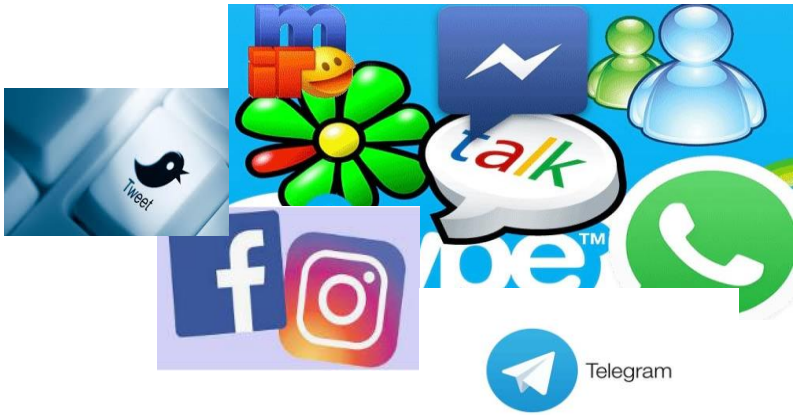
ATAQUES DIGITAIS E ASSÉDIO ONLINE

INVESTIGAÇÃO NA INTERNET e

PRESERVAÇÃO DE EVIDÊNCIAS

Procuradoria Regional Eleitoral-RJ



1. Propaganda eleitoral na internet

1.1 Jurisprudência

1.2 Propaganda eleitoral e uso de IA

2. Crimes de coação eleitoral (assédio)

3. Remoção de conteúdo na internet

3.1 Identificação do usuário eleitoral

4. Investigação para identificar o usuário

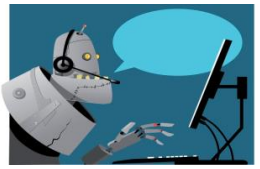
1. Propaganda eleitoral na internet

- Não é admitida a veiculação de conteúdos de cunho eleitoral mediante cadastro de usuário de aplicação de internet com a intenção de falsear identidade.(**LE, Art. 57-B, § 2º, e Res. TSE nº 23.610/19, Art. 28, § 2º).**

- É vedado o anonimato, na campanha, por meio da internet. (**LE, Art. 57-D, Res. TSE nº 23.610/19, Art. 30).** Visa evitar o uso indevido da internet (agressões gratuitas, mesquinharias, e eleva o nível da disputa eleitoral). **Art.30, § 1º -** a multa não se aplica ao provedor de aplicação de internet.

- É vedada a realização de propaganda eleitoral na internet, "*atribuindo indevidamente sua autoria a terceiro, inclusive a candidato, partido, federação ou coligação*." (**LE, Art. 57-H, Res. TSE nº 23.610/19, Art. 35).**

1. Propaganda eleitoral na internet



➢ É **vedada** a realização de propaganda eleitoral:

I - via telemarketing em qualquer horário (STF, ADI n.5122/DF, de 20/2/20);

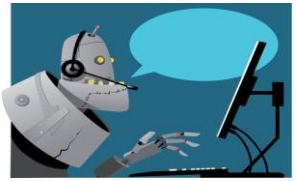
II – por meio de **disparo em massa de mensagens instantâneas sem consentimento da pessoa destinatária ou a partir da contratação expedientes, tecnologias ou serviços não fornecidos pelo provedor de aplicação e em desacordo com seus termos de uso.** (CF, Art. 5º, X e XI; CE, Art. 243,VI; LE, Art. 57-J; **Res. TSE nº 23.610/2019, Art. 34)**

Abusos e excessos serão apurados de acordo com o Art. 22, da LC 64/90 (Res. 23.610/19, Art. 34, § 2º).

1. Propaganda eleitoral na internet

Disparo em massa – estratégia coordenada de envio, compartilhamento ou encaminhamento de um mesmo conteúdo, ou de suas variações, para grande número de destinatárias (os), por qualquer meio de comunicação interpessoal. (Res. TSE nº 23.610/19, Art. 37, inc. XXI, com a redação dada pela Res. TSE nº 23.732/2024)

Os **partidos políticos, feds, coligações, candidatas (os) ou seus representantes ou qualquer pessoa natural são proibidos de contratar serviços de disparo em massa de conteúdo.** (Res. TSE nº 23.610/2019, Art.28, inc. IV, com a redação dada pelas Res. TSE nº 23.671/2021 e nº 23732/24)



1.1 Jurisprudência

"AÇÕES DE INVESTIGAÇÃO JUDICIAL ELEITORAL. ELEIÇÕES 2018. PRESIDENTE DA REPÚBLICA. VICE-PRESIDENTE. TERCEIROS. PRELIMINARES. REJEIÇÃO. TEMA DE FUNDO. ABUSO DO PODER ECONÔMICO. USO INDEVIDO DOS MEIOS DE COMUNICAÇÃO SOCIAL. ART. 22 DA LC 64/90. UTILIZAÇÃO. SERVIÇOS. DISPAROS EM MASSA. APLICATIVO DE MENSAGENS INSTANTÂNEAS (WHATSAPP). BENEFÍCIO. CANDIDATURAS. PROPOSTA DE TESE. CASO DOS AUTOS. ELEMENTOS DE PROVA. CIRCUNSTÂNCIAS. INDÍCIOS. COMPROVAÇÃO. DISPAROS. EXAME. GRAVIDADE DOS FATOS. AUSÊNCIA. ELEMENTO ESSENCIAIS. IMPROCEDÊNCIA."

(AIJEs 0601968-80/DF e 0601771-28/DF, acórdão; Relator Min. Luiz Felipe Salomão, j. 28/10/2021)

1.1 Jurisprudência

"*Ataques infundados ao sistema eletrônico de votação e à democracia, em benefício de candidato, inclusive pela internet e pelas redes sociais, induzindo o eleitor à falsa ideia de fraude, podem caracterizar abuso de poder e uso indevido dos meios de comunicação social e ensejar cassação do registro ou diploma, além de inelegibilidade por oito anos, conforme o art. 22 da LC 64/90*".

(TSE - RECURSO ORDINÁRIO ELEITORAL Nº 0603975-98 – CLASSE 11550 – CURITIBA – PARANÁ RELATOR: MINISTRO LUIS FELIPE SALOMÃO, j. 28/10/21; após liminar concedida pelo Min. Nunes Marques do STF suspendendo a cassação; o colegiado da 2ª Turma do STF restabeleceu a decisão original do TSE de cassação do mandato do deputado estadual do Paraná, em j. 7/6/22).

1.1 Jurisprudência

Tese: o uso de aplicações digitais de mensagens instantâneas, visando promover disparos em massa, contendo **desinformação e inverdades** em prejuízo de adversários e em benefício de candidato, pode configurar abuso de poder econômico e/ou uso indevido dos meios de comunicação social para os fins do art. 22, *caput* e XIV, da LC 64/90.

As provas devem ter elementos preponderantes:

(i) sobre o teor das mensagens (propaganda negativa ou informações inverídicas);
(ii) de que forma o conteúdo repercutiu perante o eleitorado;
(iii) o alcance do ilícito em termos de mensagens veiculadas;
(iv) o grau de participação dos candidatos;
(v) se a campanha foi financiada por empresas com esse fim.

1.2 Propaganda eleitoral e uso de IA

USO DE INTELIGÊNCIA ARTIFICIAL (IA) NA PROPAGANDA ELEITORAL

- **É obrigatório o aviso sobre o uso de IA na propaganda eleitoral.**
- **Não é permitida deepfakes (deep learning+fake).**
- **Restrição do uso de robôs para intermediar contato com o eleitor (a campanha não pode simular diálogo com candidato ou qualquer pessoa).**
- **Responsabilização dos provedores de internet que não retirarem do ar, imediatamente, conteúdos com desinformação, discurso de ódio, antidemocráticos, racistas, homofóbicos, de ideologia nazista e fascista (nova interpretação do STF do Art.19, do MCI, julgamento no dia 26/6/2025, Informativo STF)**

1.2 Propaganda inverídica e uso de IA

USO DE INTELIGÊNCIA ARTIFICIAL (IA) NA PROPAGANDA ELEITORAL

Res. TSE 23.610/2019, Art. 9º-B. A utilização na propaganda eleitoral, em qualquer modalidade, de conteúdo sintético multimídia gerado por meio de inteligência artificial para **criar, substituir, omitir, mesclar ou alterar a velocidade ou sobrepor imagens ou sons** impõe ao responsável pela propaganda o **dever de informar**, de modo explícito, destacado e acessível que o conteúdo foi fabricado ou manipulado e a tecnologia utilizada. (Incluído pela Res 23.732/2024)

§ 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.

1.2 Propaganda inverídica e uso de IA

USO DE INTELIGÊNCIA ARTIFICIAL (IA) NA PROPAGANDA ELEITORAL

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 Res TSE nº 23.732/2024)

§ 1º É **proibido o uso, para prejudicar ou para favorecer candidatura**, de **conteúdo sintético** em formato de áudio, vídeo ou combinação de ambos, que tenha sido gerado ou manipulado digitalmente, ainda que mediante autorização, **para criar, substituir ou alterar imagem ou voz de pessoa viva, falecida ou fictícia** (deep fake).

2. Crimes de coação (assédio) para obter voto

Art. 300, CE. Valer-se o servidor público da sua autoridade para coagir alguém a votar ou não votar em determinado candidato ou partido:
Pena - detenção até seis meses e pagamento de 60 a 100 dias-multa.
Parágrafo único. Se o agente é membro ou funcionário da Justiça Eleitoral e comete o crime prevalecendo-se do cargo a pena é agravada.

Art. 301, CE. Usar de violência ou grave ameaça para coagir alguém a votar, ou não votar, em determinado candidato ou partido, ainda que os fins visados não sejam conseguidos:
Pena - reclusão até quatro anos e pagamento de cinco a quinze dias-multa.

2. Crimes de coação (assédio) para obter voto

Art. 300, do CE - próprio de servidor público, é uma versão especializada do crime de concussão, cuja pena é de 2 a 12 anos – tem uma pena muito subestimada.

A pessoa coagida deve ser eleitora da circunscrição em disputa, apta a votar naquele local. Sem isso: crime impossível (Art. 17, do CP).

O assédio eleitoral pode ser comprovado:

Digital: mensagens, comentários, e-mails, postagens em redes sociais (Instagram, Threads, X, Facebook,Tiktok, etc.)
Físico: documentos, imagens, áudios, ligações telefônicas gravadas, vídeos, registros de ocorrências em canais internos (ouvidorias) de órgãos públicos (ou de empresas).

2. Crimes de coação (assédio) para obter voto

- Crime de baixo potencial ofensivo – Art. 300, CE (não cabe prisão flagrancial – nessa situação assina o termo circunstanciado para comparecer em juízo) ou de médio potencial ofensivo (Art. 301, CE);

- crime formal – se consuma com a promessa, direta ou velada, de causar mal injusto e grave à pessoa (Art. 301); não se exige a efetiva entrega do voto ou a abstenção.

- admite transação penal (Art. 76, da Lei nº 9.00/95)-Art. 300, CE;

- admite o *sursis* processual – Art.301, CE;

- não admite o ANPP (Art. 28-A, do CPP) – a coação por si só é uma forma de grave ameaça (Art. 300) e o Art. 301, diz expressamente que ocorre por meio de violência/grave ameaça.

2. Crimes de coação (assédio) para obter voto

Art. 301, CE. Objetividade jurídica é a liberdade de voto do eleitor, que se busca por meio da violência (contra a pessoa apta a votar) ou da grave ameaça (pode ser contra terceira pessoa).
Sujeito ativo – qualquer pessoa. Vítima – eleitor coagido.

Dolo específico – obter o voto ou a promessa de não votar em certo candidato/partido.

Absorve os crimes de ameaça e lesão corporal (Arts. 147 e 129, do CP). Sem absorção (consunção), há concurso de crimes, se as lesões são graves (pena de 1 a 5 anos) ou gravíssimas (pena 2 a 8 anos). Se resultar morte (pena de 4 a 12 anos) ou homicídio (12 a 30 anos), são absorvidos por esses.
Não se incluem as condutas de organizações criminosas para impedir atos de propaganda eleitoral em certos lugares (Art.332, CE). A pena não autoriza a aplicação da Lei nº 12.850/2013.

3. Remoção de conteúdo na internet

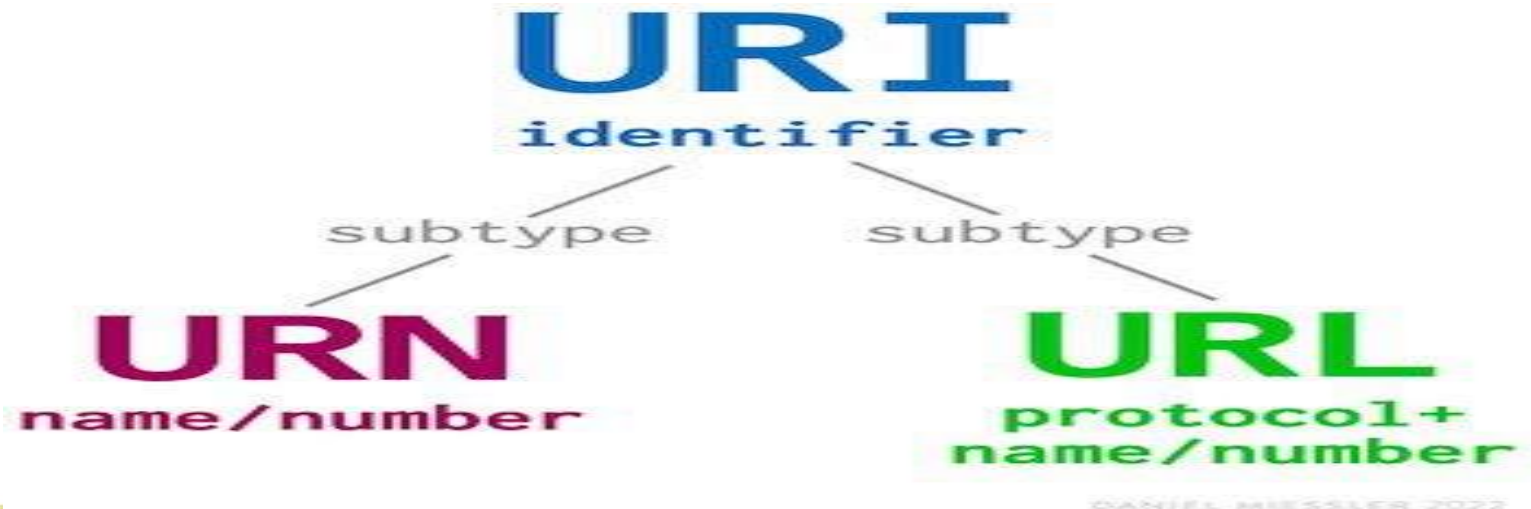
REMOÇÃO DE CONTEÚDO DA INTERNET

Res. TSE nº 23610/2019, Art. 38. A atuação da Justiça Eleitoral em relação a conteúdos divulgados na internet deve ser realizada **com a menor interferência possível no debate democrático.** **(Lei nº 9.504/1997, Art. 57-J)**

§ 1º Com o intuito de assegurar a liberdade de expressão e impedir a censura, as ordens judiciais de remoção de conteúdo divulgado na internet serão limitadas às hipóteses em que, mediante decisão fundamentada, sejam constatadas violações às regras eleitorais ou ofensas a direitos de pessoas que participam do processo eleitoral.

3. Remoção de conteúdo na Internet

§ 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.



3. Remoção de conteúdo na internet

URI - Uniforme Resource Identifier (Identificador de Recurso Uniforme), combinação única de letras, números e/ou caracteres, 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 ela se localiza, que é o protocolo – https://)**

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

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

3. Remoção de conteúdo na internet

REMOÇÃO DE CONTEÚDO DA INTERNET
PODER DE POLÍCIA

Res. TSE nº 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;

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

3. Remoção de conteúdo na internet

Exceções para retirada de conteúdo, sem ordem judicial:

- **Descumprimento de normas dos termos de uso**. Vários provedores de aplicação, como Facebook, Instagram, Google, possuem provimentos específicos, em seus termos de uso, para exclusão de conteúdo danoso, inclusive aquele com informações deturpadas.

- Se há a **prática de crime**: utilização dos serviços para a prática de crime viola os termos de uso, o que permite a exclusão rápida. Informativo do STF sobre a nova interpretação do Art. 19, do MCI (27/6/25)

3. Remoção de conteúdo na internet

Res. TSE nº 23.610/2019, Art. 9º-D, § 5º.

As ordens para remoção de conteúdo, suspensão de perfis, fornecimento de dados ou outras medidas determinadas pelas autoridades judiciárias, no exercício do poder de polícia ou nas ações eleitorais, observarão o disposto nesta Resolução e na Res.TSE nº 23.608/2019, cabendo aos provedores de aplicação cumpri-las e, se o integral atendimento da ordem depender de dados complementares, informar, com objetividade, no prazo de cumprimento, quais dados devem ser fornecidos. (Incluído pela Resolução nº 23.732/2024)

3.1 Identificação do usuário eleitoral

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 (**Lei 12.965/2014, Art.10, caput, § 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 (**Lei 12.965/2014, Art. 22**).

3.1 Identificação do usuário eleitoral

IDENTIFICAÇÃO DO USUÁRIO

Res. TSE nº 23610/2019, Art. 40, § 1º. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade (**Lei 12965/14, Art. 22, parágrafo único**):

I - fundados indícios de ocorrência do ilícito de natureza eleitoral;
II - justificativa motivada da utilidade dos dados solicitados para fins de investigação ou instrução probatória;
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.

3.1 Identificação do usuário eleitoral

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.

1. Investigação para identificar o usuário

1.1 Desinformação em site

1.2 Desinformação no Facebook/Instagram

1.3 Desinformação no WhatsApp

1.4 Desinformação no Youtube

1.5 Desinformação no X (ex-Twitter)

1.6 Desinformação no Telegram

1. Investigação 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

1. Investigação para identificar o usuário

USUÁRIO → INTERNET → APLICAÇÕES DA INTERNET

PROVEDOR DE CONEXÃO:

PROVEDOR DE CONTEÚDO

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)?

1. Investigação para identificar o usuário

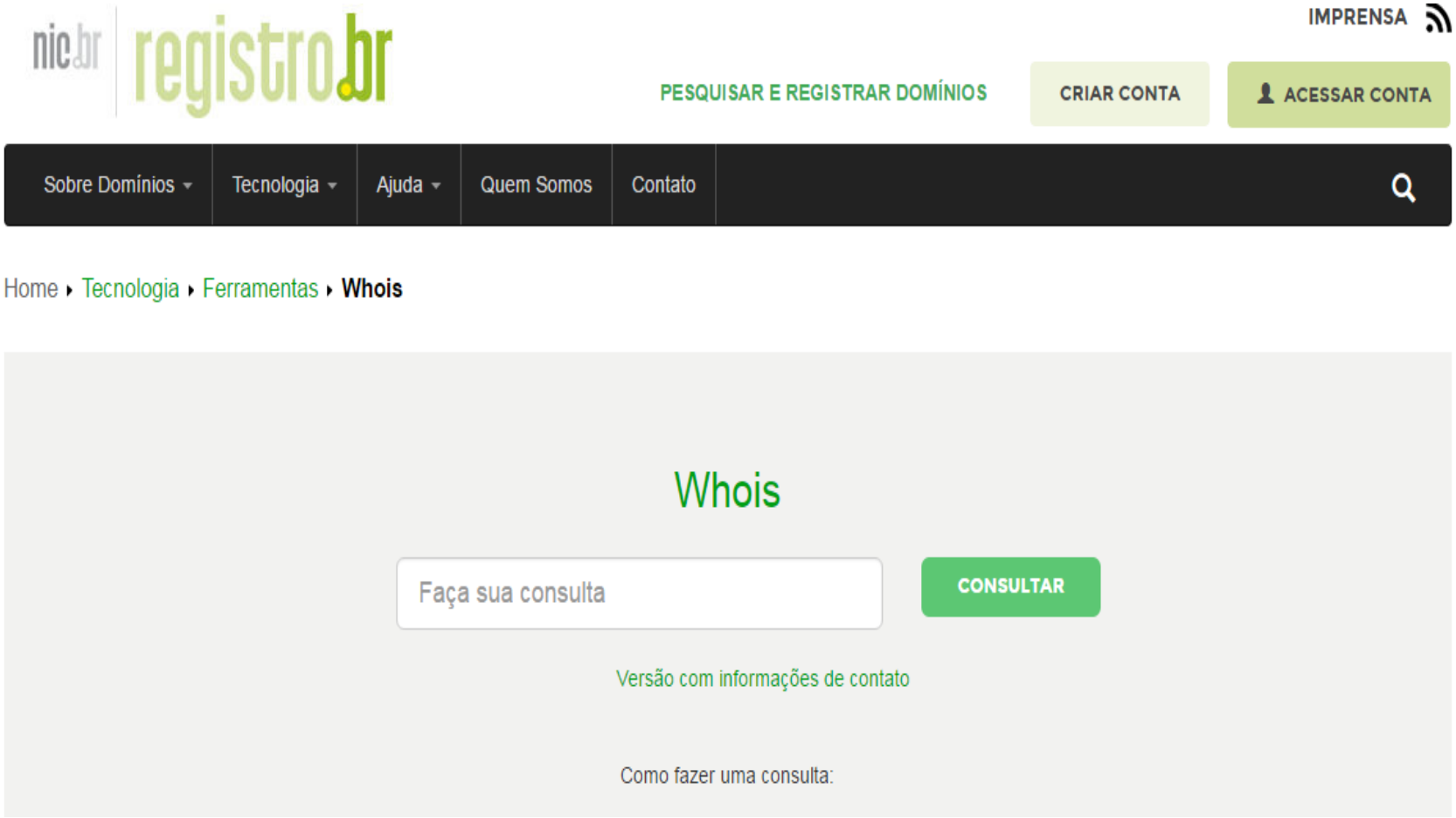
1. IDENTIFICAÇÃO DOS RESPONSÁVEIS PELO SERVIÇO

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

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

1. Investigação para identificar o usuário

1. IDENTIFICAÇÃO DOS RESPONSÁVEIS PELO SERVIÇO



1. Investigação para identificar o usuário

2. PRESERVAÇÃO DAS PROVAS (cadeia de custódia)

Salvar e garantir integridade dos dados:

- Prova digital: volátil
- Autenticidade: **garantir que a informação veio mesmo de onde se alega (obtenção direta do provedor: URL deve ser certificada com a geração de um código *hash*)**
- Integridade: **garantir que o manuseio da prova não a altera**

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;

✓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.

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 (se o IP for nateado);
•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.

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

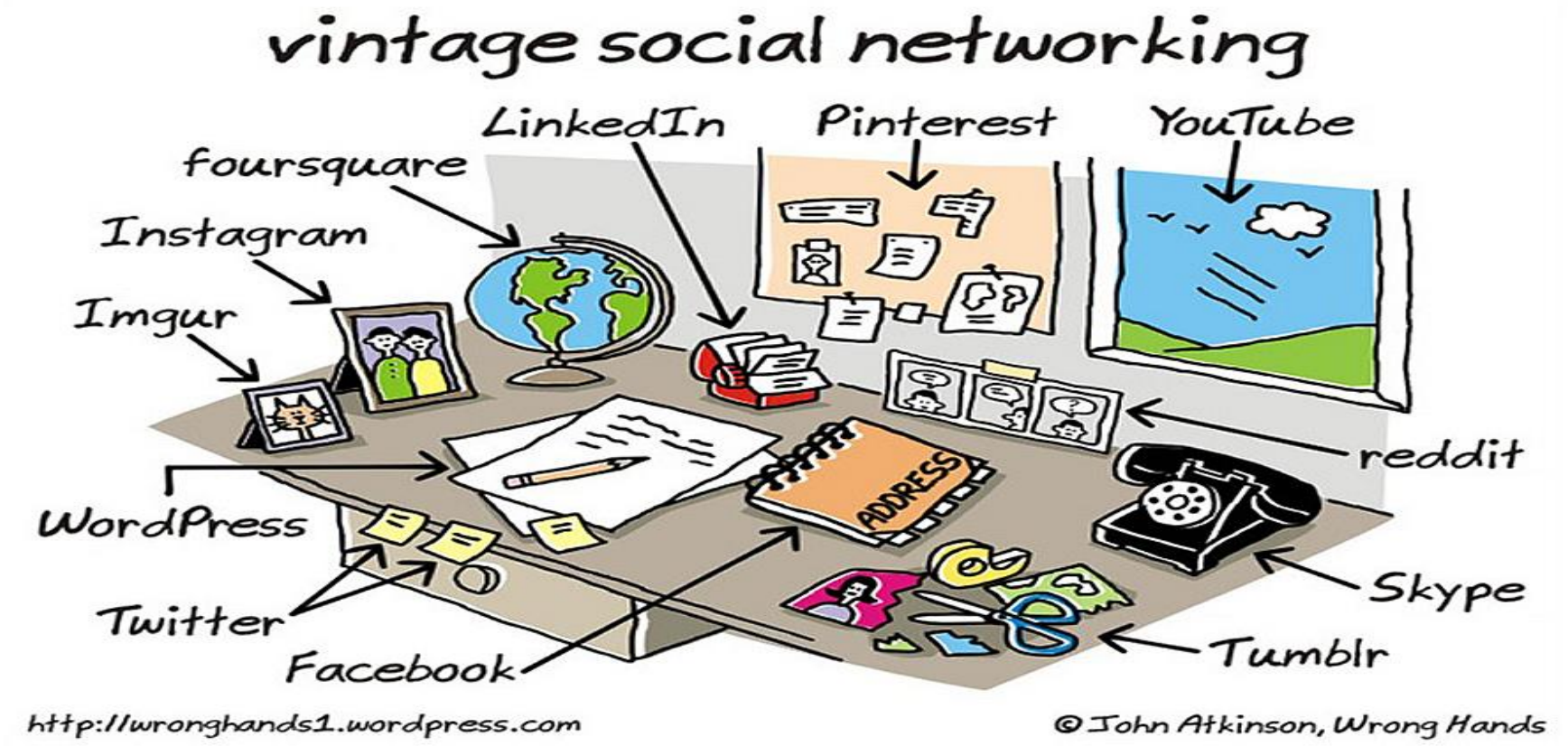
4. QUEBRA DE SIGILO DE DADOS TELEMÁTICOS (DADOS CADASTRAIS DO USUÁRIO)

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).

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* (*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.*

1.1 Investigação em site

Link de sites com postagens falsas

1º passo – preservação com a coleta da prova (prova a existência da página). Deve ser gerado um código *hash* da URL (combinação única de letras, números e/ou caracteres, que localiza certo conteúdo único na internet)

Setor pericial/perito colerá adequadamente a prova para que se ateste que o material corresponde ao publicado (essa extração gerará um código *hash*).

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*.

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

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.

1.2 Investigação no Facebook/Instagram

1º passo – pedido de preservação no portal **https//: www.facebook.com/records. Gerar o hash da página/perfil**

Precisa da **identificação correta da URL** http://t.me/allandossantos) 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).

1.2 Investigação no Facebook/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.

1.2 Investigação no Facebook/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

1.2 Investigação no Facebook/Instagram

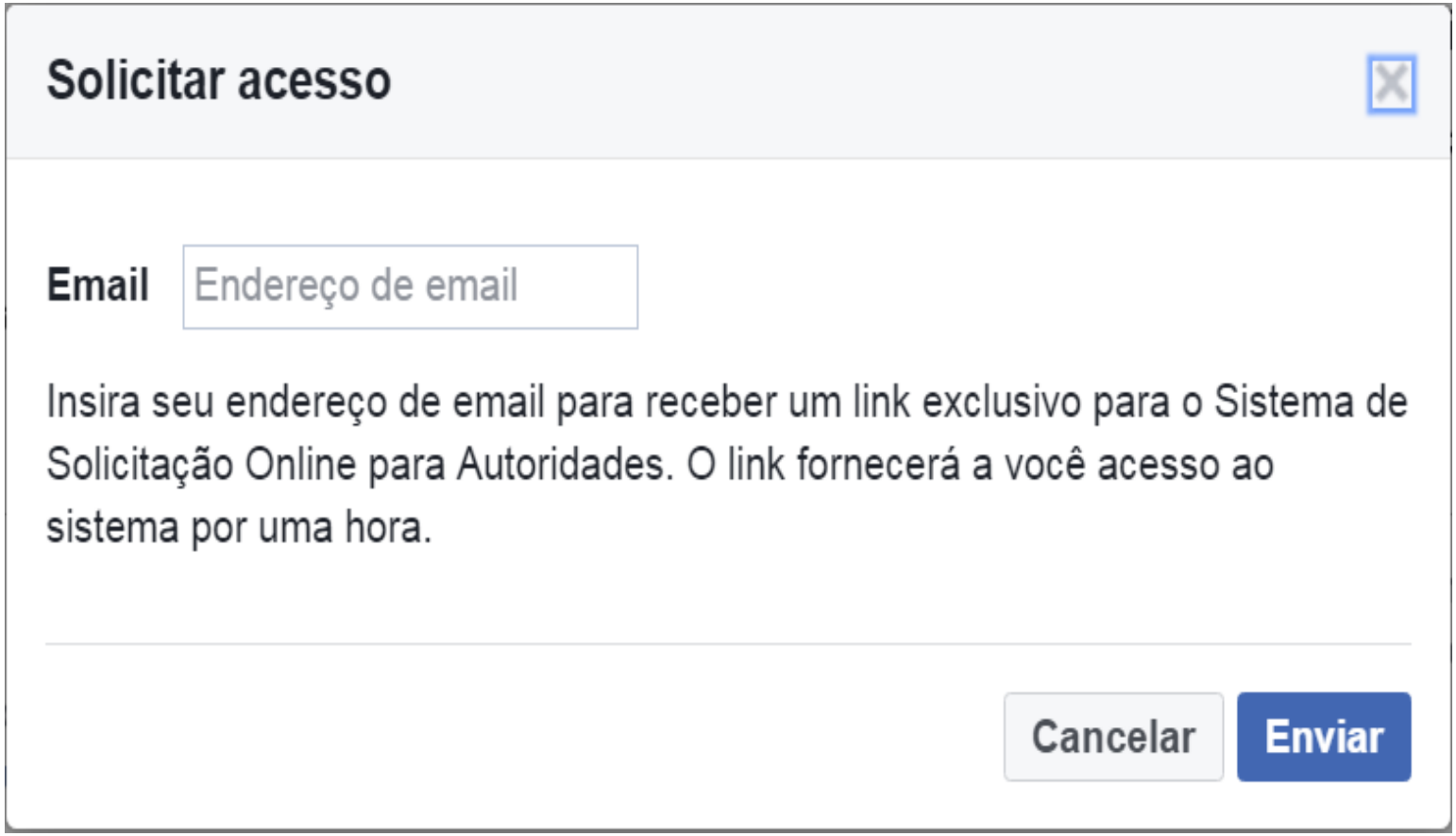
HTTP://WWW.FACEBOOK.COM/RECORDS

(ACESSO EXCLUSIVO PARA AUTORIDADES)

1.2 Investigação no Facebook/Instagram

HTTP://WWW.FACEBOOK.COM/RECORDS

(ACESSO EXCLUSIVO PARA AUTORIDADES)



1.2 Investigação no Facebook/Instagram

2º passo - colheita 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.

1.3 Investigação no WhatsApp

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 com DDD.

1.3 Investigação no WhatsApp

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

1.3 Investigação no WhatsApp

1.3 Investigação no WhatsApp

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

COM mandado judicial (Med. caut):

- Informações de grupos: data da criação; descrição; Identificador de grupo (Group ID), foto; quantidade de membros; nome do grupo; participantes
- Mudanças de números
- Contatos simétricos (o alvo tem o nº do contato na sua agenda e contato do alvo, na sua). Assimét.:pedido
- Status antigos e Foto de perfil
- Registro de IP sem porta lógica, dos últimos 6 meses (cada conexão ao serviço após período off line).

SEM mandado judicial

(dados de Perfil):

- Nome do usuário
- Número do telefone
- Modelo do Aparelho
- Versão do aplicativo
- Data inicial e final da conta
- *Status* da conexão
- Endereço de *e-mail vinculado à conta*
- Data da última conexão
- Informações do cliente WEB.

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.

1.4 Investigação no Youtube

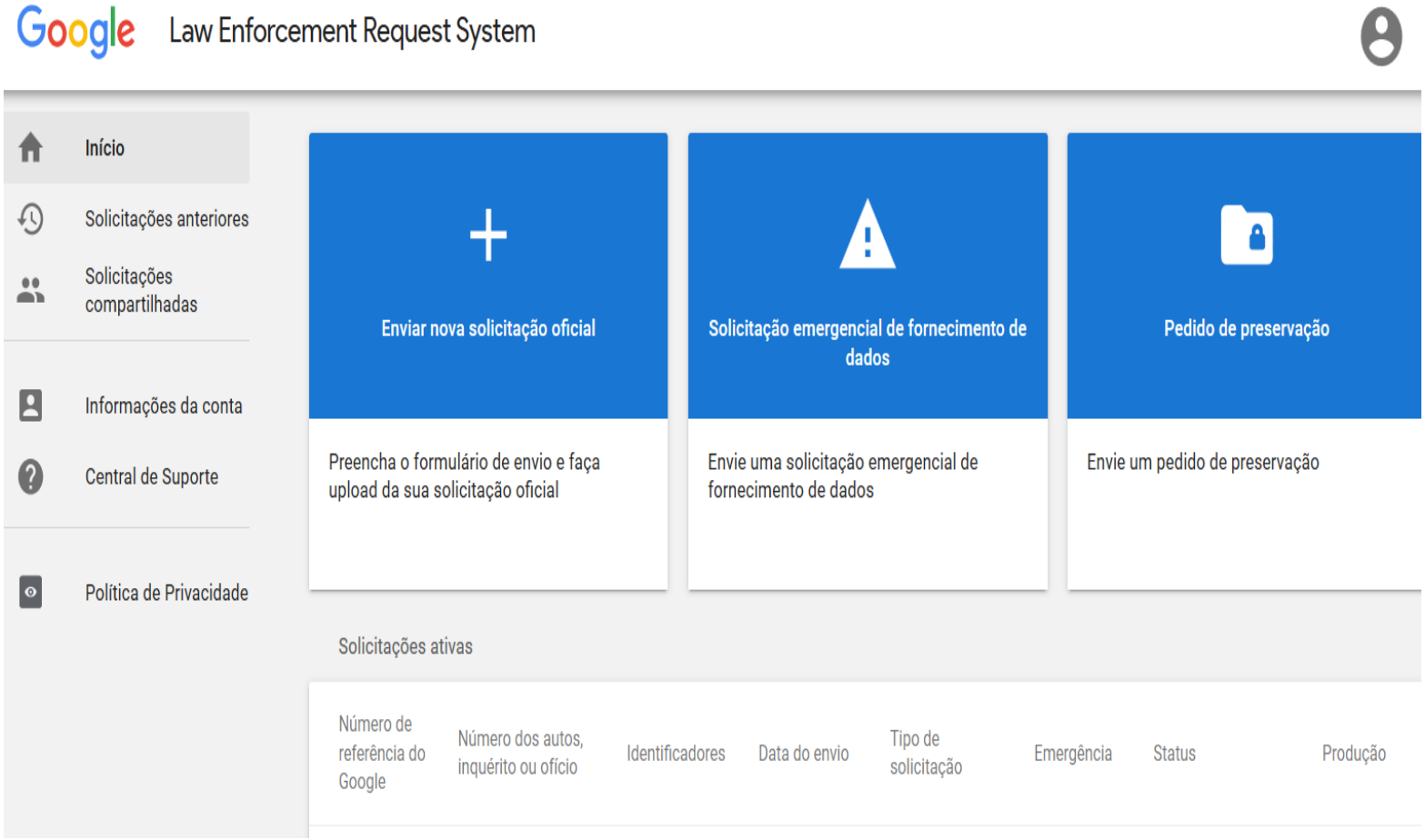
1ºpasso - pedido de preservação de dados pelo sistema *on-line* de Law Enforcement Request System da Google acessível pelo **portal http://lers.google.com**, na qual será necessária a criação de conta.
Ex. de uma URL de um vídeo específico:
https://www.youtube.com/whatch/v=2y-5hfZWADI

2º passo - coletar a prova por meio de ferramentas forenses para gerar o hash e print das telas.

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

1.4 Investigação no Youtube

http://lers.google.com



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

1.5 Investigação no X (ex-Twitter)

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 por email.**

Deve conter a identificação do perfil infringente:
a) **nome do usuário e o URL do perfil do X** envolvido (por exemplo, https://x.com/xsafety (@xsafety);
b) o **número de identificação do usuário ou UID exclusiva e pública da conta no X** ou um **nome de usuário e URL do Periscope** (ex: @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-policies/x-law-enforcement-support#.

1.5 Investigação no X (ex-Twitter)

2º passo - coletar a prova por meio de ferramentas forenses e print da (s) mensagem (ns);

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. Os ofícios podem ser enviados para o email (e para o endereço físico):

br_legalrequests@x.com

Av. Imperatriz Leopoldina, 1248, sala 203, BA088, Vila Leopoldina, Município de São Paulo/São Paulo, CEP 05305-002

1.5 Investigação no X (ex-Twitter)

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

1.5 Investigação no X (ex-Twitter)

Atribuíam antigamente o chamado "**selo azul de verificação**" às contas de interesse público. Analisavam os dados fornecidos pelos titulares (pessoas famosas ou notórias) e confirmavam que esses eram autênticos e que efetivamente pertenciam à pessoa ou à marca que representam.

Atualmente, o mesmo serviço é denominado "**X Premium**", essas contas "verificadas" são vendidas, então a confiabilidade sobre essa verificação é relativa, mas pode ajudar a identificar o titular da conta.

1.6 Investigação no Telegram

Pedidos de bloqueios da conta com nome do perfil, ex.: link - http://t.me/nome

O email "oficial" é **content.referral-c1@telegram.org**

CONTATO

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

Procuradora Regional Eleitoral

Coordenadora Adjunta

Grupo de Atuação Especial sobre Crimes Cibernéticos e crimes praticados por meio das Tecnologias da Informação (GACCTI)

Obrigada !