Aspectos teóricos e práticos do afastamento de sigilo e interceptação das comunicações telemáticas no âmbito de investigações de Organizações Criminosas

Rodrigo Vasconcelos da Cruz Sousa
Inspetor de Polícia Civil do Estado do Rio de Janeiro
Bacharel em Direito pela Universidade Veiga de Almeida (UVA)

Desirre da Cunha Rocha
Oficial de Cartório da Polícia Civil do Estado do Rio de Janeiro
Graduada em Serviço Social pela Universidade Federal do Rio de Janeiro (UFRJ)

Resumo

O presente estudo tem por escopo analisar os aspectos legais, teóricos e práticos dos institutos do afastamento de sigilo e interceptação em sistemas de telemática e demonstrar a importância dessas técnicas especializadas, notadamente a sua aplicabilidade em investigações de Organizações Criminosas (ORCRIMs), seja para a produção de provas, comprovação de vínculos entre seus membros e posterior desarticulação. Dada a relevância da evolução dos meios de comunicação que invariavelmente estão presentes na vida das pessoas, e, portanto, dos alvos de investigações de ORCRIMs, este artigo se baseará na modernização das ferramentas para análise de redes sociais, aplicativos em geral e tecnologia *cloud computing*, que auxiliam as forças policiais na busca por autoria e materialidade durante o inquérito policial, para, ao final, apresentar ferramentas atuais de combate ao crime organizado e seu efeito prático nas investigações.

Palavras-chave
dados telemáticos, quebra de sigilo, telemática, investigação.

Introdução

A demanda global por segurança da informação e privacidade gera crescente busca das empresas de comunicação por desenvolvimento de *softwares* que possam ser utilizados em aplicativos de mensagens e redes sociais, apostando cada vez mais em tecnologias de criptografias que garantam a inviolabilidade dos dados dos usuários. Entre esses dados, estão presentes as informações provenientes de grandes corporações, os dados sigilosos de estado e as questões políticas de nível transnacional.

No Brasil, o Marco Civil da Internet (Lei nº 12.965/2014), sancionado em 2014, regulamenta a proteção dos dados dos usuários e determina que a quebra dos sigilos telemáticos só ocorra em casos de ordem judicial, obrigando que as empresas internacionais que atuem no Brasil respeitem a legislação vigente (BRASIL, 2014). Entretanto, o desenvolvimento do aparato tecnológico permite que a comunicação, necessária para a continuidade da logística dos crimes praticados pelas ORCRIMs, se torne cada vez mais irrastreável. Sendo assim, as ORCRIMs se beneficiam constantemente das inovações tecnológicas para aperfeiçoarem, não só a ação criminosa, mas também para camuflar a rentabilidade ilícita oriunda destas ações, tornando cada vez mais difícil a coadunação de provas que efetivamente comprovem a autoria dos crimes praticados.

No escopo de atuação dos profissionais de inteligência que atuam com busca eletrônica, os meios de investigação criminal tradicionais, como a interceptação e a quebra de sigilo telefônico tornaram-se, desta forma, insuficientes diante da grande evolução do *modus operandi* das ORCRIMs, demonstrando a real necessidade de utilização de novas ferramentas.

É sob esse espectro que as forças policiais tendem a aperfeiçoar as investigações cibernéticas, com foco em inteligência digital. Nesse sentido, elas apostam em análises de conteúdo telemático e *cloud comuting* (*Google, Apple e Microsoft*), extratos de aplicativos de mensagens, como *Whatsapp*, utilização de softwares de extração de dados como *Cellebrite* e assim atingem de forma contundente as diversas ramificações das atividades ilícitas das ORCRIMs e os envolvidos.

Ao longo deste artigo, abordaremos o contexto histórico das tecnologias de comunicações utilizadas por membros de ORCRIMs, para então estudar os aspectos teóricos e práticos do monitoramento e interceptação das comunicações telemáticas, trazendo, por fim, ferramentas que auxiliarão na investigação em casos concretos.

2 - Contexto histórico

Na década de 90 e início dos anos 2000, grandes traficantes dos cartéis da Colômbia, México e de facções criminosas que exercem influência no Brasil, utilizaram telefones celulares com transmissão via satélite para realizarem transações criminosas, dar ordens aos seus subalternos e se comunicarem de forma segura (MARQUES, 2005). Um deles foi o traficante brasileiro Luiz

Fernando da Costa, o Fernandinho Beira-Mar, que usou telefones celulares com transmissão via satélite em diversos lugares do mundo, que foram interceptadas e rastreadas pela DEA (*Drug Enforcement Administration*) americana (MUNDOGEO, 2001).

Estes telefones celulares se conectam diretamente aos satélites e não às estações rádio-base (ERBs) como os aparelhos digitais comuns. Apesar de poderem ser interceptados, esta foi uma tecnologia que as polícias de todo o mundo resistiram em adquirir. O custo para manter este tipo de comunicação, até mesmo entre os criminosos, era alto e, por conta disso, era pouco popularizado entre eles. Consequentemente, não era garantida inviolabilidade da ligação, já que, se o interlocutor estivesse interceptado, seria facilmente captado pelas autoridades, independentemente se o alvo possuísse um aparelho com transmissão via satélite ou não. Além disso, as empresas que administravam esse tipo de serviço possuíam sede nos Estados Unidos. Por isso, haveriam conflitos judiciais na operacionalização de quaisquer medidas cautelares. O investimento financeiro para comprar e manter a tecnologia era muito cara e tais aparelhos celulares logo seriam substituídos por outras formas de se esquivar do monitoramento estatal, portanto, o Brasil optou por não se aperfeiçoar nessa tecnologia.

Posteriormente, em 1ª de agosto de 2005, a *Blackberry Messenger* (BBM) surgiu no mercado vendendo a ideia de que seu fluxo de mensagens era irrastreável e interceptável através de criptografia de mensagens e um sistema próprio de comunicação. Segundo a empresa, este tipo de comunicação não estaria abarcada na Lei de Interceptação Telefônica nº 9.296/96, pois não seria possível interceptar as mensagens de forma instantânea, tendo em vista que os servidores que armazenam tais mensagens estão situados no Canadá, ou seja, fora da jurisdição da justiça brasileira. Logo, os criminosos se tornaram adeptos desta marca com a intenção de permanecerem longe das ações de autoridades policiais.

Segundo Machado e Jezler Júnior (2020):

> "Nesse sentido, a obtenção de conversas privadas trocadas pela tecnologia BBM não será uma captação em 'tempo real', instantânea, justamente pela proteção da criptografia utilizada pela tecnologia, o que impede o desvio das mensagens durante o percurso e impõe a disponibilização de pacote de dados contendo um conjunto de mensagens à espera da quebra da criptografia, mediante fornecimento da chave pela subsidiária brasileira". (MACHADO; JEZLER JUNIOR, 2020, p.14)

Atualmente, os aplicativos de mensagens, como o Whatsapp, que apresentam alta proteção de criptografia, refletem um dos maiores obstáculos para profissionais de inteligência no âmbito de segurança.

3 - Legislação aplicável à interceptação do fluxo das comunicações telemáticas no âmbito de investigação de ORCRIMs

A realidade dos profissionais de inteligência que atuam em setores de

busca eletrônica no Brasil se baseia predominantemente em três legislações: a Lei nº 12.850 (Lei de Organização Criminosa), a Lei nº 9.296 (Lei de Interceptação Telefônica) e a Lei nº 12.965 (Marco Civil da Internet).

A Lei de Interceptação Telefônica dependerá de ordem judicial e ocorrerá por no máximo quinze dias, prorrogáveis quando comprovada necessidade:

> Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
> Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática. (BRASIL, 1996)

Entretanto, integrantes de grandes ORCRIMs praticamente não utilizam mais esta forma de se comunicar, principalmente quando se trata de conversas que versam sobre a atividade criminosa em si. Portanto, os profissionais de inteligência se utilizam de outras ferramentas que a internet fornece. Muitas empresas transnacionais, ao serem oficiadas para fornecerem dados cadastrais, são obrigadas a disponibilizar tais informações quando a investigação criminal em curso investiga uma ORCRIM:

> Art. 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito. (BRASIL, 2013)

O Marco Civil da Internet regulamentou o acesso das autoridades policiais aos dados dos usuários, como registros de conexão, acesso às aplicações de internet, conteúdo das comunicações privadas, mediante ordem judicial.

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º. (BRASIL, 2014)

Convém salientar que dados cadastrais podem ser requisitados através de ofício policial, assinado pela autoridade policial, fundamentado no poder geral de polícia (art. 6, III do Código do Processo Penal) e nos art. 13-A do Código de Processo Penal e na Lei Federal nº 9.613/98 e na Lei Federal nº

12.850/2013 e no art. 2 da Lei Federal nº 12.830/13. Desse modo, para futura representação pelo afastamento de sigilo dos dados telemáticos, notadamente visando a busca de dados dos provedores da *Google* e *Apple*, necessário se faz (caso não possua a conta de *e-mail* somente o número de IMEI do celular utilizado pelo alvo), primeiramente, encaminhar o ofício policial (administrativo), solicitando as contas vinculadas aos IMEIs no período de interesse para a investigação e, posteriormente, representar pela quebra de sigilo de dados dessas contas.

Por fim, é importante verificar se o número de IMEI está correto, ou se será necessário calcular o dígito verificador. Algumas operadoras de telefonia móvel ao fornecerem os números de IMEIs vinculados às linhas substituem o dígito verificador pelo algarismo "0". Apesar das dificuldades que regularmente se aplicam no cotidiano dos agentes que realizam investigações criminais de ORCRIMs, muito ainda é possível de fazer, respeitando criteriosamente tais legislações. Desta forma, a próxima seção elenca algumas das ações mais comuns em termos de busca eletrônica.

4. Interceptação do fluxo das comunicações telemáticas

Entende-se por interceptação o acesso autorizado por ordem judicial ao conteúdo integral e em tempo real, de todo o fluxo de comunicações do alvo, pelo prazo de 15 dias, renováveis por 15 dias (WHATSAPP, 2021).

4.1 *Whatsapp*[1]

É um aplicativo de mensagens instantâneas para telefone celular, atualmente gerido pela empresa *Facebook Inc*. Trata-se de um programa compatível com praticamente todos os smartphones do mercado e gratuito para uso. Além disso, as comunicações realizadas através de mensagens de texto utilizam criptografia ponto-a-ponto, fato este que torna o aplicativo mais atrativo, uma vez que a empresa garante a "inviolabilidade" desta criptografia frente a eventuais ataques de *hackers* ou de criminosos cibernéticos. Por conta desta criptografia, a empresa *Facebook Inc*, alega não ser possível cumprir ordens judiciais que determinem a interceptação do fluxo das comunicações do aplicativo.

Sem adentrar a discussão técnica sobre a veracidade do alegado pela empresa, incluímos o aplicativo *Whatsapp* neste tópico, pois a despeito de não fornecer o conteúdo criptografado das mensagens, a empresa *Facebook Inc* é capaz de fornecer, pelo prazo de 15 dias, o extrato das mensagens enviadas e recebidas pelo alvo. Esse extrato contempla as seguintes informações: a data, a hora e o tipo de mensagem; o tamanho da mensagem; o remetente e o destinatário (em conversas individuais e em grupo); os endereços de I.P do remetente e do destinatário.

Apesar de não ser, tecnicamente, uma interceptação, essa bilhetagem das mensagens dos alvos, em tempo real e pelo prazo de 15 dias, é uma excelente ferramenta, pois podemos verificar com quem o alvo mais se comunica, confirmar possíveis endereços (através de pesquisas posteriores aos I.Ps) e

1 - Para mais informações sobre as medidas de segurança adotadas pelo aplicativo WhatsApp, acesse: <http://www.whatsapp.com/records>. Último acesso em novembro de 2021.

localizar vínculos e clusters entre os investigados, após analisar esses dados no IBM *Analyst Notebook*.

4.1 Servidores de correio eletrônico *(e-mail) (Google, Apple, Microsoft, Yahoo):*

Apesar da comunicação através de *e-mail* já ter sido muito mais utilizada pelas pessoas de um modo geral, antes da criação de mensageiros instantâneos, ainda é possível conseguir dados relevantes para investigações sobre ORCRIMs, sobretudo em contas de *e-mails* de empresas. Citamos os servidores de e-mail mais populares atualmente, mas trata-se de rol meramente exemplificativo, não impedindo que seja realizada representação pela interceptação do fluxo de comunicações de outros servidores que porventura surgirem no caso concreto.

Basicamente, as empresas de correio eletrônico fornecem o conteúdo integral das mensagens recebidas e enviadas pelo alvo, em tempo real, pelo prazo de 15 dias, a partir da criação de uma "conta-espelho". O conteúdo é direcionado para essa "conta-espelho" na qual o usuário e a senha são fornecidos ao policial para que ele tenha acesso às mensagens.

5. Afastamento do sigilo de dados telemáticos

Entende-se por afastamento do sigilo de dados telemáticos, o acesso integral aos arquivos e informações armazenadas em servidores (*cloud computing*) ou em dispositivos físicos (celulares, dispositivos de armazenamento) no período inicial de interesse até a implementação da medida.

5.1 Dados armazenados em *cloud computing*: *Whatsapp*

A empresa *Facebook Inc*, responsável pela operação do aplicativo de mensagens *Whatsapp*, pode fornecer os seguintes dados dos usuários: dados cadastrais da conta (informações do aparelho e sistema operacional, versão do app, data e horário do registro, *status* de conexão, última conexão com data e hora, nome, endereço de *e-mail* se disponível, e informações de cliente *web*); foto de perfil; registros de acesso (IPs) dos últimos seis meses; histórico de mudança de números; grupos (data de criação, descrição, identificador do grupo ("*group-ID*"), foto quantidade de membros e nome do grupo). Após o fornecimento da listagem de grupos, fica autorizado o fornecimento de membros dos grupos que vierem a ser indicados formalmente pela autoridade policial, por meio de ofício, caso a ordem judicial original também inclua tal pedido; agenda de contatos.

5.2 *Google*[2]

A empresa *Google Inc*, multinacional, é a desenvolvedora do sistema operacional para smartphones *Android*, que está presente na maioria dos apare-

2 - Para mais informações sobre as medidas de segurança adotadas pelo Google, acesse: <http://lers.google.com>. Último acesso em novembro de 2021.

lhos que não são produzidos pela *Apple*, aparelhos estes que utilizam exclusivamente o sistema IOS. Além disso, a *Google* possui serviços como correio eletrônico (*Gmail*), armazenamento de arquivos em nuvem (*Google Drive*) e navegador de internet (*Chrome*). Os dados dos usuários que ficam armazenados nos servidores da empresa e que podem ser fornecidos através do afastamento de sigilo telemático são: os dados cadastrais, os registros de conexão (IPs), o conteúdo de *Gmail*, o conteúdo do *Google Fotos*, o conteúdo do *Google Drive*, a lista de contatos, o histórico de localização, o histórico de pesquisa, o histórico de navegação.

A grande quantidade de dados armazenados pelo sistema operacional *Android*, aliado ao fato de que, hoje em dia, praticamente todas as pessoas possuem telefone celular, tornam essa medida quase que obrigatória em se tratando de investigações versando sobre ORCRIMs. Importante destacar que arquivos de áudios, imagens e vídeos compartilhados pelo *Whatsapp* e salvos em *backup* na nuvem, poderão ser acessados. Somente mensagens de texto, que são criptografadas, não poderão ser lidas.

5.3 *Apple*[3]

A empresa *Apple*, multinacional, é a desenvolvedora do sistema operacional para *smartphones* IOS, exclusivamente utilizados por aparelhos desenvolvidos pela própria empresa. Assim como a *Google*, o sistema operacional IOS possui muitos utilizadores ao redor do mundo, sendo certo que, praticamente, essas duas empresas dividem o mercado de sistemas operacionais de telefone celular.

A *Apple* também possui serviços como correio eletrônico (*Icloudmail*), armazenamento de arquivos em nuvem (*Icloud*) e navegador de internet (*Safari*). Os dados dos usuários que ficam armazenados nos servidores da empresa e que podem ser fornecidos através do afastamento de sigilo telemático são: os dados cadastrais, os registros de conexão (IPs), o conteúdo do e-mail, o conteúdo do *Icloud*, a lista de contatos, o histórico de localização, o histórico de pesquisa e o histórico de navegação.

5.4 *Microsoft*[4]

A empresa multinacional Microsoft é a desenvolvedora de sistemas operacionais para computadores e telefones celulares (*Windows Phone*, *Windows Mobile* e recentemente *Windows 10 Mobile*), todos eles descontinuados. Dessa forma, apesar da empresa ter desenvolvido sistemas operacionais para telefone celular, a parcela da população que os utiliza é pequena, portanto quanto à Microsoft iremos nos ater ao serviço de correio eletrônico (*Hotmail*) e ao serviço de armazenamento na nuvem (*One Drive*).

5.5 *Facebook / Instagram*[5]

Facebook e *Instagram* são duas redes sociais extremamente populares, operacionalizadas pela empresa *Facebook Inc.* Desse modo, solicitações sobre

3 - Para mais informações sobre as medidas de segurança adotadas pela plataforma Apple, acesse: <https://support.apple.com/pt-br/guide/security/welcome/web>. Último acesso em novembro de 2021.

4 - Para mais informações sobre as medidas de segurança adotadas pela plataforma Microsoft, acesse: <https://support.microsoft.com/en-us/windows/what-is-microsoft-security-essentials-c25ad47a-7d15-8072-1438-b07dffcbbb20>. Último acesso em novembro de 2021.

5 - Para mais informações sobre as medidas de segurança adotadas pela rede social Facebook, acesse: <http://www.facebook.com/records>. Último acesso em novembro de 2021.

usuários de ambas devem ser enviadas para o portal de requisições de autoridades do *Facebook*.

Por conta de sua popularidade e pela quantidade de informações que armazenam essas redes sociais também são uma excelente ferramenta para buscar dados de alvos, sejam dados qualificativos, endereços, locais de atuação, veículos etc. As informações armazenadas pela empresa e disponíveis para requisições são: os dados cadastrais (nome, *e-mail*, telefone celular vinculado), a data de criação do perfil, o I.P. de criação do perfil, o histórico de acessos contendo os endereços de I.P.

5.6 *Twitter*[6]

É uma rede social, bastante popular, operacionalizada pela empresa *Twitter Inc*. Percebemos, em nossas investigações, que este site está sendo bastante utilizado por criminosos, notadamente traficantes de drogas.

As informações captadas pela empresa e que são passíveis de requisições são: os dados cadastrais (nome, telefone celular, e-mail, data da criação e I.P. de criação), o histórico de acessos contendo endereços de I.Ps, as mensagens diretas e as fotos publicadas. Importante destacar que, além do identificador da conta do *Twitter* que vem precedido de "@", é necessário também informar na requisição o número "UID", o *user identifier* (em tradução livre, identificador de usuário) da conta. Alguns sites gratuitos na internet fazem essa checagem do "UID" do perfil do *Twitter*.

5.7 *Uber / Uber eats*[7]

Uber é um aplicativo de transporte privado urbano e *Uber Eats* é uma plataforma (aplicativo) de pedidos e entrega de alimentos, ambas operacionalizadas pela multinacional *Uber Inc*. As informações importantes podem ser alcançadas através de requisições direcionadas à *Uber*, notadamente se o(s) alvo(s) utiliza(m) este aplicativo para se locomover ou pedir comida.

A seguir listamos os dados que estão disponíveis para requisição (*Uber*): os dados cadastrais completos (nome, CPF, telefone celular, *e-mail*) e as viagens realizadas (data, hora e itinerário). Já para o *Uber Eats*: dados cadastrais completos (nome, CPF, telefone celular, endereço de entrega) e os pedidos realizados (data, hora e estabelecimentos).

5.8 *Ifood*[8]

Ifood é um aplicativo de pedidos e entrega de alimentos, operacionalizada pela empresa de mesmo nome. A exemplo do aplicativo *Uber Eats*, requisições direcionadas à empresa *Ifood*, podem ser muito úteis para a confirmação de endereços dos alvos, caso eles possuam cadastro no aplicativo. As informações disponíveis para requisição são: dados cadastrais (nome, CPF, telefone celular, *e-mail*, endereço para entrega) e o histórico de pedidos (data, hora, estabelecimento).

6 - Para mais informações sobre as medidas de segurança adotadas pela rede social Twitter, acesse: <https://legalrequests.twitter.com/forms/landing_disclaimer>. Último acesso em novembro de 2021.

7 - Para mais informações sobre as medidas de segurança adotadas pela plataforma Uber, acesse: <http://lert.uber.com>. Último acesso em novembro de 2021.

8 - Para mais informações sobre as medidas de segurança adotadas pela plataforma ifood, acesse: <https://webmiddleware.ifood.com.br/seguranca>. Último acesso em novembro de 2021.

6. Dados armazenados em dispositivos físicos (telefone celular, HD, pendrive, etc.)

A extração de dados armazenados em dispositivos físicos, telefone celular, HD, *pendrive*, depende de prévia autorização judicial. Em se tratando de aparelhos telefônicos desbloqueados, HD's e *pendrives* sem senha, é possível fazer a extração de forma manual. No entanto, quando o aparelho telefônico está bloqueado por senha, a extração de dados deverá ser feita com algum *software* forense de extração de dados.

Nesse ponto, destacamos a empresa israelense "*Cellebrite*", desenvolvedora do *software* atualmente utilizado pela Polícia Civil do Estado do Rio de Janeiro, para esse tipo de extração de dados.

6.1 *Cellebrite*

É uma empresa israelense desenvolvedora de ferramentas forenses de extração de dados. O *software* de extração de dados forense, utilizado por organizações governamentais é o "*Universal Forensic Extraction Device*" (UFED), em português Dispositivo Universal de Extração Forense.

Segundo a empresa *Cellebrite*, o programa UFED é capaz de quebrar códigos, decifrar informações criptografadas e adquirir dados ocultos e excluídos. Ela afirma ainda que o UFED tem a capacidade de extrair dados de smartphones, dispositivos PDA, telefones celulares, dispositivos GPS e computadores *tablet*. O UFED pode extrair, descriptografar, traduzir e analisar contatos da agenda telefônica, todos os tipos de conteúdo multimídia, mensagens SMS e MMS, registros de chamadas, números de série eletrônicos (ESN), Identidade Internacional de Equipamentos Móveis (IMEI) e informações de localização do SIM, além de ser funcional em sistemas operacionais, como IOS, *Android, BlackBerry, Symbian, Windows Mobile e Palm*. Alguns arquivos excluídos também podem ser recuperados e extraídos. Trata-se de excelente ferramenta para busca de dados sigilosos.

A licença para utilização do *software* é paga. Atualmente o programa está disponível no âmbito da SEPOL (Secretaria de Estado de Polícia Civil), tendo sido utilizado com êxito em investigações de repercussão, a exemplo do Caso Marielle Franco e recentemente do Caso Henry Borel.

Considerações finais

Com o constante avanço da tecnologia e dos meios de comunicação, não há dúvida de que as forças policiais devem buscar atualização contínua, notadamente no que diz respeito à interceptação da comunicação dos membros das ORCRIMs. Historicamente, essas organizações investiram em novidades tecnológicas para aprimorar sua comunicação, sempre na tentativa de se furtar da ação dos órgãos de persecução penal.

É sabido que, atualmente, os membros de ORCRIMs praticamente não utilizam mais chamadas telefônicas convencionais para se comunicarem, o

que representa um desafio constante para os operadores da área, na busca de soluções para o efetivo monitoramento dessas comunicações. Nessa esteira, asseveramos a importância das ferramentas aqui trazidas, que aliadas a outras técnicas de investigação, são, em nosso entender, fundamentais para investigações de crimes praticados por ORCRIMs.

Referências bibliográficas

BRASIL. **Código de Processo Penal**. Decreto lei nº 3.689, de 03 de outubro de 1941. Disponível em: http://www.planalto.gov.br/CCIVIL/Decreto-Lei/Del3689.htm. Último acesso em novembro de 2021.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, 23 de abril de 2014.

_____. Lei nº 9.613, de 3 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. **Diário Oficial da União**, Brasília, 3 de março de 1998.

_____. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. **Diário Oficial da União**, Brasília, 24 de julho de 1996.

_____. Lei nº 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. **Diário Oficial da União**, Brasília, 2 de agosto de 2013.

_____. Lei nº 12.830, de 20 de junho de 2013. Dispõe sobre a investigação criminal conduzida pelo delegado de polícia. **Diário Oficial da União**, Brasília, 20 de junho de 2013.

CELLEBRITE. UFED 1.2.0.0 Release Notes. Disponível em: <https://cf-media.cellebrite.com/wp-content/uploads/2017/07/UFED6.2_ReleaseNotes_EN.pdf>. Último acesso em novembro de 2021.

DANTOS, Pedro. Quadrilha de Beira-Mar foi desmantelada nos últimos dois anos. **Folha de S.Paulo**, Rio de Janeiro, 21 de abril de 2001. Disponível em: <https://www1.folha.uol.com.br/folha/cotidiano/ult95u27451.shtml>. Último acesso em novembro de 2021.

FREITAS JÚNIOR, Aldair Dias De, JORGE, Higor Vinicius Nogueira, GARZELLA, Oleno Carlos Faria. **Manual de Interceptação Telefônica e Telemática**. Salvador: Editora JusPodivm, 2020.

G1. O que é o software usado pela polícia do Rio para investigar celulares no caso Henry Borel. **G1**, 08 de abril de 2021. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/04/08/o-que-e-o-software-usado-pela-policia-do-rio-para-investigar-celulares-no-caso-henry-borel.ghtml>. Último acesso em novembro de 2021.

GOMES, Marcelo e COELHO, André. Caso Marielle: Justiça autoriza empresa a extrair dados de celulares de Ronnie Lessa e Élcio Queiroz. **G1**, 01 de agosto de 2019. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/08/01/caso-marielle-justica-autoriza-pericia-particular-nos-celulares-de-ronnie-lessa-e-elcio-queiroz.ghtml>. Último acesso em novembro de 2021.

HOOG, Andrew. **Cellebrite UFED**. Consultado em 8 de junho de 2012. Cópia arquivada em 20 de junho de 2013.

JEZLER JÚNIOR, Ivan, MACHADO, Vitor Paczek. É inválida a utilização da Lei 9.296 na captação de mensagens trocadas pelo Blackberry Messenger? **Boletim IBCCrim**., n. 311, p. 14 – 15, 2018.

MARQUES, Hugo. País deixa de combater crimes por deficiência tecnológica. **Jornal do Brasil**, Brasília, 18 de abril de 2005. Disponível em: <https://www2.senado.leg.br/bdsf/bitstream/handle/id/60858/noticia.htm?sequence=1>. Último acesso em novembro de 2021.

MOREIRA, Romulo de Andrade. Operação Lava-Jato: onde há fumaça há fogo e, possivelmente, nulidade. **Jus.com.br**, janeiro de 2015. Disponível em: <https://jus.com.br/artigos/35778/operacao-lava-jato-onde-ha-fumaca-ha-fogo-e-possivelmente-nulidade>. Último acesso em novembro de 2021.

MUNDO GEO. Satélite intercepta Beira-Mar. Mundo Geo, 09 de janeiro de 2001. Disponível em <https://mundogeo.com/2001/01/09/satelite-intercepta-beira-mar/>. Último acesso em novembro de 2021.

NETO, Francisco S., CABETTE, Eduardo. Acesso às comunicações do "Blackberry messenger": uma análise sobre a legalidade. **Jus Brasil**, 2018. Disponível em <https://canalcienciascriminais.jusbrasil.com.br/artigos/659135143/acesso-as-comunicacoes-do-blackberry-messenger-uma-analise-sobre-a-legalidade>. Último acesso em novembro de 2021.

OSBORNE, Charlie. For investigators, a better way to extract data from mobile devices. **ZD Net**, 31 de maio de 2012. Disponível em: < https://www.zdnet.com/article/for-investigators-a-better-way-to-extract-data-from-mobile-devices/>. Último acesso em novembro de 2021.

WHATSAPP INC. Informações para as autoridades policiais, 2021. Disponível em: <https://faq.whatsapp.com/general/security-and-privacy/information-for-law-enforcement-authorities/?lang=pt_br>. Último acesso em novembro de 2021.

WHITFIELD, Lee. Forensic 4cast Awards 2012 – Results. **Forensic 4: cast**, 27 de junho de 2012. Disponível em: < https://forensic4cast.com/2012/06/forensic-4cast-awards-2012-results/>. Último acesso em novembro de 2021.