Coordenação
HIGOR VINICIUS NOGUEIRA JORGE
Prefácio **MÁRCIO ADRIANO ANSELMO**
Apresentação **FRANCISCO SANNINI NETO**

Enfrentamento da Corrupção e Investigação Criminal Tecnológica

3ª edição revista, atualizada e ampliada

Procedimentos, Fontes Abertas, Estudo de Casos e Direito Anticorrupção

Alesandro Gonçalves Barreto
Alexsander Castro de Oliveira
Andrei Fragoso Rocha de Oliveira
César Henrique Sanfelice Rocha de Oliveira
Delmar Araújo Bittencourt
Gustavo André Alves
Hélio Molina Jorge Júnior
Hericson dos Santos
Higor Vinicius Nogueira Jorge
Ivana David
Janio Konno Júnior
João Leonardo de Andrade Júnior
Joaquim Leitão Júnior
Jorge André Domingues Barreto
Jorge Figueiredo Junior
Juan Manuel Aguilar Antonio
Letícia Sabbadini Muller
Luciano Henrique Cintra
Marcelino de Andrade Amaral
Márcio Rogério Porto
Marcos Vinícius Alves e Silva Filho
Marcos Vinnícius Marinho Monteiro
María Angélica Castillo Ríos
Milena Santana de Araújo Lima
Murillo Ribeiro de Lima
Murillo Yago Batalha
Octávio Celso Gondim Paulo Neto
Rafael Francisco Marcondes de Moraes
Rafael Velasquez Saavedra da Silva
Ricardo Magno Teixeira Fonseca
Romina Florencia Cabrera
Ruchester Marreiros Barbosa
Sérgio Hussein Mourad Tenório
Ulisses da Nobrega Silva
Wagner Andrade de Lucena
Wagner Martins Carrasco de Oliveira
Walter Martins Muller

2023
EDITORA JusPODIVM
www.editorajuspodivm.com.br

1

EMPREGO DO AFASTAMENTO DO SIGILO PERANTE GOOGLE E APPLE NO ENFRENTAMENTO DA CORRUPÇÃO

Higor Vinicius Nogueira Jorge[1],
Márcio Rogério Porto[2],
Hélio Molina Jorge Júnior[3] **e**
Ulisses da Nóbrega Silva[4]

Sumário: 1. Introdução. **2.** Classificação das fontes de dados. **3.** Google. **4.** Dados armazenados na "Sua linha de tempo" do Google Maps e outras informações de localização. **5.** Histórico de exibição, histórico de pesquisas, curtidas e comentários do Youtube. **6.** Histórico de pesquisas no Google Pesquisa (termos pesquisados). **7.** Imagens armazenadas no Google Fotos. **8.** Dados armazenados no Google Drive, incluindo, *backup* do WhatsApp e de outros aplicativos de comunicação que realizem *backup* por intermédio do Google. **9.** Caixa de entrada, enviados, rascunhos e lixeira do Gmail, bem como dados cadastrais, registros de acessos, contendo data, horário, padrão de fuso horário e endereçamento IP. **10.** Histórico de navegação do Google Chrome sincronizado com a conta do Google. **11.** Contatos. **12.** Informações sobre tipo e configurações de navegador, tipo e configurações de dispositivo, sistema operacional, rede móvel, bem como interação de *apps*, navegadores e dispositivos com os serviços do Google. **13.** Informações sobre aplicativos adquiridos e instalados por intermédio da PlayStore. **14.** Sistema de Solicitação de Aplicação da Lei (*Law Enforcement Request System – Lers*) do Google. **15.** Imagens demonstrando o acesso ao *Lers* do Google: **15.1** Modelo de representação de afastamento do sigilo dos dados eletrônicos armazenados pelo Google; **15.2.** Modelo de ofício indicando perfis de usuários e informações de interesse da investigação (ofício a ser encaminhado com base nas primeiras informações apresentadas pelo Google, ou seja, após o Google informar os seus usuários que foram utilizados no celular no período que constou na ordem judicial). **16.** APPLE: **16.1.** Modelo de representação de afastamento do sigilo dos dados eletrônicos armazenados pela Apple. **17.** Procedimentos detalhados para utilização da plataforma LERS: **17.1** Tópico extra – confirmação periódica de conta. **18.** Referências.

---

1. **Higor Vinicius Nogueira Jorge** é Delegado de Polícia, mestrando em Educação pela Universidade Estadual do Mato Grosso do Sul – UEMS, professor concursado da Academia de Polícia na Polícia Civil do Estado de São Paulo, titular da cadeira 30 da Academia de Ciên-

1. INTRODUÇÃO

A evolução tecnológica proporcionou avanços significativos em todas as áreas de conhecimento humano, possibilitando agilidade, melhorias e facilidades indiscutíveis em todos os ramos de atividades praticadas, tanto no setor privado, quanto no setor público.

Em decorrência desta evolução, a sociedade brasileira e internacional, nos últimos vinte anos, vivenciou grandes transformações que culminaram na massificação de registros, em sistemas computacionais e bancos de dados, de eventos dos mais variados tipos.

---

cias, Artes e Letras dos Delegados de Polícia do Estado de São Paulo e membro do conselho de ética da Associação dos Delegados de Polícia do Estado de São Paulo. Também é membro da Associação Internacional de Informática Forense (ASIIF), da Associação Internacional de Investigação de Crimes de Alta Tecnologia (Htcia) e da Associação Internacional da Polícia (Ipa – Brasil), além de professor de inteligência cibernética do Ministério da Justiça e Segurança Pública. Apresentou aulas nas pós-graduações das seguintes instituições de ensino: WB Educacional, MeuCurso, Complexo de Ensino Renato Saraiva (Cers), Escola Brasileira de Direito (Ebradi), Escola Superior de Advocacia da OAB-SP (ESA-OAB/SP – Campinas), Verbo Jurídico, Associação dos Diplomados da Escola Superior de Guerra – Campinas, Damásio Educacional e Escola da Magistratura do Estado do Rio de Janeiro (Emerj). Em 2017, 2018, 2019, 2020, 2021 e 2022 foi escolhido na categoria "Jurídica" entre os melhores Delegados do Brasil pelo Portal Nacional dos Delegados & Revista da Defesa Social. Nos últimos anos escreveu e coordenou dezenas de livros, bem como ministrou cursos e palestras sobre educação digital, investigação de crimes cibernéticos, investigação criminal tecnológica, direito eletrônico, inteligência policial, segurança na internet e outros temas correlatos nos estados de São Paulo, Sergipe, Ceará, Bahia, Paraíba, Alagoas, Belo Horizonte, Amapá, Mato Grosso do Sul, Pará, Tocantins, Santa Catarina, Roraima, Rio Grande do Sul, Minas Gerais e no Distrito Federal. Possui os sites www.higorjorge.com.br e www.crimesciberneticos.net, Instagram @higorjorge, Twitter @higorjorge e Facebook www.facebook.com/professorhigorjorge no Facebook.

2. **Márcio Rogério Porto** é Escrivão de Polícia da Polícia Civil do Estado de São Paulo, atuando no Centro de Inteligência Policial e no Setor de Investigações na Área de Tecnologia da Delegacia Seccional de Polícia de Cruzeiro-SP, pertencente ao Departamento de Polícia Judiciária do Interior 1 (Deinter-1) São José dos Campos-SP.

3. **Hélio Molina Jorge Júnior** é engenheiro de materiais formado pela Universidade Federal de São Carlos – UFSCAR, especializando em direito penal e processo penal pelo MeuCurso, revisor e coautor de obras jurídicas.

4. **Ulisses da Nóbrega Silva** é Graduado em Sistemas de Informação e Administração. Pós-graduado em Análise de Sistemas. Agente Especial da Polícia Civil do Distrito Federal há 16 anos, atualmente lotado na Delegacia de Repressão aos Crimes Cibernéticos da Polícia Civil do Distrito Federal – DRCC/PCDF, onde ocupa o cargo de chefe de investigação. Docente há 05 (cinco) anos na Escola Superior de Polícia Civil, titular da cadeira Investigação em Ambiente Cibernético. Docente em cursos promovidos pela SENASP, MPDFT, ASMEGO, PCDF, Polícia do Senado Federal e Polícia da Câmara dos Deputados.

Indícios que antes somente poderiam ser obtidos através de relatos de testemunhas, como a informação da presença de determinado suspeito nas imediações de um eventual local de crime, na data e hora em que o fato ocorreu, atualmente, pode ser obtida com relativa facilidade em decorrência do advento tecnológico, seja através da triangulação de informações de sistemas relacionados com antenas de telefonia móvel (ERBs), seja por meio de informações de sistemas de geolocalização presentes nos dispositivos móveis atuais, seja por intermédio de imagens de câmeras de segurança.

Desta narrativa, torna-se possível observar que a imensa maioria das atividades realizadas, de alguma maneira, acaba registrada em sistemas computacionais, muitas vezes, por iniciativa dos próprios envolvidos, podendo citar, como exemplos, as comunicações, os deslocamentos, as compras presenciais ou informatizadas, as atividades de consumo de bens e de serviços, os pagamentos, as movimentações financeiras, as atividades de lazer e de viagem, os atendimentos médicos, às atividades estudantis e acadêmicas, as atividades de trabalho, os relacionamentos sociais e amorosos, além de uma série de outras atividades não elencadas.

Estes eventos são sistematicamente registrados, de forma direta ou indireta, em banco de dados de sistemas computacionais e também, muitos deles, em sistemas de monitoramentos por câmeras de seguranças espalhadas em estabelecimentos, residências e vias públicas, somando-se também as informações que independem da vontade do indivíduo, como são os casos dos registros oficiais, decorrentes das emissões de documentos e outras atividades promovidas por órgãos públicos.

Todo este volume de dados e informações apresenta-se como fonte importantíssima de produção de conhecimento, sendo capaz de auxiliar no processo investigativo não somente dos casos ligados com combate dos crimes praticados por meios digitais, como também dos demais delitos previstos no Código Penal e outras Leis Extravagantes de matéria penal, em especial o crime de corrupção.

No que diz respeito ao crime de corrupção, investigações pretéritas apontam que parcela significativa dos casos envolve organizações criminosas, as quais, com o objetivo de desfrutarem dos recursos e valores obtidos de forma ilícita sem serem importunadas pelas autoridades públicas, recorrem ao advento da "lavagem de dinheiro", caracterizada pela tentativa de dar aparência lícita para os bens e valores obtidos em função de suas atividades ilícitas praticadas.

Neste contexto, sem a pretensão de esgotar o tema, o presente trabalho tem por objetivo identificar e demonstrar as fontes fechadas de informação contidas nas nuvens das empresas Google e Apple que apresentam maior impacto positivo na produção de conhecimento destinado ao apoio da atividade investigativa, principalmente no que diz respeito à identificação de autoria, verificação de

relacionamentos e integração de indivíduos e familiares nos delitos praticados, na identificar possíveis coautores ou partícipes, no apontamento de recursos materiais, bem e valores obtidos em função de atividades ilícitas e, em última análise, demonstrar que a atividade também pode favorecer a identificação e mapeamento, de forma mais segura, de integrantes do crime organizado especializado na prática de corrupção.

2. CLASSIFICAÇÃO DAS FONTES DE DADOS

Por intermédio das informações contidas nas descrições de sistemas computacionais, manuais de utilização, conteúdo de divulgação e propaganda; consulta em livros e revistas especializadas; artigos e trabalhos acadêmicos; conteúdo divulgado em apresentações e conferências; e outras fontes de conteúdo, buscou-se analisar o potencial de contribuição das informações disponibilizadas pelas empresas e sua aplicabilidade nas investigações destinadas ao combate à corrupção e suas peculiaridades já apontadas.

Inicialmente, foram classificados os principais conteúdos com o objetivo de identificar as fontes, apresentar suas características e os tipos de dados possíveis. Neste sentido, a metodologia utilizou-se de palavra-chave que indica o TIPO de contribuição de acordo com o CONTEÚDO obtenível através das fontes abordadas, conforme descreve o Quadro 1, a seguir:

Quadro 1 – Tipo de contribuição de acordo com o conteúdo.

TIPO	CONTEÚDO
Qualificação	Nome, apelido, documento, fotografia, endereço, e-mail, nome virtual (*nickname*), redes sociais (perfil social virtual), localização, deslocamentos, características físicas, impressão digital, DNA, número telefônico.
Família	Genitores, irmãos, familiares, cônjuges, grau de parentesco, grau de proximidade.
Relacionamento	Amizade, contatos pessoais, sociedades empresariais, convívio próximo (vizinhança, prédio, condomínio fechado), convívio profissional, ligações telefônicas, mensagens eletrônicas, SMS, comunicações instantâneas.
Coautoria	Participação conjunta em delitos, distribuição de tarefas criminosas, olheiros, coautores, participes, mandantes, financiadores.
Recurso	Dinheiro, imóveis, veículos, equipamentos, armas, jóias, pedras preciosas, obras de arte, outros recursos materiais, ativos financeiros, contas bancárias, ativos virtuais, apólices de seguro, linhas telefônicas, conexão com a internet, aplicativos de mensageria.
Mapeamento	Participação em associação criminosa, membros de quadrilhas ou milícias, integração ao crime organizado.
Técnico	URL, endereço IP, mapas, geolocalização, imagens, metadados, outros dados técnicos da internet, manuais descritivos, dispositivos eletrônicos.

Fonte: Autoria Própria.

3. GOOGLE

O Google armazena uma grande quantidade de informações de seus usuários, mas grande parte deles não possui consciência desse fato e, muitas vezes, os policiais que realizam a investigação criminal não compreendem a dimensão das possibilidades ofertadas pela ferramenta.

No que concerne a investigação dos denominados "crimes do colarinho branco", o investigado pode ter grande quantidade de informações armazenadas no celular ou na nuvem do celular, ou seja, nos aplicativos cujas informações estão armazenadas na internet.

O celular de um criminoso após ser apreendido, mediante ordem judicial, pode ser encaminhado para perícia com o intuito das informações serem extraídas dele, contudo, sobre essa temática falaremos nos tópicos seguintes.

Neste tópico abordaremos algumas informações que podem ser extraídas da nuvem do Google do celular. O mesmo ocorre com relação à Apple e outras empresas que oferecem produtos que armazenam, no ambiente virtual, inúmeras informações.

Considerando esse pressuposto, apresentamos alguns aspectos essenciais sobre esse tipo de recurso, de modo a nortear a polícia judiciária a utilizar as informações armazenadas pelo Google.

Aprioristicamente cabe considerar que o delegado de polícia, durante a tramitação de um inquérito policial, pode representar para que o Poder Judiciário emita uma determinação para que o Google, Apple ou Microsoft promova o fornecimento de informações de interesse da investigação.

Ao se tomar conhecimento de dados vinculados a contas Google, Apple ou Microsoft de determinado investigado, é recomendável que já requisite a preservação dos dados (art. 13, § 2º e art. 15, § 2º da Lei nº 12.965, de 23 de abril de 2014), por intermédio da plataforma ou, caso não exista essa possibilidade, mediante Ofício da Autoridade Policial, o que evitará a perda de provas quando o usuário investigado, que porventura tomar conhecimento da investigação ou não for preso em possível atuação em campo da Polícia Civil ou Federal.

A seguir apresentaremos, no que concerne ao Google, algumas informações que podem ser armazenadas e a aplicação prática das informações na investigação dos crimes supra indicados:

4. DADOS ARMAZENADOS NA "SUA LINHA DE TEMPO" DO GOOGLE MAPS E OUTRAS INFORMAÇÕES DE LOCALIZAÇÃO

As informações armazenadas na "Sua linha de tempo" do *Google Maps* permitem ter acesso à localização aproximada do alvo durante o período de interesse.

São fornecidas as coordenadas geográficas dos locais onde o alvo esteve, junta-mente com outros dados capazes de auxiliar a compreensão dos fatos.

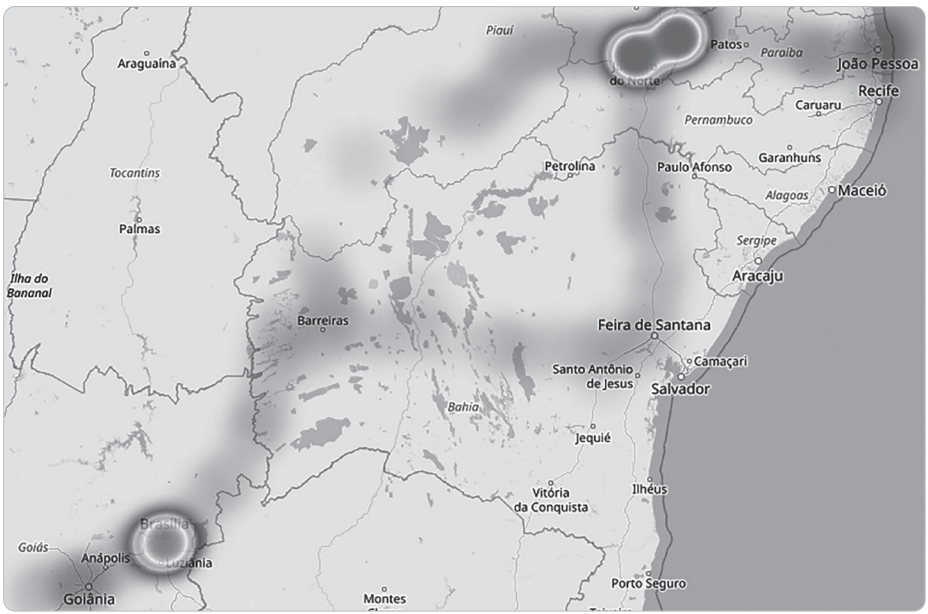
Um exemplo prático: Um administrador municipal esteve no dia 26 de abril de 2023 na empresa da vítima, onde exigiu certa quantia de dinheiro para autorizar a construção de um loteamento na cidade.

As informações ajudaram a robustecer as informações da vítima no sentido de que o administrador municipal realmente esteve no local, conforme indicado pela vítima.

Notoriamente outras informações poderiam tornar ainda melhor o conjunto probatório, sendo recomendável, nestes casos, que a vítima promova a gravação por áudio e vídeo do administrador municipal exigindo dinheiro e, conforme as peculiaridades do caso, realizar o denominado "flagrante esperado" em desfavor do criminoso.

Outro exemplo prático: um investigado viajou da Paraíba para o Distrito Federal e trouxe uma mala de dinheiro para pagar uma "propina" a determinado empresário, fruto de fraude a uma licitação. Quando de sua oitiva, o investigado, morador da Paraíba, declarou jamais ter pisado no Distrito Federal.

Com um dos arquivos fornecidos pela Google, que contém o histórico de localizações do suspeito, no formato emaildoinvestigado@gmail.com.locationhistory.json e ao usar a ferramenta disponível em https://locationhistoryvisualizer.com/heatmap é possível verificar que as declarações prestadas na polícia foram falsas, pois as áreas quentes (coloridas) no mapa, sugerem que ele esteve no Distrito Federal:



Outra possibilidade ocorre nas hipóteses em que o Google oferece uma planilha do Excel com informações sobre data, horário e geolocalização do alvo, sendo que a planilha pode ser editada para ser inserida como uma camada no Google Maps e, deste modo, oferecer cada localização do investigado no período informado pela empresa.

5. HISTÓRICO DE EXIBIÇÃO, HISTÓRICO DE PESQUISAS, CURTIDAS E COMENTÁRIOS DO YOUTUBE

Saber o tipo de vídeo que o investigado assiste, por intermédio do Youtube, pode também colaborar com uma investigação, bem como compreender o tipo de vídeos que o alvo tem reproduzido no seu dispositivo e conhecer melhor o perfil do alvo.

O Google pode informar o histórico de exibição (vídeos que o alvo assistiu), histórico de pesquisas (termos pesquisados pelo investigado), curtidas e comentários nos vídeos disponibilizados pelo Youtube.

6. HISTÓRICO DE PESQUISAS NO GOOGLE PESQUISA (TERMOS PESQUISADOS)

É relevante ter acesso aos termos pesquisados no Google pelo investigado, sendo mais uma ferramenta que pode auxiliar na investigação criminal, considerando que atualmente é muito comum a pessoa realizar pesquisas no referido buscador, sobre qualquer assunto de interesse, sem imaginar que referidos dados podem colaborar com a apuração de eventuais atos criminosos.

Um exemplo pitoresco foi de um administrador de uma fundação, investigado por enriquecimento ilícito que, poucas semanas antes da deflagração de uma atuação em campo da Polícia Civil que promoveu a prisão de várias pessoas pesquisou os seguintes termos: "como lavar dinheiro", "a polícia intercepta ligação de WhatsApp?", "como saber se a polícia grampeou meu celular" e "como esconder dinheiro da polícia". Durante referida investigação, a análise das pesquisas realizadas no Google permitiu constatar que havia realizado um vultoso investimento em criptoativos. Posteriormente, foi realizada atuação em campo dos policiais que permitiram o cumprimento de mandado de busca e apreensão em sua residência e, durante sua oitiva, ao ser confrontado com as pesquisas que realizou, optou por confessar a autoria delitiva.

Um outro exemplo ocorreu em uma cidade do interior do estado de São Paulo, onde o investigado realizou várias pesquisas, com a própria voz, no Google Pesquisa (a plataforma permite pesquisas por voz), comprovando sua participação nos crimes em investigação, sem saber que as gravações com sua voz ficaram armazenadas pelo Google e foram capazes de subsidiar seu formal indiciamento e posteriormente sua condenação.

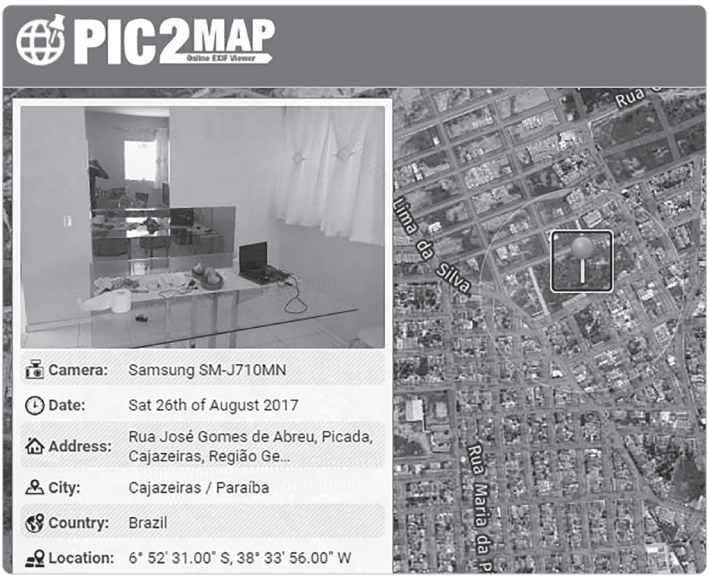
7. IMAGENS ARMAZENADAS NO GOOGLE FOTOS

Muitas vezes o celular é configurado para que as fotos armazenadas sejam enviadas para o Google Fotos, sendo que, durante a investigação e o afastamento do sigilo da nuvem do Google, os policiais recebem acesso as imagens que podem comprovar eventuais práticas ilícitas pelo investigado.

Há alguns anos, durante uma investigação, foi observada uma imagem de uma mala de viagens com grande quantidade de dinheiro. A imagem foi analisada e, de acordo com os metadados da imagem, foi possível ter acesso a localização aproximada do local onde a foto foi obtida, sendo que se tratava de uma propriedade rural utilizada por ele. O delegado de polícia representou pelo cumprimento de mandado de busca e apreensão no local e foi possível promover a apreensão da mala e do dinheiro de origem ilícita que estava em seu interior.

Sempre que existem imagens a serem analisadas cabe realizar pesquisas em fontes abertas, inclusive, uma medida sugerida é sempre analisar os metadados das imagens.

Um dos sites recomendados para rapidamente se descobrir o local em que uma fotografia foi tirada é o https://www.pic2map.com.



Já se o objetivo é visualizar todos os locais visitados, recomenda-se o uso da ferramenta gratuita Avilla Forensics 3.5, elaborada pelo policial civil Daniel Avilla, disponível no endereço https://github.com/AvillaDaniel/AvillaForensics/. A ferramenta possui inúmeras utilidades e tem sido muito utilizada no Brasil e em outros países.

8. DADOS ARMAZENADOS NO GOOGLE DRIVE, INCLUINDO, *BACKUP* DO WHATSAPP[5] E DE OUTROS APLICATIVOS DE COMUNICAÇÃO QUE REALIZEM *BACKUP* POR INTERMÉDIO DO GOOGLE

Os dados armazenados no Google Drive são muito importantes e, em alguns casos, são capazes de fazer a diferença entre elucidar ou não elucidar determinado delito.

Dentre os inúmeros dados armazenados no Google Drive, o backup do WhatsApp permite obter elementos muito relevantes durante uma investigação.

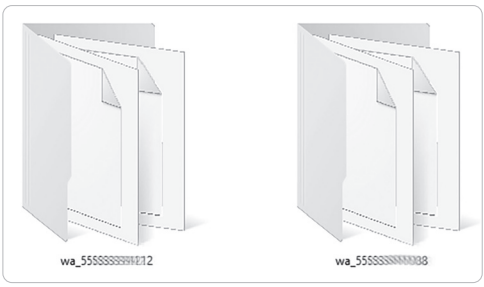
Importante considerar que as conversas do alvo são criptografadas e não são aproveitadas, contudo, os áudios, fotos e vídeos podem ser reproduzidos e analisados pelos policiais.

Existem inúmeros exemplos, que demonstram a relevância dos dados, como no caso de uma investigação onde foi possível ter acesso aos áudios armazenados no WhatsApp do investigado, sendo que eles apresentavam diversas tratativas com o objetivo de fraudar um concurso público no âmbito municipal.

Em outra investigação, em razão de uma pessoa ter matado outra, realizou-se o afastamento de sigilo do perfil do investigado e tiveram acesso a um vídeo gravado pelo investigado, logo após atingir a vítima com inúmeros disparos de arma de fogo, depois que realizaram o denominado "tribunal do crime" vinculado a uma organização criminosa.

Os arquivos disponibilizados do backup WhatsApp, contidos na nuvem da Google, tem nome similar à emaildoinvestigado.9999999.DriveMobileBackups.Backup_001.

Após a descompressão do arquivo, serão visíveis as pastas com os números de telefones vinculados ao WhatsApp do investigado, quantos forem os terminais telefônicos que foram armazenados em backups na nuvem Google, tais como as duas pastas de backup, como mostradas a seguir:



5. Importante salientar que o *backup* das conversas é criptografado, mas o *backup* dos áudios, fotos e vídeos não. Recomendável informar o Poder Judiciário caso tal fato ocorrer.

Já com relação à estrutura de arquivos WhatsApp, a próxima imagem demonstra os principais arquivos armazenados, os quais são explicados na sequência:

Nome	Data	Tipo
Backups_chatsettingsbackup.db.crypt1	18/09/2019 00:09	Arquivo CRYPT1
Backups_statusranking.db.crypt1	18/09/2019 00:09	Arquivo CRYPT1
Backups_stickers.db.crypt1	18/09/2019 00:09	Arquivo CRYPT1
Databases_msgstore.db.crypt12	18/09/2019 00:09	Arquivo CRYPT12
Media_.Statuses_0a5733dd196e48ae8ae8f31d022093bd.jpg	18/09/2019 00:13	Arquivo JPG
Media_.Statuses_1bb8df8e03a94d2ca9fc7fd2455c5675.jpg	18/09/2019 00:13	Arquivo JPG
Media_.Statuses_1bc140c478644c02a04dd4cc7070b26a.mp4	17/09/2019 16:12	MP4 Video File (VLC)
Media_WhatsApp Animated Gifs_Private_VID-20190914-WA0010.mp4	17/09/2019 01:51	MP4 Video File (VLC)
Media_WhatsApp Animated Gifs_Sent_VID-20190516-WA0112.mp4	21/05/2019 23:58	MP4 Video File (VLC)
Media_WhatsApp Audio_Private_AUD-20190423-WA0120.opus	23/04/2019 23:47	OPUS Audio File (VLC)
Media_WhatsApp Documents_Private_boleto_0eed543636be51ce5af...	27/03/2019 01:36	Adobe Acrobat Document
Media_WhatsApp Documents_Sent_DOC-20190104-WA0042.pdf	08/01/2019 23:53	Adobe Acrobat Document
Media_WhatsApp Images_IMG-20181226-WA0032.jpeg	26/12/2018 14:41	Arquivo JPEG
Media_WhatsApp Images_Private_IMG-20181226-WA0040.jpg	01/01/2019 23:41	Arquivo JPG
Media_WhatsApp Images_Sent_IMG-20181226-WA0007.jpg	01/01/2019 23:41	Arquivo JPG
Media_WhatsApp Images_Sent_IMG-20181227-WA0001.jpg	01/01/2019 23:41	Arquivo JPG
Media_WhatsApp Stickers_STK-20190917-WA0141.webp	18/09/2019 00:15	Chrome HTML Document
Media_WhatsApp Voice Notes_201903_PTT-20190118-WA0137.opus	22/01/2019 23:51	OPUS Audio File (VLC)

Partes do nome dos arquivos possuem a data invertida (**AAAAMMDD**) em sua composição, o que facilita quando da busca por um crime de corrupção que se sabe ter ocorrido em um determinado dia.

Podem existir fragmentos de nome **Sent**, quando a mídia foi enviada pelo proprietário do backup e **Private**[6], quando existem arquivos invisíveis.

Mais ainda:

1. Arquivos iniciados com **Backups** e **Databases** são os arquivos do backup do chat, que são criptografados e não passíveis de serem usados na investigação;
2. Arquivos **Media_Statuses** são àqueles disponibilizados no status do perfil WhatsApp e visualizados por até 24 horas, podendo ser imagem ou vídeos;

6. Normalmente em uma conversa individual ou em um grupo, todas as imagens que a pessoa envia para alguém ou são recebidas de um grupo serão exibidas na galeria de mídia. No entanto, as versões mais recentes do Whatsapp permitem tornar a mídia privada (foto, áudio, vídeo ou mesmo documento) quando recebida de um bate-papo específico ou de um grupo por meio de uma opção chamada "Visibilidade da mídia". Desta forma, se a opção "Visibilidade da mídia" estiver definida como "Não", o arquivo será gravado com o termo Private. Estes arquivos podem ser bastante importantes, dependendo do alvo investigado.

3. Arquivos **Media_WhatsApp** que são enviados anexados aos chats de texto e são muito úteis à investigação:
   - **a.** **Animated** Gifs são os gifs animados;
   - **b.** **Audio** são os arquivos de áudio em geral;
   - **c.** **Documents** são os documentos, normalmente em PDF ou TXT;
   - **d.** **Image** são os arquivos de imagem em geral;
   - **e.** **Stickers** são os adesivos;
   - **f.** **Voice Notes PTT**[7] são, talvez, os arquivos mais importantes, pois podem funcionar como uma verdadeira escuta telefônica, haja vista que os criminosos já não falam ao telefone, mas por aplicativos de comunicação.

9. CAIXA DE ENTRADA, ENVIADOS, RASCUNHOS E LIXEIRA DO GMAIL, BEM COMO DADOS CADASTRAIS, REGISTROS DE ACESSOS, CONTENDO DATA, HORÁRIO, PADRÃO DE FUSO HORÁRIO E ENDEREÇAMENTO IP[8]

Os e-mails do Gmail do alvo podem colaborar com a investigação tendo em vista que muitos criminosos realizam tratativas por intermédio do serviço de mensagens e outros enviam cópias das conversas sensíveis para e-mail. É possível também obter os registros de acesso contendo IP, data, horário, padrão de fuso horário e endereçamento IP, que podem colaborar com a identificação ou até mesmo localização da pessoa que esteja utilizando indevidamente o e-mail.

---

7. PTT: Push to Talk – Pressione para Falar. São os arquivos de áudio do WhatsApp que o interlocutor seguro o botão do microfone enquanto fala.

8. Um tema polêmico reside no fornecimento da porta de origem, também denominada no meio investigativo de "porta lógica". O Google fornece os endereçamentos IPs, mas não as portas de origem. O problema é que alguns provedores de internet informam que os IPs que constam nos logs (registros de acesso contendo data, horário, padrão de fuso horário e IPs) fornecidos pela Autoridade Policial foram fornecidos para diversos clientes e, por isso, o Delegado de Polícia deveria fornecer a porta de origem relacionada com cada log. Grande parte das empresas provedoras de conteúdo se recusam a informar a porta de origem (exemplos: Google, Facebook, Instagram etc.), mesmo diante de ordem judicial determinando que apresente referida informação. Caso a porta de origem não for informada é recomendável oficiar a empresa provedora de conexão, para que informe cada um dos clientes que utilizaram os IPs, conforme os logs que foram apresentados pela empresa provedora de conteúdo, em seguida, será necessário analisar os dados para identificar os clientes que utilizaram os IPs em todos os acessos que constam nos logs do provedor de conteúdo. É possível utilizar planilha do Excel para facilitar a análise e identificação, especialmente daquele(s) usuário(s) que aparece(m) com maior frequência.

Os arquivos são recebidos no formato MBOX e devem ser importados para o Mozilla Thunderbird (conforme recomendação da própria Google) e tratados na busca das mensagens importantes para o conteúdo probatório.

No Distrito Federal, a prática das investigações realizadas pela Polícia Judiciária chegou à conclusão que algumas mensagens do total recebido devem ser priorizadas quando da busca por indícios de crime:

1. O autor e o remetente são, ao mesmo tempo, o investigado. A justificativa se deve ao fato que as pessoas costumam enviar mensagens para elas mesmas quando aquele conteúdo é relevante e não pode ser perdido;
2. Com anexos. A quantidade de mensagens que possuem arquivos anexados é menor que o restante. Na maioria das vezes, corresponde a até 10% do total analisado. Por outro lado, nestas mensagens é possível verificar cópias de notas fiscais, procurações de cessão de direito, cártulas de cheques e outros documentos úteis ao caso; e
3. Palavra senha no corpo do texto: Muitos usuários, por não conseguirem se lembrar de todas as credenciais de acesso que possuem, costumam se utilizar deste recurso para armazenar o *login* e a senha de determinados sites. Apesar de o acesso em *cloud computing* não estar abrangido em muitos dos casos, a Autoridade Policial, ao tomar conhecimento destas credencias, pode representar pela Quebra do Sigilo desta informação no Poder Judiciário.

10. HISTÓRICO DE NAVEGAÇÃO DO GOOGLE CHROME SINCRONIZADO COM A CONTA DO GOOGLE

O usuário do navegador Google Chrome pode sincronizar o navegador com sua conta do Google e as informações podem ficar armazenadas na conta do referido serviço que, mediante ordem judicial decorrente de representação de delegado de polícia, podem ser fornecidas, de modo que seja possível compreender melhor como realiza a navegação na internet.

11. CONTATOS

Os contatos do alvo, armazenados pelo Google, são fornecidos e podem auxiliar que os policiais tenham acesso aos reais telefones do alvo ou para que saibam os telefones de outras pessoas ligadas ao perfil.

Com os novos números telefônicos vinculados à lista de contatos, é possível fazer a preservação dos dados e/ou solicitar dados cadastrais de perfis vincula-

dos ao Facebook, Instagram, WhatsApp, Mercado Livre, OLX, Pagseguro, MercadoPago, dentre outras plataformas, todas usadas para a troca de mensagens e lavagem de dinheiro.

12. INFORMAÇÕES SOBRE TIPO E CONFIGURAÇÕES DE NAVEGADOR, TIPO E CONFIGURAÇÕES DE DISPOSITIVO, SISTEMA OPERACIONAL, REDE MÓVEL, BEM COMO INTERAÇÃO DE *APPS*, NAVEGADORES E DISPOSITIVOS COM OS SERVIÇOS DO GOOGLE

O Google possui condições de informar tipo e configurações de navegador, tipo e configurações de dispositivo, sistema operacional, rede móvel, bem como interação de apps, navegadores e dispositivos com os serviços do Google.

Por exemplo, foi realizado o afastamento de sigilo da nuvem do alvo e foram identificadas fotos que demonstraram que ele teria sido o autor do crime. Posteriormente o celular foi apreendido e constatou-se que as informações, fornecidas pelo Google, sobre o equipamento são as mesmas pertencentes ao equipamento apreendido em poder do alvo. Em muitos casos o criminoso muda frequentemente o chip e o aparelho e as informações supracitadas podem colaborar com a investigação.

Nos casos de crimes contra o patrimônio, estas informações também podem auxiliar na identificação de dispositivos subtraídos, ao passo que nos crimes de corrupção e de lavagem de dinheiro, tem potencial de identificar aquisição de equipamentos e dispositivos de valores elevados e incompatíveis com a renda declarada do investigado.

13. INFORMAÇÕES SOBRE APLICATIVOS ADQUIRIDOS E INSTALADOS POR INTERMÉDIO DA PLAYSTORE

Os aplicativos instalados no dispositivo do investigado permitem iniciar um novo flanco de investigação, com fulcro no afastamento de sigilo de cada um dos aplicativos utilizados pelo alvo.

Um exemplo que demonstra como as informações sobre os aplicativos adquiridos podem ser utilizadas de forma eficaz em uma investigação: um tesoureiro de uma prefeitura era investigado em razão das informações no sentido de que estaria recebendo dinheiro de fornecedores da prefeitura, de acordo com as informações, receberia o equivalente a 10% das principais aquisições de produtos de limpeza adquiridos pelo órgão. Durante a investigação foi realizado o afastamento do sigilo do Google do investigado e constataram que ele tinha

três aplicativos de instituições bancárias instalados no seu celular. Em razão dos fatos as instituições bancárias foram oficiadas e informaram as contas utilizadas pelo investigado vinculadas aos aplicativos instalados em seu dispositivo, que estavam em nome de outras pessoas, mas eram utilizadas pelo investigado para promover lavagem de dinheiro.

Nesta linha, outro exemplo são os aplicativos destinados à aquisição de produtos e serviços, como APPs de hospedagem, de transportes e viagens, de compras on-line, de administração de moedas virtuais, entre outros.

Caso o alvo utilize os serviços do Google para fazer e receber chamadas ou enviar e receber mensagens, a empresa deve apresentar as informações que possuir, além das informações de voz e áudio caso o alvo utilizar recursos de áudio e pessoas com quem o alvo se comunicou e/ou compartilhou conteúdo.

Referidos dados podem conter informações relevantes dependendo das peculiaridades da investigação.

O *Google LERS* não faz pesquisas com nomes, dados, CPFs, ou dados dos documentos do investigado.

Abaixo são apresentadas as informações que podem utilizadas para realizar pesquisas via Google:

Conta do Google (*Google Account*)

IMEI ou MEID

Número CSSN

Número de série com fabricante e modelo

ID do Android

Importante considerar que, em razão da grande quantidade de informações armazenadas no Google, inicialmente, a título de resposta, o Google apresentará as contas dos clientes que utilizaram seus serviços no período de interesse (geralmente são apresentados os e-mails dos clientes, para que a autoridade informe quais contas possui interesse e os serviços que pretende obter as informações) e um ofício informando sobre os produtos (serviços) oferecidos pelo Google que os referidos usuários utilizam. Será necessário fazer o *download* das informações e, após analisar o que é interessante para a investigação, encaminhar um ofício direto para o Google, indicando os usuários do Google (contas dos clientes – e-mails), os produtos e o período de interesse para que seja fornecido novo link na plataforma do Google, com todas as informações produzidas sobre os alvos. Dentre os modelos apresentados nestas Orientações, consta modelo desse tipo de ofício.

Recomendamos que a representação e, por consequência, ordem judicial tenham o seguinte endereçamento:

> **Google LLC 1600 Amphitheatre Parkway, Mountain View, CA 94043 (Google Brasil Internet Ltda – Avenida Brigadeiro Faria Lima, 3477, 18º andar, CEP 04538-133, São Paulo, SP)**

O endereçamento correto é fundamental para que o Google cumpra a solicitação.

14. SISTEMA DE SOLICITAÇÃO DE APLICAÇÃO DA LEI (*LAW ENFORCEMENT REQUEST SYSTEM – LERS*) DO GOOGLE

O Google possui a plataforma *LERS* que permite acesso ao seu sistema de auxílio da persecução penal. Em poder da ordem judicial ou da requisição do delegado de polícia, a plataforma *LERS* do Google é utilizada para enviar referidos documentos para a empresa e para receber as respostas e os conhecimentos produzidos em virtude da solicitação.

Para isso o policial deve acessar o endereço **lers.google.com**, clicar em "Criar Conta", inserir o seu e-mail institucional e enviar. Imediatamente receberá um link que permitirá o cadastramento de suas informações (nome completo e cargo das autoridades que precisam de contas, endereço de e-mail institucional individual, números de telefone fixos, nome e endereço físico da agência/delegacia/vara). Depois de alguns dias receberá um nome de usuário permanente (*permanent username*) e uma senha temporária *(temporary password*), que será alterada no primeiro acesso. A plataforma será acessada no endereço **lers.google.com**, sendo necessário apenas que realize a digitalização da solicitação (ordem judicial, requisição etc.) para o envio pela referida plataforma nos formatos **.pdf**, **.doc** ou **.tif**. Informo que a resposta do Google também será oferecida por intermédio da plataforma para que seja realizado o *download*.

Este trabalho reserva, no tópico final, apresentação detalhada dos principais procedimentos, passo a passo, para obtenção de acesso junto à plataforma *LERS*.

15. IMAGENS DEMONSTRANDO O ACESSO AO *LERS* DO GOOGLE

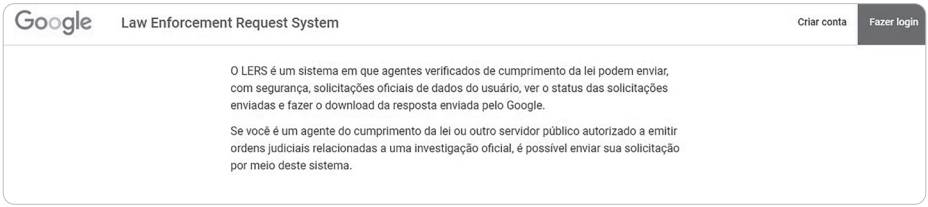


Figura 1 – Página inicial do LERS do Google que permite acesso a plataforma

A página inicial do LERS do Google permite o acesso à plataforma para os usuários que já possuam login (nome de usuário) e senha.

Quanto aos usuários que ainda não possuem uma conta na plataforma é necessário acesso o link "Criar conta" e inserir o e-mail institucional pessoal.

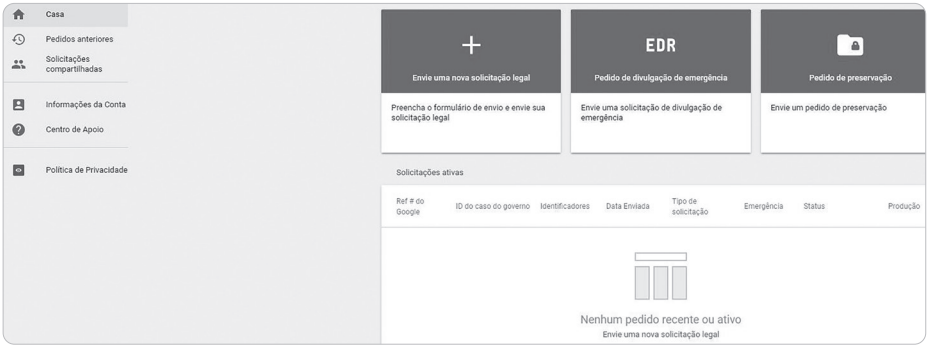


Figura 2 – Página inicial do LERS do Google apresentada após a inserção do nome de usuário e senha

Caso o usuário acesse a aba para envio da solicitação, será necessário preencher um formulário com as informações da investigação, incluindo, tipo de solicitação (pedido de preservação, pedido de polícia, solicitação de procurador, ordem judicial e solicitação de divulgação de emergência), estatuto legal (inserir a legislação que respalda a solicitação), informar se a solicitação trata de alguma emergência em curso, natureza da investigação (exploração infantil, substâncias controladas, fraude, terrorismo, crime violento etc.), número dos autos (inquérito policial, termo circunstanciado, processo judicial etc.), data da assinatura da solicitação legal, identificador(es) da conta do(s) alvo(s), intervalo de datas, anexar solicitação legal direcionada ao **Google LLC 1600 Amphitheatre Parkway, Mountain View, CA 94043 (Google Brasil Internet Ltda – Avenida Brigadeiro Faria Lima, 3477, 18º andar, CEP 04538-133, São Paulo, SP)** e, depois que clicar em enviar, será apresentada uma tela para conferir alguns dados da solicitação.

Importante considerar que a resposta será oferecida por intermédio de um link onde será realizado o download dos arquivos produzidos pelo Google, conforme indicado na imagem supra.

Figura 3 – Resposta do Google para download

Figura 4 – Resposta do Google ampliada

Na página inicial do LERS o usuário também poderá clicar na aba para enviar pedido de divulgação de emergência (EDR) ou no pedido de preservação.

15.1 Modelo de representação de afastamento do sigilo dos dados eletrônicos armazenados pelo Google[9]

EXCELENTÍSSIMO SENHOR DOUTOR JUIZ DE DIREITO DA COMARCA DE [...] – SP

A **POLÍCIA CIVIL DO ESTADO DE SÃO PAULO**, representada neste ato pelo Delegado de Polícia subscritor, que no uso de suas atribuições legais e regulamentares conferidas pelo artigo 144, § 4º, da Constituição Federal, artigo 140, da Constituição Estadual Paulista, artigo 4º e seguintes do Código de Processo Penal Brasileiro, Portaria DGP-18/1998, sob as premissas da Lei 12.830/13 e

9. Adaptação do modelo extraído da obra: Investigação Criminal Tecnológica – volumes I e II – Higor Vinicius Nogueira Jorge – Editora Brasport – 2018.

demais dispositivos legais correlatos representa pelo **AFASTAMENTO DO SIGILO DOS DADOS ELETRÔNICOS ARMAZENADOS PELO GOOGLE** do investigado [inserir qualificação do investigado e um relatório sintético sobre os fatos apurados pela polícia judiciária até o presente momento].

Dessa forma, como medida de investigação criminal tecnológica, visando a absoluta elucidação do delito, robustecendo o conjunto probatório sobre a prática de crimes pelo investigado, levando em consideração que as evidências armaze-nadas no ambiente eletrônico representam um grande desafio para a persecução penal, em razão da volatilidade e complexidade para sua obtenção, existindo, inclusive, a possibilidade de identificação de outras pessoas envolvidas com os fatos e inexistindo outras medidas para esse fim, solicito que Vossa Excelência, após vista do membro do Ministério Público, requisite a medida infra apresen-tada e estipule multa diária caso demore mais 48 horas para oferecer a informa-ção pretendida:

Perante a empresa **Google LLC 1600 Amphitheatre Parkway, Mountain View, CA 94043 (Google Brasil Internet Ltda – Avenida Brigadeiro Faria Lima, 3477, 18º andar, CEP 04538-133, São Paulo, SP)**, tendo como alvo o telefone do investigado [...], que utiliza [inserir conta do Google, IMEI, número CSSN, número de série com modelo e marca ou Android ID] para, considerando o período compreendido entre [inserir o período de interesse], fornecer, de forma sigilosa, no prazo de 48 horas:

Dados armazenados na "Sua linha de tempo" do *Google Maps* e outras informa-ções de localização;

Histórico de exibição, histórico de pesquisas, curtidas e comentários do *Youtube*;

Histórico de pesquisas no Google Pesquisa (termos pesquisados);

Imagens armazenadas no Google Fotos;

Dados armazenados no Google Drive, incluindo, *backup* do *WhatsApp*[10] e de outros aplicativos de comunicação que realizem *backup* por intermédio do Google;

Caixa de entrada, enviados, rascunhos e lixeira do Gmail, bem como dados cadastrais, registros de acessos, contendo data, horário, padrão de fuso horário, endereçamento IP e porta lógica[11];

10. Importante salientar que o *backup* das conversas é criptografado, mas o *backup* dos áudios, fotos e vídeos não.

11. Grande parte das empresas se recusam a informar a porta lógica, mesmo diante de ordem judicial determinando que apresente referida informação. Caso a empresa não informe, seus

Histórico de navegação do *Google Chrome* sincronizado com a conta do Google;

Contatos;

Informações sobre tipo e configurações de navegador, tipo e configurações de dispositivo, sistema operacional, rede móvel, bem como interação de *apps*, navegadores e dispositivos com os serviços do Google;

Informações sobre aplicativos adquiridos e instalados por intermédio da *PlayStore*;

Caso o alvo utilize os serviços do Google para fazer e receber chamadas ou enviar e receber mensagens, a empresa deve apresentar as informações que possuir;

Informações de voz e áudio caso o alvo utilizar recursos de áudio;

Pessoas com quem o alvo se comunicou e/ou compartilhou conteúdo;

Cabe esclarecer que eventual ordem judicial ou qualquer outra determinação oriunda de autoridade pública deve ser enviada pelo **Sistema de Solicitação de Aplicação da Lei (*Law Enforcement Request System – LERS*) do Google**. Para acessar a ferramenta é necessário criar uma conta no endereço **lers.google.com**, sendo necessário apenas que realize a digitalização da solicitação (ordem judicial, requisição do delegado etc.) para o envio pela referida plataforma nos formatos **.pdf**, **.doc** ou **.tif**. Informo que a resposta do Google também será oferecida por intermédio da plataforma para que seja realizado o *download*.

[cidade], [dia] de [mês] de [ano].

[...]

Delegado de Polícia

responsáveis podem responder pelo crime de desobediência e é possível representar para que o Poder Judiciário arbitre multa diária até que a informação seja oferecida.

15.2. Modelo de ofício indicando perfis de usuários e informações de interesse da investigação (ofício a ser encaminhado com base nas primeiras informações apresentadas pelo Google, ou seja, após o Google informar os seus usuários que foram utilizados no celular no período que constou na ordem judicial)

Ilustríssimo Representante do Google

Com relação aos autos n. 1500834-91.2019.8.26.0541 (Google Ref. 2634441), informo que temos interesse nas contas vinculadas aos seguintes e-mails:

xxxxxxxxxxxxx@gmail.com

xxxxxxxxxxx@gmail.com

Apresentamos abaixo as informações dos referidos perfis que necessitamos obtê-las, considerando o período entre 1 de janeiro de 2018 e 22 de julho de 2019:

- aplicativos baixados no Google Play,
- atividades de voz e áudio,
- conteúdo de Drive,
- conteúdo de Gmail,
- conteúdo de Google Photos,
- dados cadastrais,
- registros de conexão (IPs),
- histórico de localização,
- histórico de navegação,
- histórico de pesquisa (incluindo pesquisa no Google Mapas),
- informações de Android (IMEI/MEID),
- informações de YouTube,
- backup do WhatsApp e Telegram,
- lista de contatos.

Aguardo o envio das informações com certa celeridade em razão de [...].

Aproveitamos o ensejo para renovar meus protestos de estima e consideração.

16. APPLE

Caso o tratar-se de um Iphone, ou seja, de um dispositivo pertencente à Apple, é recomendável solicitar as informações como no modelo abaixo e, após

o deferimento da representação, encaminhar a ordem judicial para o e-mail: lawenforcement@apple.com.

Os procedimentos são muito semelhantes, mas a Apple não possui uma plataforma para o Sistema de Solicitação de Aplicação da Lei e, por isso, a única forma de envio, além do envio físico da documentação, que não recomendável pelo subscritor, é o envio por intermédio de e-mail.

A resposta será fornecida por intermédio de dois e-mails oriundos da Apple, sendo que um apresentará os dados e informações produzidos criptografados e outro apresentará a senha que permitirá fazer o *download* do conteúdo e permitirá retirar a criptografia do conteúdo por intermédio de software indicado pela empresa.

16.1. Modelo de representação de afastamento do sigilo dos dados eletrônicos armazenados pela Apple[12]

EXCELENTÍSSIMO SENHOR DOUTOR JUIZ DE DIREITO DA COMARCA DE [...] – SP

A **POLÍCIA CIVIL DO ESTADO DE SÃO PAULO**, representada neste ato pelo Delegado de Polícia subscritor, que no uso de suas atribuições legais e regulamentares conferidas pelo artigo 144, § 4º, da Constituição Federal, artigo 140, da Constituição Estadual Paulista, artigo 4º e seguintes do Código de Processo Penal Brasileiro, Portaria DGP-18/1998, sob as premissas da Lei 12.830/13 e demais dispositivos legais correlatos representa pelo **AFASTAMENTO DO SIGILO DOS DADOS ELETRÔNICOS ARMAZENADOS PELA APPLE** do investigado [inserir qualificação do investigado e um relatório sintético sobre os fatos apurados pela polícia judiciária até o presente momento].

Dessa forma, como medida de investigação criminal tecnológica, visando a absoluta elucidação do delito, robustecendo o conjunto probatório sobre a prática de crimes pelo investigado, levando em consideração que as evidências armazenadas no ambiente eletrônico representam um grande desafio para a persecução penal, em razão da volatilidade e complexidade para sua obtenção, existindo, inclusive, a possibilidade de identificação de outras pessoas envolvidas com os fatos e inexistindo outras medidas para esse fim, solicito que Vossa Excelência, após vista do ínclito membro do Ministério Público, requisite a medida infra apresentada e estipule multa diária caso demore mais de 48 horas para oferecer a informação pretendida:

12. Adaptação do modelo extraído da obra: Investigação Criminal Tecnológica – volumes I e II – Higor Vinicius Nogueira Jorge – Editora Brasport – 2018.

Perante a empresa **Apple (endereço: Rua Leopoldo Couto de Magalhães Junior, 700, Itaim Bibi, CEP 01454-901, São Paulo, SP, e-mail para envio de ordem judicial: lawenforcement@apple.com)**, para que, tendo como alvo o telefone do investigado [...], que utiliza [inserir conta do iCloud, Apple Device Serial, IMEI ou endereço de e-mail] para, considerando o período compreendido entre [inserir o período de interesse], fornecer, de forma sigilosa, no prazo de 48 horas:

Basic Subscriber Information;

Connection Logs with IP Addresses;

My Photo Stream;

iCloud Photo Library;

Photos and Videos in the Camera Roll;

iCloud Drive, Contacts, Calendars;

Bookmarks;

Safari Browsing History;

Maps Search History;

Messages;

iOS Device Backups;

Device settings;

App data;

iMessage;

Business Chat;

SMS, and MMS messages;

Voicemail

Cabe esclarecer que eventual ordem judicial ou qualquer outra determinação oriunda de autoridade pública deve ser enviada para o e-mail: lawenforcement@apple.com. Informo que a resposta da Apple também será oferecida por e-mail, em um link que será enviado pela empresa para que seja realizado o *download*. A Apple enviará outro e-mail contendo a senha para realizar o *download* do conteúdo produzido e retirar a criptografia por um programa indicado pela empresa.

[cidade], [dia] de [mês] de [ano].

[...]

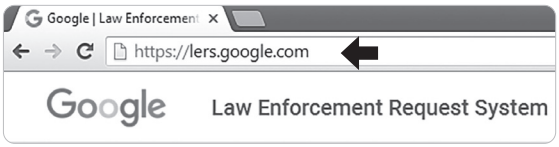
Delegado de Polícia

17. PROCEDIMENTOS DETALHADOS PARA UTILIZAÇÃO DA PLATAFORMA LERS

Conforme já antecipado nos tópicos anteriores, visando facilitar a comunicação das autoridades públicas, bem como, prover meios de envio de ordens judiciais relacionadas com investigações criminais, a empresa Google mantém sistema computacional web, denominado plataforma LERS (Law Enforcement Request System).

Além do envio das autorizações judiciais de acesso aos dados e informações dos usuários armazenadas nos servidores da empresa, a plataforma destina-se ainda à verificação do status dos pedidos e do recebimento das respostas da empresa com os eventuais conteúdos solicitados para download.

Para utilização da plataforma, torna-se necessária a realização de registro o qual é descrito de maneira detalhada, a seguir:



1) **Acessar** a URL: **https://lers.google.com**

2) **Clicar** no botão: **"Criar conta"**