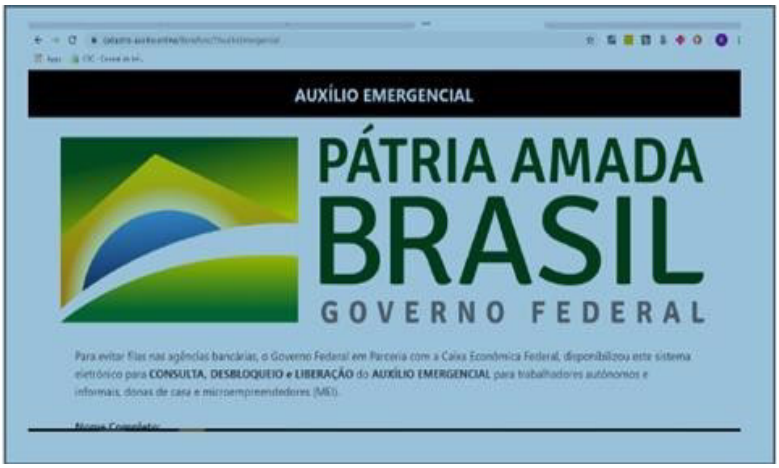
Assim que recebida a notícia da infração, sendo necessária a coleta da prova eletrônica, isto é, a prova da existência da página, o PRE ou promotor deve encaminhar a notícia à ASSPA ou setor pericial do MP, que deverá coletar adequadamente a prova utilizan do ferramentas forenses que atestem que o material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

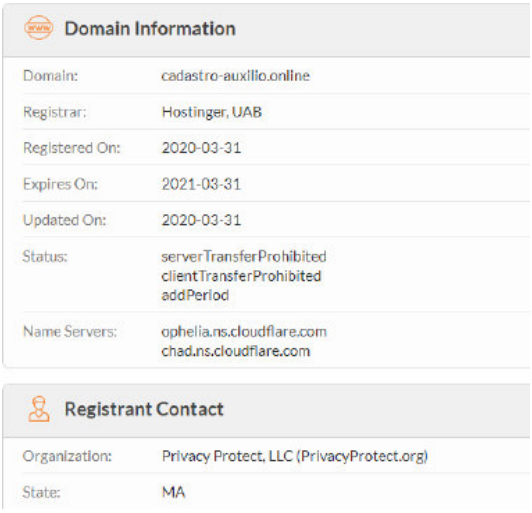
Para identificar o provedor de hospedagem e eventual provedor de anonimização, devem ser consultados os serviços https://www.registro.br/ (para endereços nacionais) ou no http://whois.icann.org (para endereços no exterior), nos termos do item VII.2 acima.

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 medida cautelar judicial de quebra de sigilo telemático do *site* a fim de instruir o pedido de cooperação jurídica 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.

IX.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.

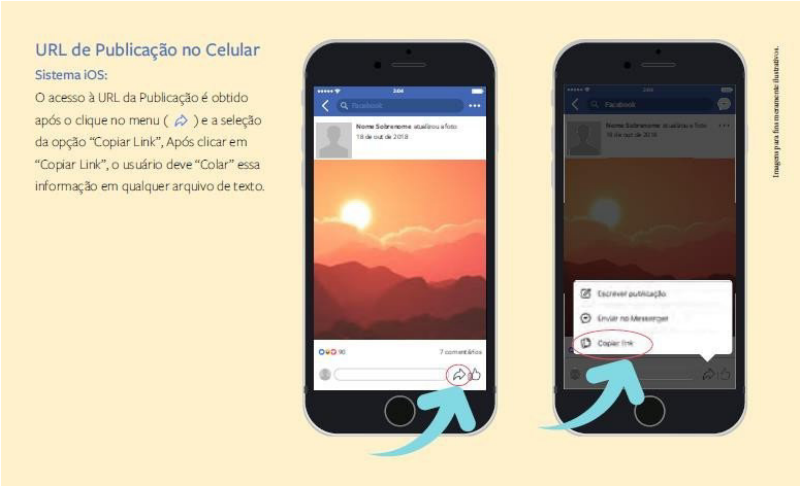
Ao mesmo tempo em que se busca a preservação dos dados junto ao Facebook, é necessária a coleta adequadada prova, com todos os cuidadosforenses para queseja mantida íntegra e preservada, dando-se início à cadeia de custódia. Para tanto, as informações necessárias para acesso à publicação devem ser encaminhadas 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 podeser 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.

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

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/Whats App/Messenger):

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

IX.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 VIII.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 VIII.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 VIII.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:

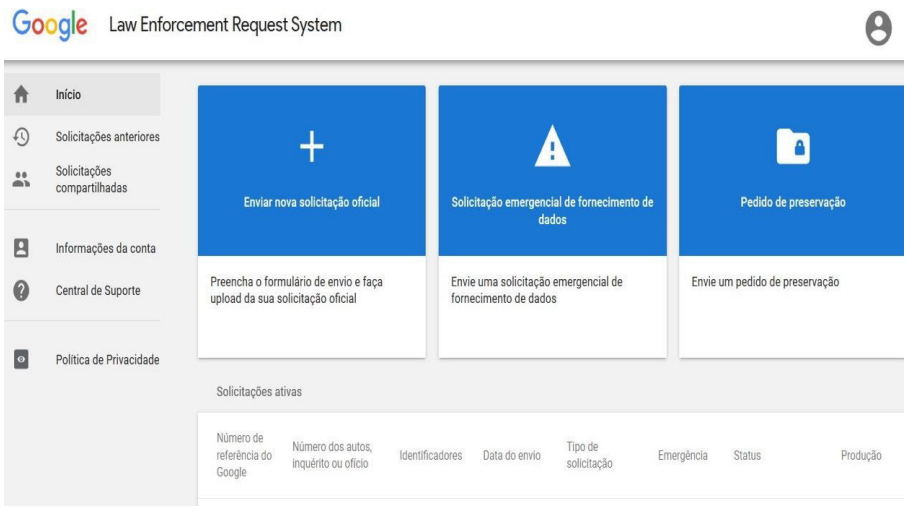
Por fim, nos ofícios, deve constar o endereço do WhatsApp LLC, como segue:

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

IX.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

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

Na hipótese de veiculação de conteúdo ilícito pelo X, o pedido de preservação de dados que até o início de 2022 era realizado pelo sistema on line https://legalrequests.twitter.com foi descontinuado e, atualmente, o pedido de preservação e os demais devem ser enviados por meio do e-mail **br_legalrequests@x.com**

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://x.com/xsafety (@xsafety); e/ou o número de identificação do usuário ou UID exclusivo e público da conta no X ou um nome de usuário e URL do Periscope (por exemplo, @xsafety e https://periscope.tv/xsafety). Para localizar um UID do X ou o nome de usuário do Periscope, consulte https://help.x.com/pt/rules-and-policie/x- law-enforcementsupport#

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 VIII.2.

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

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 VIII.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. Imperatriz Leopoldina, 1248, sala 203, BA088, Vila Leopoldina, São Paulo/SP
CEP 05305-002

Importante: o X 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, as operadoras do X atribuíam o "selo azul de verificação" às contas de interesse público, ou seja, analisavam os dados fornecidos pelos titulares e confirmavam que eram autênticos e que efetivamente pertenciam à pessoa ou à marca que representam (v. https://help.x.com/pt/managing your-account/x-verified-accounts). Hoje, esse serviço só é pago, 3 chama-se X-PREMIUM, e não é mais oferecido por notoriedade ou para pessoas famosas. Atualmente, por serem vendidas, a confiabilidade sobre essa verificação é relativa, mas ajuda identificar o usuário da conta.

X.1) 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-seimperiosa, 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 preenchidosos 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.2) Modelo de peça de medida cautelar de quebra de sigilo telemático ao Facebook

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 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-seimperiosa, 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 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.

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)]; inclusivenome 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

X.3) Modelo de ofício para preservação de registros e remoção de site ilícito para serviço de hospedagem

OFÍCIO nº Localidade, data de 2026.

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.

X.4) Modelo de ofício para preservação de registros e remoção de site ilícito para serviço de privacidade

OFÍCIO nº Localidade, data de 2026.

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, o MPE vem 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, 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 (inclusive financeiro), 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,

X.5) Modelo de ofício de requisição de dados cadastrais e de preservação para provedor de conexão (Claro S/A)

OFÍCIO nº Localidade, data de 2026.

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(ua) Procurador(a) Regional Eleitoral ou 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, solicita 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 institucional XX.

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

Atenciosamente,

X.6) Ofício de solicitação de remoção de conteúdo a provedor de aplicação (Facebook)

OFÍCIO n° Localidade, data de 2026.
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 meio do(a) Procurador(a) Regional Eleitoral ou 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 a conduta XX e, portanto, possivelmente violou normas contidas nos termos de uso desse provedor de aplicação.

Assim sendo, solicita 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, solicita que o presente pedido não seja informado ao usuário, posto que o sigilo é necessário ao bom êxito das investigações.

Atenciosamente,

X.7) Ofício de solicitação de preservação de dados a provedor de aplicação/conexão

OFÍCIO nº Localidade, data de 2026.

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(ua) Procurador(a) Regional Eleitoral ou 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,

X.8) *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

Solicita 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 p rovedora de hospedagem de sites) no país (indicar o país).

Ressalta 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.

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

Atenciosamente,

XI) Fontes

GONÇALVES, Luiz Carlos dos Santos. Investigação e processo dos crimes eleitorais e conexos. São Paulo: SaraivJur, 2022. p. 108.

CINTRA, Antônio Carlos de Araújo, GRINOVER. DINAMARCO, Ada Pellegrini, Cândido R. *Teoria Geral do Processo*. São Paulo: Revista dos Tribunais. 8ªedição, revista e ampliada. 1991.

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 e Covid 19, do GACC (Grupo de Apoio sobre Criminalidade Cibernética). Brasília; 2ª CCR/PGR, 2021.

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.voitto.com.br/blog/artigo/o-que-e-hash-e-como-funciona/amp.

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

XII) Endereços de contato dos provedores

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

Ministério Público *nas* ELEIÇÕES 2026

Ministério Público *nas*
ELEIÇÕES 2026

ILÍCITOS ELEITORAIS NA INTERNET: COMO INVESTIGAR?

Ministério Público Eleitoral

Ministério Público *nas*
ELEIÇÕES 2026

1.Acesso à internet (provs. conexão e aplicação)

2. Marco Civil da Internet e Res.TSE 23610/2019

3. Remoção de Conteúdo

4. Investigação para identificar o usuário

4.1 Desinformação/Investigação em site

4.2 Desinformação/Investigação no Face/Insta

4.3 Desinformação/Investigação no WhatsApp

4.4 Desinformação/Investigação no Youtube

4.5 Desinformação/Investigação no X

5. Estratégia contra Desinformação - PGE

Ministério Público nas ELEIÇÕES 2026

1. Acesso à internet

Toda conexão à rede é feita por meio de um modem, ligado a um **provedor de conexão à internet** (CLARO/NET, Oi TELEMAR, TIM, VIVO, etc).

Para que o usuário possa ser “encontrado”, o provedor lhe atribui um **número de protocolo exclusivo**, pelo período de conexão.

IP = número do protocolo

Ministério Público nas ELEIÇÕES 2026

1.1 Provedores de conexão à internet

Transição do IPv4 para

- endereços IPv4 – esgotamento em 12/2014, sem a implementação total do IPv6;
- situações ocorrem em que há a alocação de um endereço de IP para mais de um usuário durante a transição do IPv4 para o IPv6 (uso da técnica CG-NAT44 = IP nateado);
- grande dificuldade na identificação de usuários infratores;
  - **necessidade do pedido da porta lógica (ou de origem) de acesso aos provedores de conexão e aos de aplicação de internet (art. 9º-G, §2º, III, Res. TSE nº 23.610/19 incluído pela Res 23732/24)**
- recém aprovado o Decreto nº 12975, de 20/5/26, que obriga a guarda da porta lógica (ou de origem) para os provedores de conexão e de aplicação à internet (art.15-A, §§ 1º e 2º,MCI)

1.2 Provedores de aplicação de internet

SERVIÇOS MAIS COMUNS PRESTADOS NA INTERNET
permitem a inserção de postagens na internet

- **world wide web** – www (site, blog, fotoblog)
- **e-mail (@**gmail, hotmail, terra)
- **formação de redes e comunidades virtuais** (Facebook, Instagram, X – ex-Twitter, TikTok)
- **troca instantânea de mensagens** (Whatsapp,Telegram)
- **hospedagem e compartilhamento de arquivos** (redes P2P: eMule, Aresgalaxy, Gnutella, Gigatribe)
- **voip** (voz sobre IP)
- **chat** (salas de bate-papo)
- **fóruns de discussão** (Yahoo groups)
- **serviços de streaming** (YouTube, Globoplay)
- **e-commerce** (Mercado Livre, Amazon)

Ministério Público nas ELEIÇÕES 2026

2. Marco Civil da Internet e Res. TSE 23610/19

Define termos técnicos, direitos e garantias dos usuários, e diretrizes do Poder Público.

art. 5º – Conceitos básicos:

- **endereço de protocolo de internet (endereço IP):** o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais (inc.III); (art.37, VI, Res. TSE 23610/19)
- **registro de conexão:** o 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 (inc. VI, MCI e art.37, inc. VII, Res. TSE 23610/19).

-**registro de acesso a aplicações de internet:** o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP (inc. VIII, MCI, e art.37, VIII, Res. TSE 23610/19).

2. Marco Civil da Internet e Res. TSE 23610/19

- estabelece que as informações dos provedores de conexão e de aplicação à internet somente poderão ser obtidas por ordem judicial (art. 10, § 1º, MCI, e art. 39, da Res. TSE 23610/2019);

- provedores com representação no Brasil ou prestando serviços no País devem cumprir a legislação nacional (art.11, § 2º, MCI e art.40, § 2ª, da Res.TSE 23610/2019).

2. Marco Civil da Internet – Lei nº 12.965/14

art. 11º – estabelece aplicação da legislação brasileira para as operações de coleta, armazenamento, guarda e tratamento de registros realizados em território nacional, sendo obrigatoriamente respeitados os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º - pelo menos um dos terminais localizados no Brasil,

§ 2º - mesmo a 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.

2. Marco Civil da Internet – Lei nº 12.965/14

PROVEDORES SEM REPRESENTAÇÃO NO BRASIL

1.Provedores **sem representação** no Brasil, mas que oferecem seus serviços ao público em território nacional, devem cumprir a legislação brasileira:

- ***Targeting Test:***
  - serviço oferecido em português;
  - publicidade voltada para o público em território nacional;
  - vendas na moeda nacional.

2. **Provedores que NÃO oferecem seus serviços ao público no Brasil**, mas que são utilizados a partir do território nacional: para obtenção dos dados, a menos que eles estejam acessíveis às autoridades nacionais (art. 240 CPP e arts. 842 e ss do CPC), necessário o pedido de cooperação internacional (MLAT). **Res. TSE 23610/19, art. 28.**

2. Marco Civil da Internet – Lei nº 12.965/14

PRAZOS DE RETENÇÃO:

- **registros de acesso às aplicações de internet**: 6 meses (arts.15 e 15-A);
- **registros de conexão**: 1 ano (arts. 13 e 15-A).

PEDIDO DE PRESERVAÇÃO por PRAZO SUPERIOR: pode ser feito pelo MP, polícia ou autoridade administrativa.

Registros armazenados são apenas de metadados:
IP, porta, data e hora GMT (não são criptografados)

2. Marco Civil da Internet – Lei nº 12.965/14

CONTEÚDO: não há obrigação de guarda, mas fornecimento somente por ordem judicial. Pode ser feito pedido de preservação também.

Conteúdo armazenado – art. 7, inc. III, do MCI (CPP, art. 240, alíneas *f* e *h* e CPC, arts. 842 e 843).

Conteúdo *online* - fluxo (tempo real) – art. 7, inc. II, do MCI (na forma da Lei nº 9296/96).

2. Marco Civil da Internet – Lei nº 12.965/14

SANÇÕES do ART. 12: descumprimento (arts. 10 e 11, MCI)

I - ADVERTÊNCIA COM INDICAÇÃO DE PRAZO PARA ADOÇÃO DE MEDIDAS CORRETIVAS;

II - MULTA ATÉ 10% DO FATURAMENTO DO GRUPO ECONÔMICO NO BRASIL - condição econômica do infrator + princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção; (Res. TSE nº 23610/19, art. 27-A, § 8º)

III - SUSPENSÃO TEMPORÁRIA DAS ATIVIDADES – que envolvam os atos previstos no art. 11;

IV - PROIBIÇÃO DE EXERCÍCIO DAS ATIVIDADES - que envolvam os atos previstos no art. 11

APLICAÇÃO SEM PREJUÍZO DAS DEMAIS SANÇÕES CÍVEIS, CRIMINAIS OU ADMINISTRATIVAS CABÍVEIS.

3. Remoção de Conteúdo

REMOÇÃO DE CONTEÚDO DA INTERNET
PODER DE POLÍCIA

Res. 23.610/2019, art. 7º. O juízo eleitoral com atribuições fixadas na forma do art. 8º desta Resolução somente poderá determinar a imediata retirada de conteúdo na internet que, em sua forma ou meio de veiculação, esteja em desacordo com o disposto nesta Resolução.

§ 1º Caso a irregularidade constatada na internet se refira ao teor da propaganda, não será admitido o exercício do poder de polícia, nos termos do art. 19 da Lei nº 12.965/2014 (que prever que o provedor deve ser intimado por ordem judicial).

Ex.: disparo em massa no WhatsApp – meio ilegal de veiculação; impulsionamento de propaganda eleitoral negativa de adversário – forma ilegal de veiculação.

Ministério Público nas ELEIÇÕES 2026

3. Remoção de Conteúdo

Uma das novidades da nova Resolução TSE nº 23.755/2026 foi a alteração da responsabilidade civil dos provedores de aplicação à internet sobre o conteúdo de informações falsas ou sem comprovação técnica que descredibilizem a integridade do sistema eletrônico de votação; que incite crime contra o Estado Democrático de Direito; que fomente a subversão da ordem constitucional ou ruptura da normalidade institucional democrática; ou configure violência política contra a mulher (art. 326-B, CE), tornando-os responsáveis pela remoção desse tipo de conteúdo, independente de ordem judicial, ao incluir o § 4º-A, 4º-B e 4º- C, no art. 28, da Res. TSE nº 23.610/2019.

O usuário responsável pela publicação deve ser comunicado pelo provedor dos motivos e pode requerer judicialmente o restabelecimento da publicação (§4º- C, art. 28).

Ministério Público nas ELEIÇÕES 2026

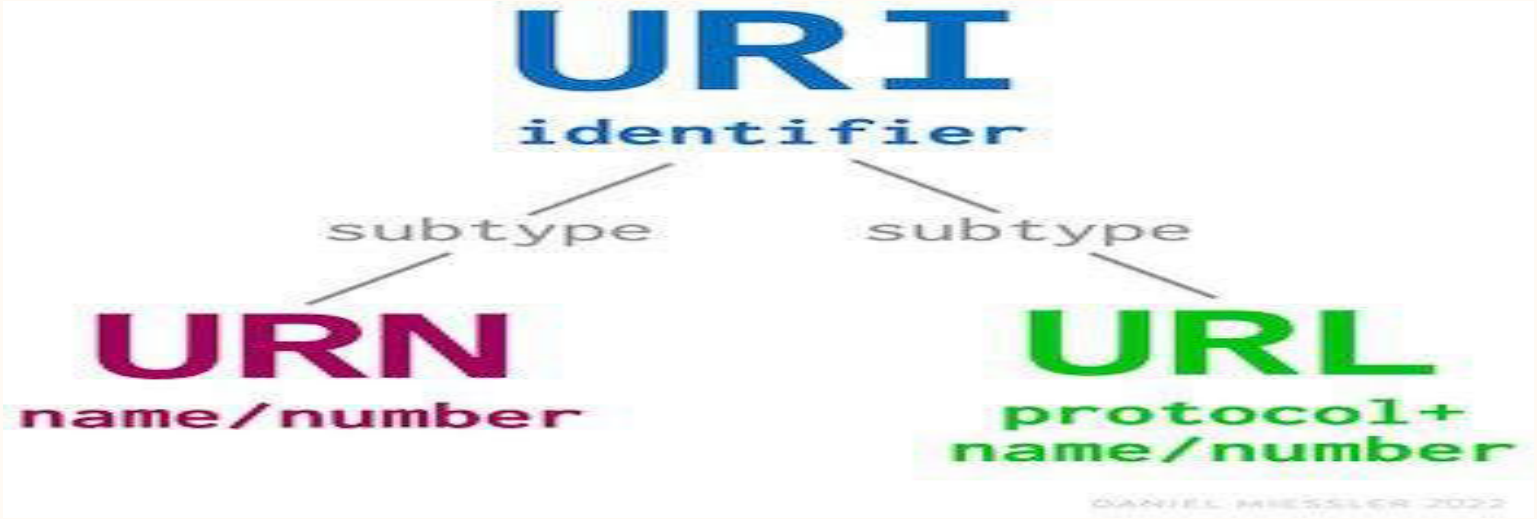
3. Remoção de Conteúdo

A nova Res. do TSE nº 23755/2026 incluiu o **art. 38-A, na Res. TSE 23.610/2019** ao prever que o juízo eleitoral, em processo com ampla defesa e contraditório (§ 1º), remova perfil com usuário falso, apócrifo ou que não exista no mundo real (automatizado ou robo), cuja publicação seja crime eleitoral ou desinformação sobre a integridadede do processo eleitoral, cujas publicações configurem reiterada prática assim reconhecida pela Justiça Eleitoral.

E permitiu ao provedor de aplicação à internet a remoção desse mesmo conteúdo, independente de ordem judicial, desde que o perfil seja falso, automatizado ou robo no **§ 2º, do Art. 38-A, da Res. TSE 23.610/2019**. Exclui a hipótese de perfil aprócrifo (anônimo).

3. Remoção de Conteúdo

Res. TSE 23.610/2019, art. 38, § 4º. A ordem judicial que determinar a remoção de conteúdo divulgado na internet fixará prazo razoável para o cumprimento, não inferior a 24 h, e deverá conter, sob pena de nulidade, a URL e, caso inexistente esta, a URI ou a URN do conteúdo específico, 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.



Ministério Público nas ELEIÇÕES 2026

3. Remoção de Conteúdo

URI - Uniforme Resource Identifier (Identificador de Recurso Uniforme), combinação única de letras, números e/ou caracteres, que identifica certo conteúdo na internet, por meio da página. A URL e URN são subconjuntos do conjunto de URIs.
Ex: **www.prerj.mpf.mp.br (identifica a página, mas sem o meio em que ele se localiza, que é o protocolo – https://)**

URL - Uniforme Resource Locator (Localizador de Recurso Uniforme), que localiza certo conteúdo na internet de forma precisa,padrão). Ex: **https://www.prerj.mpf.mp.br/denuncia-de-ilícitos-na-internet (endereço mais completo)**

URN – Uniforme Resource Name (Nome de Recurso Uniforme), identifica um nome estático. Ex: **prerj.mpf.mp.br**

4. Identificação do usuário

IDENTIFICAÇÃO DO USUÁRIO

Res. TSE nº 23.610/2019, art. 39. O provedor responsável pela guarda somente será obrigado a disponibilizar os registros de conexão e de acesso a aplicações de internet, de forma autônoma ou associados a dados cadastrais, a dados pessoais ou a outras informações disponíveis que possam contribuir para a identificação do usuário, mediante ordem judicial, na forma prevista nesta Seção (**MCI, art.10, caput e § 1º**).

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 (**MCI, art. 22**).

4. Identificação do usuário

IDENTIFICAÇÃO DO USUÁRIO

Res. TSE nº 23610/2019, art. 40.

§ 2º A ausência de identificação imediata do usuário responsável pela divulgação do conteúdo não constitui circunstância suficiente para o deferimento liminar do pedido de quebra de sigilo de dados.

§ 4º Nos casos previstos no caput deste artigo, os provedores indicados no art. 39 desta Resolução podem ser oficiados para cumprir determinações judiciais, sem que sejam incluídos no polo passivo das demandas, nos termos do § 1º-B do art. 17 da resolução deste Tribunal que regula representações, reclamações e direito de resposta.

Ministério Público nas ELEIÇÕES 2026

4.1Investigação para identificar o usuário

VISÃO GERAL DO PROCEDIMENTO

identificação do meio empregado

identificação dos responsáveis pelo serviço
preservação de dados

quebra de sigilo de dados telemáticos: IP

quebra de sigilo de dados telemáticos: conexão

comprovação da autoria e da materialidade

Ministério Público nas ELEIÇÕES 2026

4.1 Investigação para identificar o usuário

USUÁRIO → INTERNET → APLICAÇÕES DA INTERNET

PROVEDOR DE CONEXÃO:

TIM · vivo · Claro-Brasil (NET, Claro, Embratel)

PROVEDOR DE APLICAÇÃO
ou
PROVEDOR DE CONTEÚDO

Google · Facebook · Instagram · Tweet · WhatsApp · mercado livre

Ministério Público nas ELEIÇÕES 2026

4.1 Investigação para identificar o usuário

- ✓**comunicação instantânea** (Whatsapp,Telegram…)?
- ✓**redes de relacionamentos** (Facebook, Instagram, X, TikTok)?
- ✓**página da web** (blogs, fotologs, sites)?
- ✓**e-mail** (@ gmail, hotmail, globo, terra...)?
- ✓**fóruns de discussão** (yahoo groups...)?
- ✓**sala de bate-papo** (chats)?

4.1 Investigação para identificar o usuário

1. IDENTIFICAÇÃO DOS RESPONSÁVEIS PELO SERVIÇO

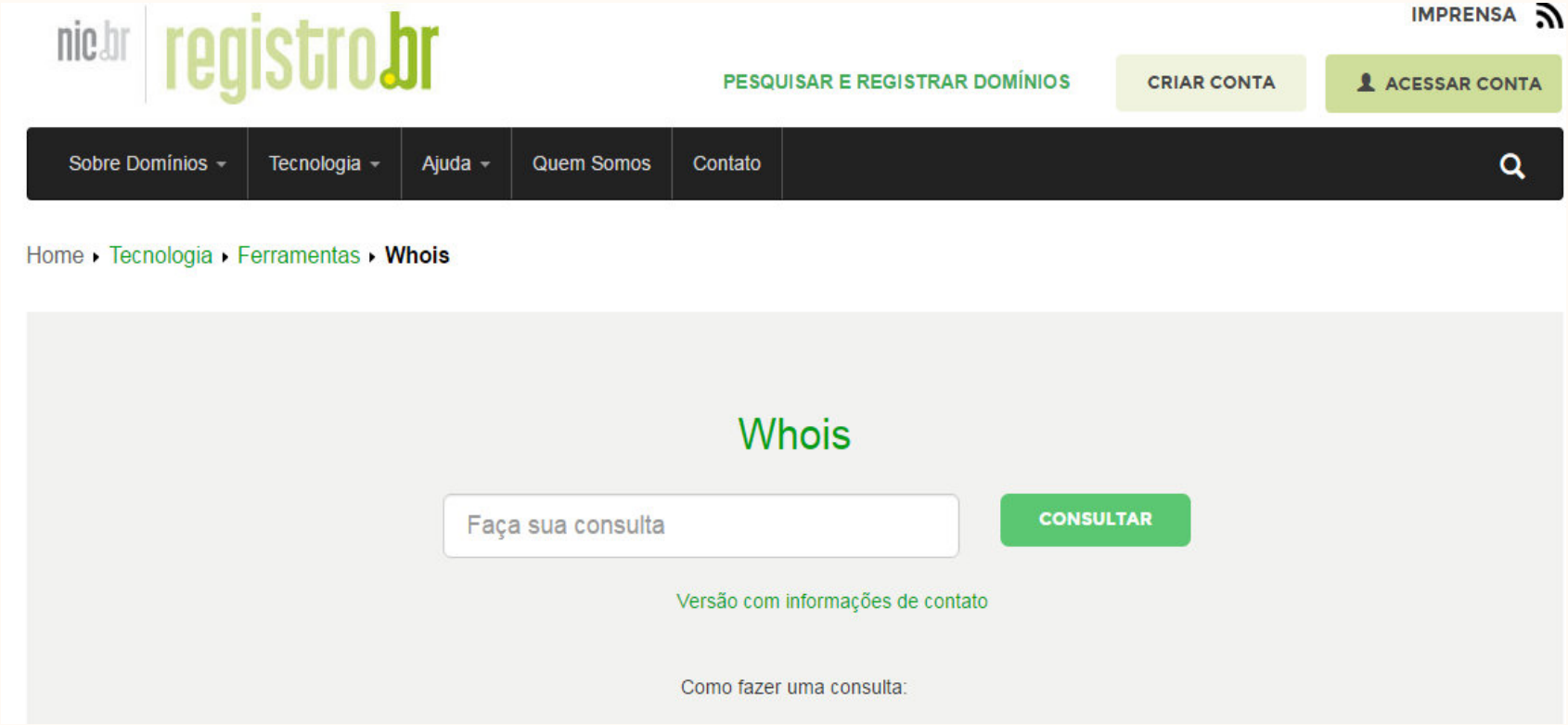
- Endereços nacionais (.br) → https://registro.br

- Endereços estrangeiros→ http://whois.icann.org

Ministério Público nas ELEIÇÕES 2026

4.1 Investigação para identificar o usuário

1. IDENTIFICAÇÃO DOS RESPONSÁVEIS PELO SERVIÇO



4.1 Investigação para identificar o usuário

2. PRESERVAÇÃO DAS PROVAS (cadeia de custódia)

Salvar e garantir integridade dos dados:

- Evidência/Prova Digital: volátil
- Autenticidade: **garantir que a evidência digital veio mesmo de onde se alega (certificar gerando um código *hash*, código aritmético que confere uma impressão digital única do arquivo)**
- Integridade: **garantir que o manuseio da prova não a altera**

4.1 Investigação para identificar o usuário

2. PRESERVAÇÃO DAS PROVAS (cadeia de custódia)

✓notificar provedor para preservar registros de acesso à aplicação de internet e *logs* de postagens (*uploads*) e acessos (sempre avisar que **não notifique** o usuário dos dados);

✓obrigação dos provedores de retenção (salvo conteúdo) e preservação por período superior;

✓ os principais provedores de aplicações de internet disponibilizam portais para realização desse pedido de preservação.

4.1 Investigação para identificar o usuário

3. QUEBRA DE SIGILO DE DADOS TELEMÁTICOS (IP)

•**pedido judicial** para obtenção dos registros de acesso à aplicação de internet e *logs* de postagens (*uploads*) e acessos (Art. 15, MCI), indagando:

•endereço IP;
•data, horário e referência GMT da conexão;
•porta lógica;
•dados como *email*, nome cadastrado, *nickname* (pode ser usado em outros aplicativos).

✓se não houver vínculo do provedor com o Brasil, necessário recorrer à cooperação jurídica internacional.

4.1 Investigação para identificar o usuário

3. QUEBRA DE SIGILO DE DADOS TELEMÁTICOS (IP)

User RAW IP Data

ID 810836003439[redacted], "carlos [redacted]", carlos[redacted]@gmail.com

Orkut Account

Profile URL:	http://www.orkut.com/Profile.aspx?uid=81083600343[redacted]
First Name:	"carlos"
Last Name:	"[redacted]"
Status:	Removed, Login Deleted (HARD DELETED)
Signup Date:	2012/12/15-15:06:26-UTC
Last Login:	-

Google Account

Account Name:	"carlos [redacted]"
Primary e-Mail:	carlos[redacted]@gmail.com
Secondary e-Mail:	carlos[redacted]@bol.com.br
Other e-Mails:	carlosn[redacted]@bol.com.br
Status:	Disabled User deleted account, from -, Geo: -, on -
Services:	Doritos, Gmail, Google me, Google profile, Has plusone, Orkut, Picasa, Search history, Talk
Unregistered Services:	-
Created on:	2012/12/15-15:06:09-UTC
IP:	189.27.83.2 (on 2012/12/15-15:06:09-UTC)
Geo:	BRAZIL (BRA), Mato Grosso do Sul, Campo Grande
Lang:	pt_BR
Previous e-Mails:	-
Countries in IP data:	BRAZIL

Available User IP Logs

Time	Event	IP	Geo
2012/12/18-12:46:47-UTC	Login Attempt	189.27.82.250	BRAZIL (BRA), ms, campo grande
2012/12/15-15:16:33-UTC	Logout	189.27.83.2	BRAZIL (BRA), ms, campo grande
2012/12/15-15:06:09-UTC	Login	189.27.83.2	BRAZIL (BRA), ms, campo grande

DONE

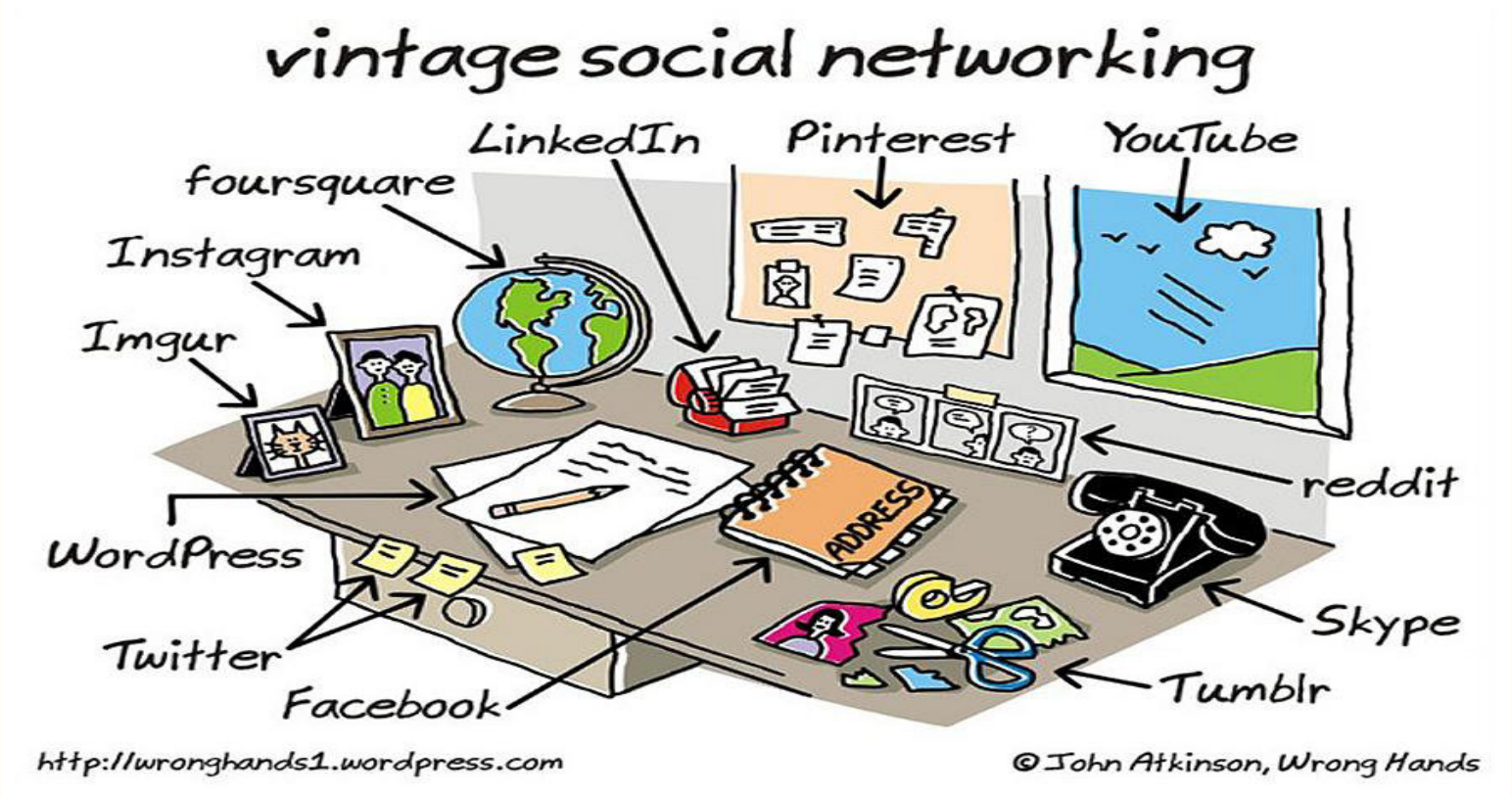
4. QUEBRA DE SIGILO DE DADOS TELEMÁTICOS (DADOS CADASTRAIS DO USUÁRIO)

Visa identificar a máquina de onde o fato foi praticado, a partir do IP fornecido (Art. 13, MCI)

- ✓em geral, a expedição de ofício é para concessionária de telefonia ou portal (PORTALJUD-Telefônica, Vivo).
- ✓pedido e ofício devem fazer referência obrigatória a:
  - endereço IP (indicado pelo prov. de aplicação);
  - data, horário e referência GMT da conexão;
  - porta lógica (Art. 9º-G, §2º, III, Res. TSE nº 23.610/19 incluído Res 23732/24)
- ✓endereços: www.registro.br

5. COMPROVAÇÃO DA MATERIALIDADE E DA AUTORIA – BUSCA E APREENSÃO

Especificidades na Obtenção de Provas Digitais – cuidados na coleta e preservação

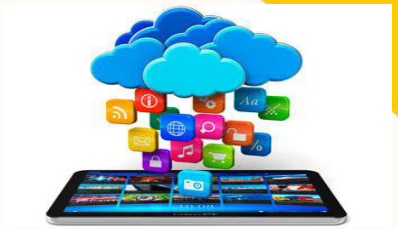


5. COMPROVAÇÃO DA MATERIALIDADE E DA AUTORIA – BUSCA E APREENSÃO

- ✓ Precedida de ordem de missão policial.
- ✓ Busca e apreensão do terminal (autorização para acesso aos dados e arquivos), pen drives, HD externo.
- ✓ oitiva do assinante da conexão - no local (STF - RECLAMAÇÃO 33.711:ouvir sem advertir sobre o direito ao silêncio).
- ✓ **Celulares:** STF **2007**, bastava mandado genérico. STJ **2016** HC 51.531/ REsp 1.727.266/SC, j.05/06/2018 - autorização específica para conteúdo do celular no flagrante (dados e conversas). **STF Repercussão Geral ARE1.042.075/24.11.17, Rel. Min. Dias Toffolli -** acesso a agenda e a histórico de ligações deve ter prévia ordem judicial - tema de repercussão geral (mérito pendente).

4.1 Investigação para identificar o usuário

Armazenamento na Nuvem



a) sincronização com a nuvem – busca e apreensão a partir do local do terminal (senha);

b) pedido de apreensão virtual para a empresa que presta o serviço de *cloud computing.* O conteúdo armazenado na nuvem nem sempre é criptografado (*backup* nos serviços do Google Drive, iCloud etc).

Garantir a cadeia de custódia:

laudo pericial no computador e demais materiais apreendidos/ no local, agente técnico especializado/*software,* que verifica *hashes.*

4.1.1 Investigação em site

Link de sites com postagens falsas

1º passo – preservação com a coleta da prova (prova a existência da página). Setor pericial/técnico colerá adequadamente a prova para que se ateste que a evidência noticiada corresponde ao publicado. Essa extração gerará um código *hash* da URL (Uniforme Resource Locator - combinação única de letras, números e/ou caracteres, que localiza certo conteúdo único na internet)

2º passo – identificação de onde o *site* está hospedado.
O serviço de hospedagem (exs.: GoDaddy, UOL ou WordPress), em geral, informa os dados da pessoa que criou o *site* malicioso, o IP de criação e os *logs* de acesso ao *site*.

4.1.1 Investigação em site

Link de sites com postagens falsas

Serviço de anonimização – uma empresa de privacidade *on-line*, que registra o *site* na empresa de hospedagem, no lugar do real proprietário daquele domínio. Essa empresa possui os dados do real proprietário (dados cadastrais e financeiros).

Para consulta dos provedores de hospedagem e anonimização – https://registro.br (nacionais) ou https://Whois.icann.org (estrangeiros).

Sem vínculo com o Br - aba ou *e-mail* para reportar abusos – pode avisar a empresa sobre o conteúdo ilícito, pedindo a **preservação dos dados e a remoção do *site***. Pedir auxílio à PF, por meio do *e-mail* cybercrime_brazil_24x7@dpf.gov.br

4.1.1 Investigação em site

Link de sites com postagens falsas

3º passo – pedido de preservação de registros de criação do *site* e *logs* de acesso (IPs, data e hora) e de remoção do *site* malicioso

A empresa de hospedagem, ou anonimização, deve ser oficiada para preservar os dados do real usuário (dados do IP de criação da conta e *logs* de acesso, e dados cadastrais, inclusive financeiros) para posterior ordem judicial para envio dos dados.

4º passo – decisão judicial de quebra de sigilo telemático

Sem vínculo do provedor de hospedagem e/ou anonimização no Brasil - procedimento de cooperação jurídica internacional.

4.1.2 Investigação no Facebook e Instagram

1º passo – pedido de preservação no portal **https//: www.facebook.com/records. Hash e print da página.**

Precisa da **identificação correta da URL** do perfil que se pretende investigar.

As URLs das contas podem ser investigadas com:

a) o número de identificação do usuário (http://www.facebook.com/profile.php?id=1000000XXXXXXXX) ou o nome de usuário do perfil do Facebook, (http://www.facebook.com/nomedeusuario);
b) endereço de *e-mail* e
c) número de telefone (+55, DDD, número).

4.1.2 Investigação no Facebook e Instagram

Para localizar a URL:

No **computador**, ao acessar o **perfil**, a URL é exibida na barra de endereços do navegador. Se específica de uma **publicação ou comentário**: clique na respectiva data ou hora de disponibilização, que a URL aparecerá 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.

Ministério Público nas ELEIÇÕES 2026

4.1.2 Investigação no Facebook e Instagram

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.

Portal FACEBOOK para autoridades

- cadastro prévio (*e-mail* institucional)
- recebimento de link por e-mail
- acesso limitado por 1 hora
- solicitação de preservação de dados do Facebook e Instagram

Ministério Público nas ELEIÇÕES 2026

4.1.2 Investigação no Facebook e Instagram

HTTP://WWW.FACEBOOK.COM/RECORDS

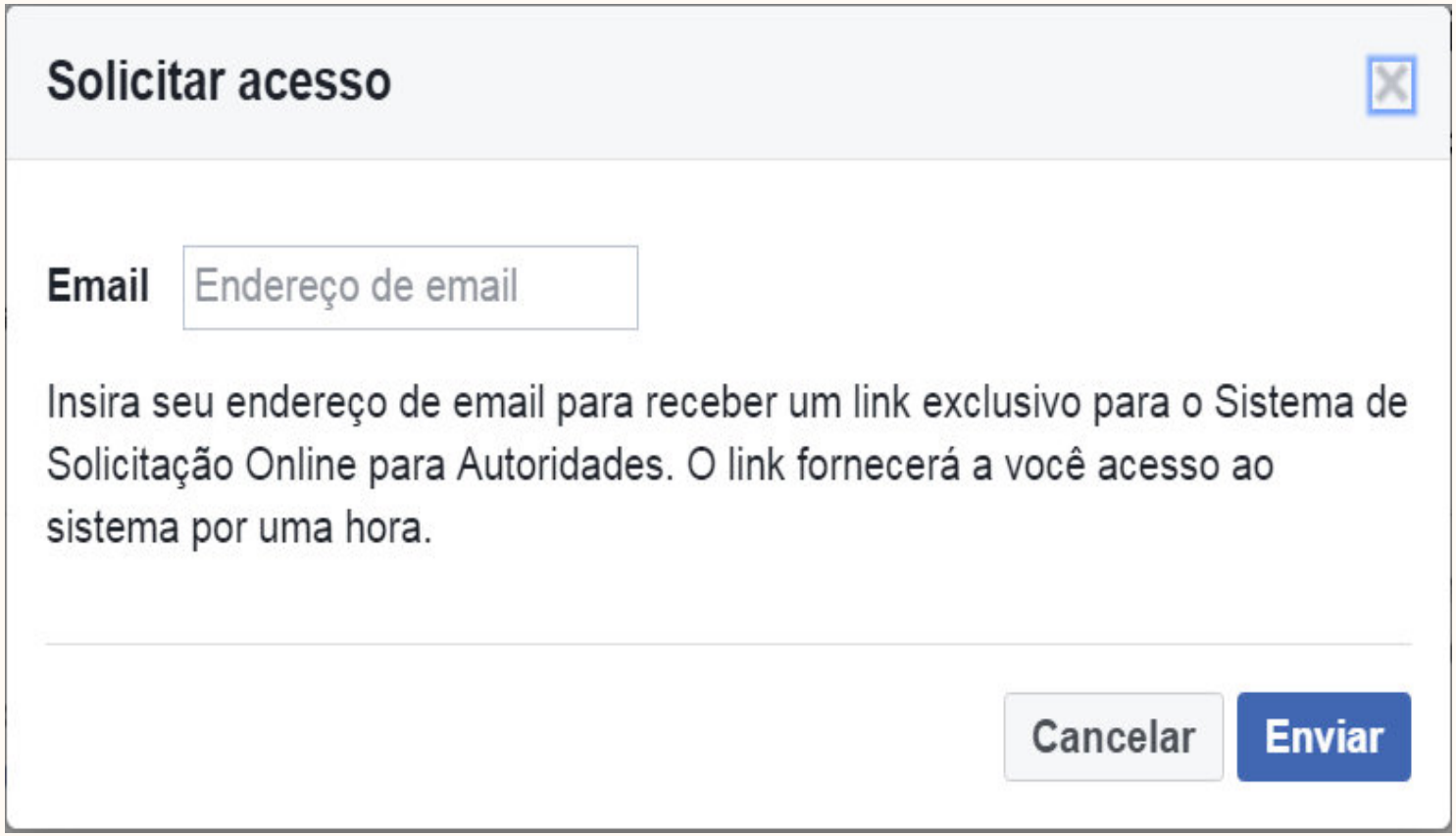
(ACESSO EXCLUSIVO PARA AUTORIDADES)

Ministério Público nas ELEIÇÕES 2026

4.1.2 Investigação no Facebook e Instagram

HTTP://WWW.FACEBOOK.COM/RECORDS

(ACESSO EXCLUSIVO PARA AUTORIDADES)

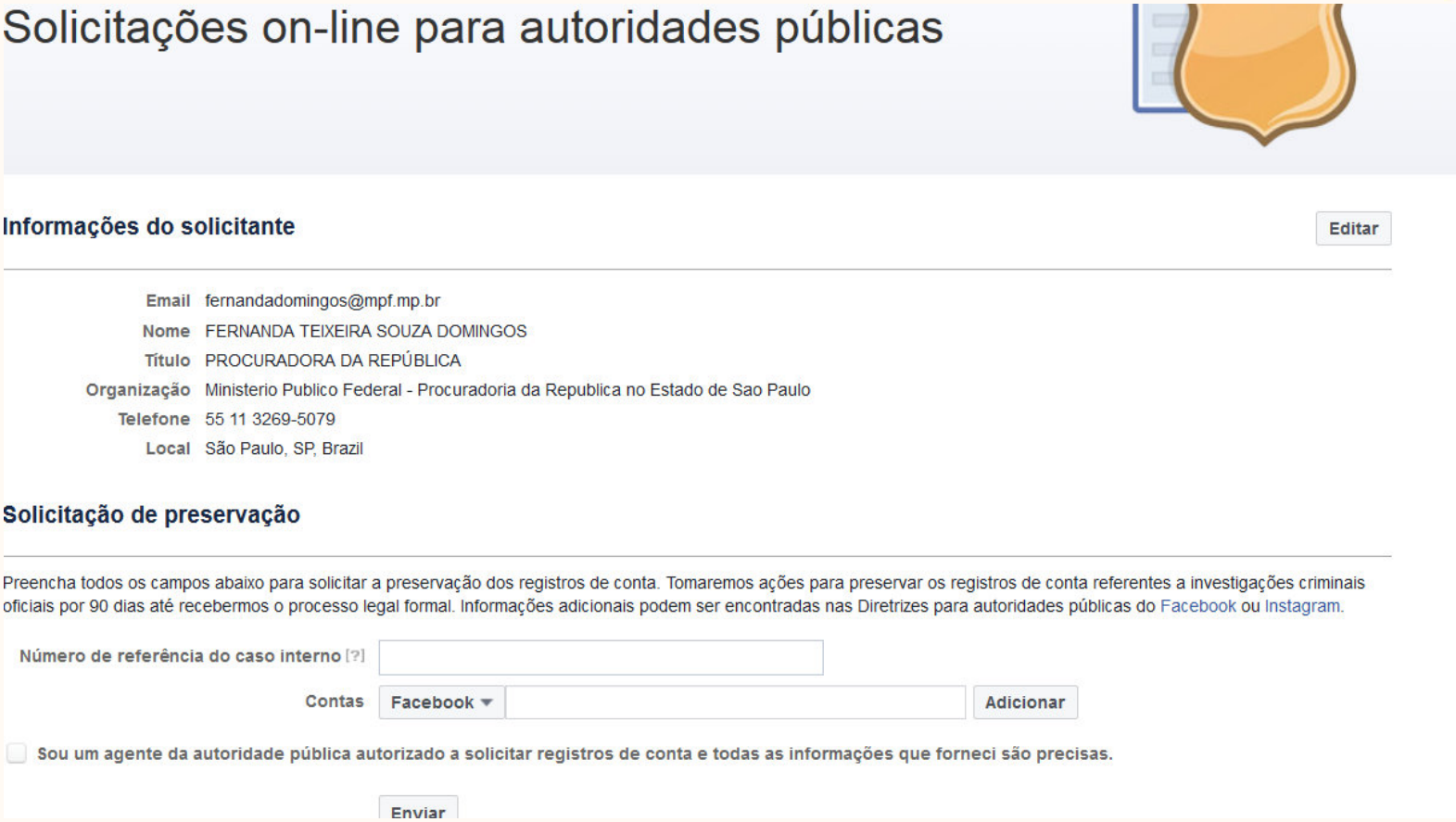


Ministério Público nas
ELEIÇÕES 2026

4.1.2 Investigação no Facebook e Instagram

HTTP://WWW.FACEBOOK.COM/RECORDS

(ACESSO EXCLUSIVO PARA AUTORIDADES)



Ministério Público nas ELEIÇÕES 2026

4.1.2 Investigação no Facebook e Instagram

O Sistema de Solicitação On-Line para Autoridades, localizado em **facebook.com/records**, está à disposição das Autoridades Policiais ou do Ministério Público para o envio, rastreamento e processamento de solicitações. Como proceder:

1) Acesse www.facebook.com/records;
2) Clique no item "*Sou um agente autorizado da autoridade política e esta é uma solicitação oficial*";
3) Clique em "*Solicitar acesso*";
4) Digite o seu endereço de **e-mail institucional** (exemplo: endereços terminados em gov.br, jus.br ou mp.br);
5) No e-mail cadastrado, você receberá uma mensagem com um link onde poderá submeter o pedido de acesso a registros. O link ficará disponível por uma hora.
6) Clique no link do e-mail recebido;
7) Clique em "*Solicitação de registros*" no topo da página;
8) Assegure-se de que as suas informações estão corretas. Se necessário, clique em "*editar*" para alterá-las;
9) Insira os dados solicitados;
10) "Número de referência do caso interno": n° IPL, proc ou PIC.

4.1.2 Investigação no Facebook e Instagram

2º passo - coleta adequada da prova - início à cadeia de custódia. As informações necessárias para acesso à publicação devem ser encaminhadas de imediato ao setor próprio para a extração do cálculo *hash;*

3º passo - se necessário, **pedido de retirada do conteúdo,** se ferir os termos de uso; diretamente ao Facebook (*e-mail* para records@facebook.com, com o *link* do conteúdo a ser retirado). – obter a URL específica da postagem que se quer remover, sob pena de ser retirado também conteúdo lícito;

4º passo – decisão cautelar de quebra de sigilo telemático para obtenção dos registros de acesso à aplicação e de *upload* e acessos, e, se necessário, **decisão judicial de retirada do conteúdo.** Ofícios pelo portal.

Ministério Público nas
ELEIÇÕES 2026

4.1.3 Investigação no WhatsApp

Ministério Público nas ELEIÇÕES 2026

4.1.3 Investigação no WhatsApp

Dois meios diferentes de propagação:

1) Envio de arquivo ou mensagem no aplicativo – **Preservação no Portal www.whatsapp.com/records** e investigação padrão.

2) Envio de ***link*** que remete a outro *site* na internet, onde efetivamente está o conteúdo ilícito. Não basta excluir a mensagem, porque o *link* continuará funcionando – investigação tem que seguir o padrão do item sobre **Desinformação em *sites*.**

É necessário informar o telefone do usuário.

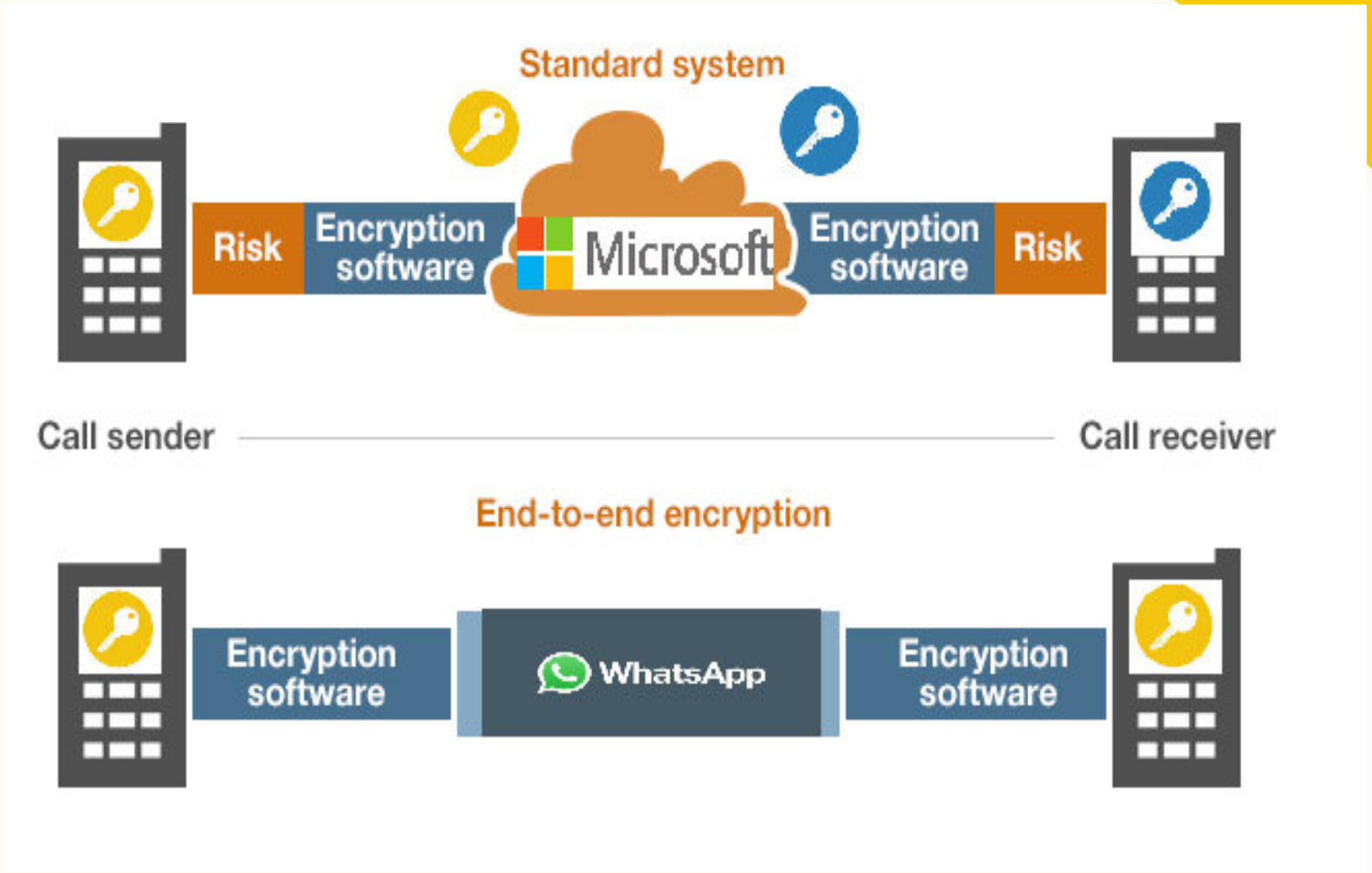
Ministério Público nas ELEIÇÕES 2026

4.1.3 Investigação no WhatsApp

Portal - HTTP://WWW.WHATSAPP.COM/RECORDS

Ministério Público nas
ELEIÇÕES 2026

4.1.3 Investigação no WhatsApp



Ministério Público nas ELEIÇÕES 2026

4.1.3 Investigação no WhatsApp

WHATSAPP - dados que podem ser solicitados (por ofício, via o portal www.whatsapp.com/records)

COM mandado judicial

(Medida cautelar)

- Informações de grupos (nomes e ID), de quais o investigado é administrador, participa e dos participantes
- Mudanças de números
- Agenda de Contatos
- Última conexão com IP, porta, data, hora

SEM mandado judicial

(Dados de Perfil):

- Nome
- Foto
- Telefone
- Modelo do Aparelho
- Versão do aplicativo
- *status* da conexão
- endereço de *e-mail*
- Informações do cliente WEB.

Ministério Público nas ELEIÇÕES 2026

4.1.3 Investigação no WhatsApp

Comunicação pelo WhatsApp, por utilizar Criptografia ponta-a-ponta, não se pode obter o conteúdo, mas, por medida cautelar de interceptação telemática, é possível obter os dados das comunicações:

1) **Extratos de mensagens: informações de remetente, destinatário, data e hora da mensagem;**
2) **tipo de mensagem;**
3) **IP da conta alvo, se disponível.**

Pode ser pedido que as informações sejam entregues a cada 24 h, a partir da implantação da medida até 15 dias seguintes.

Ministério Público nas ELEIÇÕES 2026

4.1.4 Investigação no Youtube

1ºpasso - pedido de preservação de dados pelo sistema *on-line* de Law Enforcement Request System da Google acessível pelo **portal http://lers.google.com**, na qual será necessária a criação de conta **(pedir que o usuário não seja notificado pelo prazo x).**
Ex. de uma URL de um vídeo específico:
https://www.youtube.com/whatch/v=2y-5hfZWADI

2º passo - coletar a evidência digital noticiada por meio de ferramentas forenses para extração do código hash;

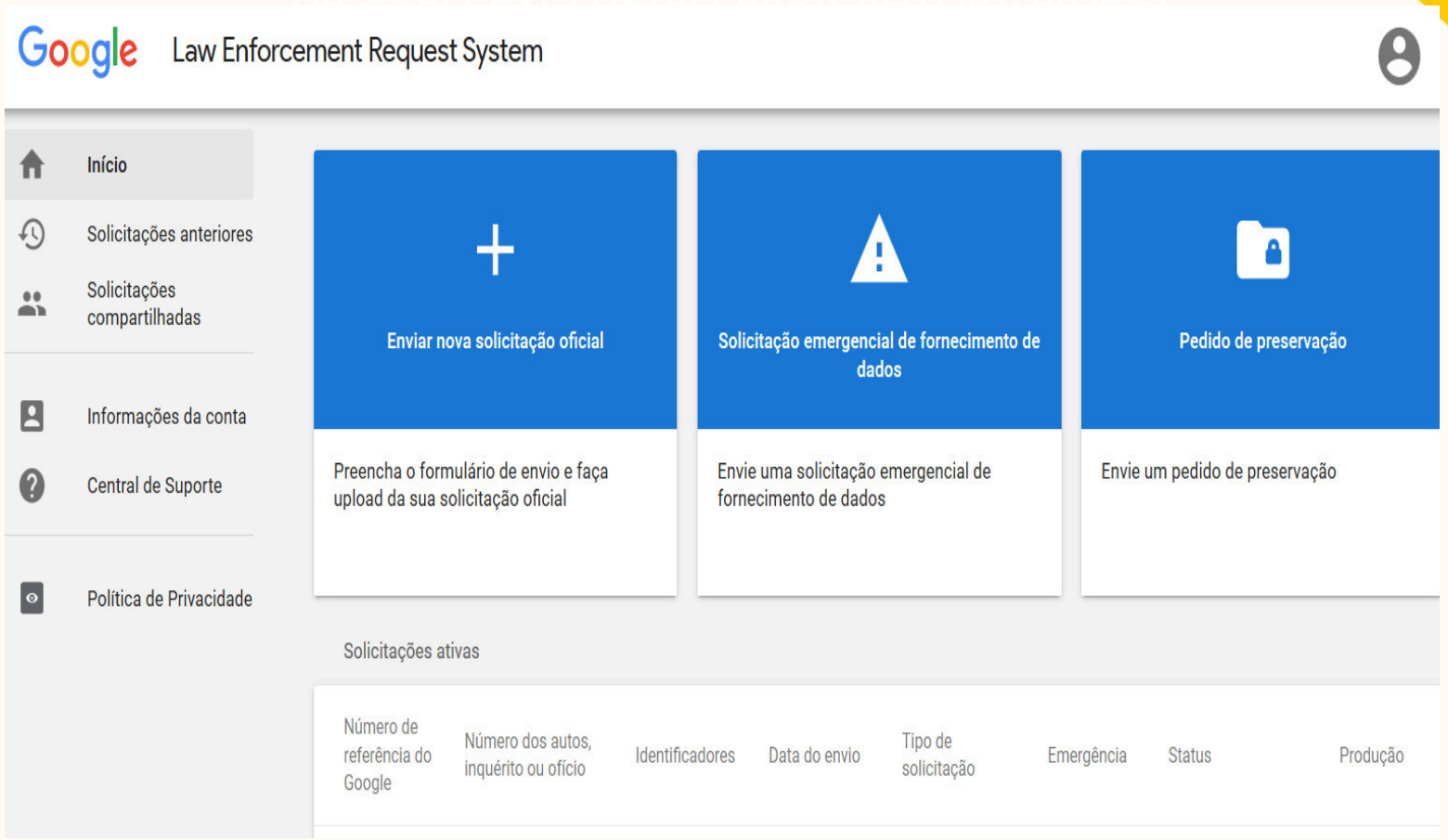
3º passo – pedido de retirada do conteúdo nocivo, caso viole seus Termos de Serviço: https://www.youtube.com/reportingtool/legal;

Ministério Público nas
ELEIÇÕES 2026

4.1.4 Investigação no Youtube

http://lers.google.com

(ACESSO EXCLUSIVO PARA AUTORIDADES)



Ministério Público nas ELEIÇÕES 2026

4.1.4 Investigação no Youtube

4º passo – decisão cautelar de quebra de sigilo telemático, e, se necessário, decisão judicial de retirada do conteúdo; para obtenção das seguintes informações, entre outras:

- *logs* de acesso (IP, porta, 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 armazenadas no Google Photos, dados armazenados no Google Drive, etc.

Oficios podem ser enviados também pelos *e-mails*: lis-latam@google.com e juridicobrasil@google.com

Ministério Público nas ELEIÇÕES 2026

4.1.5 Investigação no X

1º passo - pedido de preservação de dados era pelo sistema *on-line* https://legalrequests.twitter.com. **Infelizmente, em 2022, foi descontinuado o portal. Pedido de preservação e todos os demais devem ser para o email do X** (para o eleitoral o prov indica endereço distinto).

Deve conter a identificação do perfil infringente:
a) **nome do usuário e o URL do perfil do Twitter** envolvido (por exemplo, https://twitter.com/twittersafety (@twittersafety);
b) o **número de identificação do usuário ou UID exclusiva e pública da conta no Twitter** ou um **nome de usuário e URL do Periscope** (ex: @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#.

Ministério Público nas ELEIÇÕES 2026

4.1.5 Investigação no X

2º passo - coletar a evidência por meio de ferramentas forenses e extração do hash;

3º passo - retirada do conteúdo, se necessária. Seguir as orientações publicadas em https://help.x.com/pt/rules-and-policies/x-law- enforcement-support#;

4º passo – decisão cautelar de afastamento de sigilo telemático, e, se necessário, decisão judicial de retirada do conteúdo.

Ministério Público nas ELEIÇÕES 2026

4.1.5 Investigação no X

Informações que podem ser obtidas sobre o usuário:

- *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
- nº 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

Ministério Público nas ELEIÇÕES 2026

4.1.5 Investigação no X

Atribuíam o “selo azul de verificação” às contas de interesse público. Analisavam os dados fornecidos pelos titulares e confirmavam que esses eram autênticos e que efetivamente pertenciam à pessoa ou à marca que representavam (v.https://help.x.com/pt/managing-your- account/twitter-verified-accounts).Tal informação podia ajudar a verificar se o tweet investigado partiu realmente do titular da conta.

Atualmente, essas contas verificadas são pagas, e o serviço chama-se **PREMIUM X**, então a confiabilidade sobre essa verificação é relativa.

Ministério Público nas ELEIÇÕES 2026

5. Estratégia de Enfrentamento à Desinformação da PGE

Procuradoria Geral Eleitoral/2ª Câmara Criminal - PGR criaram:

Grupo de Trabalho sobre Desinformação na Internet, interferência cibernética na Democracia e influência nas Eleições (Portaria PGE/2ª CCR nº 1, de 21/10/2025).

Parceria: Instituto de Tecnologia e Sociedade do Rio (ITS-Rio) para **capacitação de membros do MPE e servidores** e,

Monitoramento de programas de IA dos principais provedores usados no País sobre as campanhas pres/gov/sen para verificar se foram respeitados padrões aceitáveis ou não nas respostas, com relatórios mensais ao GT de Desinformação na internet.

Monitoramento de notícias jornalísticas sobre desinformação eleitoral na internet e envio para o GT distribuir as notícias para as PREs com atribuição.

Ministério Público *nas*
ELEIÇÕES 2026

CONTATO

Neide Cardoso de Oliveira **neidec@mpf.mp.br**

Procuradora Regional da República

Coordenadora do Grupo de Trabalho de Desinformação na Internet, interferência cibernética na Democracia e processo eleitoral (GTDIE)

Obrigada !

MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA - CEARÁ
GABINETE DO PROCURADOR REGIONAL ELEITORAL/PRCE

Despacho nº 13717/2026

Referência: {{procedimentoPrincipal}}

Assunto: SOLICITAÇÕES DIVERSAS

Trata-se de Ofício Circular da Vice-PGE que encaminha o "Guia prático sobre Desinformação e Investigação na Internet" atualizado e ainda o material utilizado em palestra proferida pela Procuradora Regional da República Neide Mara Cavalcanti Cardoso de Oliveira, sobre o tema "Ilícitos Eleitorais na internet: como investigar?".

Divulgue-se no âmbito da PRE e encaminhe-se aos Promotores Eleitorais no Ceará.

Fortaleza, 8 de junho de 2026.

CELSO COSTA LIMA VERDE LEAL

PROCURADOR REGIONAL ELEITORAL