Adair Dias de Freitas Júnior
Higor Vinicius Nogueira Jorge
Oleno Carlos Faria Garzella

Manual de
INTERCEPTAÇÃO TELEFÔNICA e TELEMÁTICA

Teoria • Prática • Legislação

Prefácio
Alesandro Gonçalves Barreto

Apresentação
Júlio Gustavo Vieira Guebert

2020

EDITORA JusPODIVM
www.editorajuspodivm.com.br

ASPECTOS PRÁTICOS

• ASPECTOS INAUGURAIS

Como qualquer nova tarefa, lançar-se pela primeira vez à execução de procedimentos investigativos especiais, como é o caso da interceptação do fluxo das comunicações telefônicas e telemáticas, é uma atividade extremamente desafiadora.

Para suplantar a barreira que o novo operador de tais procedimentos possa encontrar, tecer-se-á, a seguir, sintéticos comentários com os principais aspectos necessários à execução da investigação telefônica e telemática.

Nesse mister, será apresentado um caso prático fantasioso, baseado em fatos verídicos, em que o leitor possa se fundar para alcançar entendimento claro e simplificado acerca das etapas que deverá perpassar quando estiver diante de um caso real.

Importante esclarecer que dependendo do órgão (Polícia Civil, Polícia Federal, Ministério Público Estadual, Ministério Público Federal etc.) ou o Estado da Federação, onde realizar-se-á a investigação criminal, existem peculiaridades que devem ser observadas. Optou-se por apresentar um passo a passo tomando por base o Estado de São Paulo.

Forma mais didática de viabilizar a compreensão do leitor, o caso concreto construído, sem a identificação dos investiga-

dos e do local em que ocorreram os eventos, conterá exibição de imagens, não sigilosas, dos acessos iniciais de sítios eletrônicos por meio dos quais ocorrerá a procedimentalização das interceptações.

É de todo salutar que o leitor se permita a completa imersão no caso, buscando ocupar o lugar dos Agentes de Polícia Judiciária ou Delegado de Polícia no desenvolvimento dos procedimentos. Sem mais delongas, passemos à prática.

• CASO PRÁTICO – HOMICÍDIO QUALIFICADO

Ato I – Contexto fático

Em determinada data, o empresário Charlie e sua esposa Juliete foram encontrados, no interior do veículo do casal, com perfurações cranianas provocadas por projéteis de arma de fogo e seus corpos carbonizados.

Ato II – Apuração preliminar

Houve a **instauração de inquérito policial**[1] e, após a realização de **diligências investigativas iniciais** pelos Agentes de Polícia Judiciária, foi confeccionado um **relatório de serviço**[2] que trazia a principal hipótese investigativa trabalhada e, em decorrência desta, a demonstração de que apenas a interceptação telefônica e telemática seria apta a atingir a elucidação do delito.

1. O primeiro ato da investigação deverá ser a instauração de inquérito policial, se conduzida pela Polícia Judiciária, ou procedimento investigativo criminal, nas hipóteses de investigação realizada pelo Ministério Público.
2. O relatório de serviço preliminar é peça indispensável que deverá apontar a hipótese investigativa adotada e, pela narrativa racional e lógica dos acontecimentos e produtos iniciais da investigação, indicar a indispensabilidade da interceptação telefônica como única medida apta a atingir a elucidação do delito.

Ato III – Representação

Diante da apuração preliminar, os sócios das vítimas passaram a ser investigados. Após tomar conhecimento do **relatório de serviço** apresentado pelos agentes de Polícia Judiciária, o delegado de polícia confeccionou **representação**[3] perante o Poder Judiciário para que fosse deferida e emitida ordem de implementação de interceptação telefônica das linhas celulares dos investigados.

Ato IV – Deferimento

O Judiciário local, ao receber um **envelope lacrado**[4], contendo **representação** e **relatório de serviço**, abre vistas ao Ministério Público, que opina quanto ao deferimento da medida cautelar sigilosa. O Juiz de Direito do caso, analisando os indícios trazidos pela peça policial e, verificando presentes os requisitos legais da Lei 9.296/1996, defere o pleito, determinando a expedição de **ordem judicial**[5] às operadoras de telefonia para a implementação de interceptação telefônica.

Ato V – Implementação

De posse da ordem judicial, os agentes de Polícia Judiciária procederam ao seu envio para o **Centro de Inteligência Policial**

3. A representação é peça de Polícia Judiciária em que o delegado de polícia deverá narrar, de forma objetiva, os fatos apurados, a apuração preliminar trazida pelos agentes policiais e, em decorrência disso, solicitar autorização e ordem judicial de interceptação telefônica.

4. A representação e o relatório de serviço deverão seguir, em forma física obrigatória, dentro de envelope lacrado, ao cartório distribuidor do Fórum local. É imperiosa a manutenção do sigilo em medidas de interceptação telefônica e telemática.

5. A ordem judicial de interceptação telefônica expedida pelo juízo deverá conter transcrição exata do pedido, em linguagem técnica obrigatória, contida na representação. Em regra, tal decisão terá forma de ofício expedido pelo juiz de Direito às operadoras de telefonia.

da Delegacia Seccional de Polícia[6] da localidade e **também para as operadoras**[7] atuantes sobre aquela área.

Ato VI – Acompanhamento

Após a devida implementação da interceptação das linhas telefônicas dos investigados, a equipe policial teve acesso aos registros de ligações realizadas pelos averiguados, ocasião pela qual observou que, logo antes do horário apontado como de cometimento do crime, um dos sócios efetuou 3 ligações para seu contador, sob a área de cobertura de uma Estação Rádio Base – ERB – que abrangia determinado escritório em que a investigação teve notícia de utilização para reunião de negócios, na data dos fatos, entre as partes.

Analisando, por meio dos dados de localização das ERBs, o deslocamento dos investigados e das vítimas nos horários próximos ao apontado como do momento do cometimento do crime, observou-se que a área de encontro dos corpos era convergente com o caminho traçado por um dos investigados, razão pela qual, já tendo angariado elementos indiciários, por ordem da autoridade policial, notificou-se um dos averiguados a comparecer na delegacia de polícia a fim de prestar esclarecimentos.

O notificado, após ser inquirido e confrontado com dados tornados conhecidos pela investigação, poucas horas depois de

---

6. Os Centros de Inteligência são responsáveis por reencaminhar a ordem judicial aos respectivos órgãos superiores na cadeia de inteligência policial. O Departamento de Inteligência, por sua vez, fará a retransmissão do ofício judicial às operadoras para que estas implementem, em ação conjunta com o órgão policial, o desvio das linhas interceptadas aos celulares dos agentes policiais e ao equipamento de gravação da Polícia Judiciária.

7. Em complemento, os agentes responsáveis pelo acompanhamento da interceptação deverão enviar, diretamente, às operadoras, cópias da orem judicial a fim de que aquelas criem contas de acesso aos sistemas de monitoramento dos alvos investigados. Esta etapa deve ser feita por cada um dos agentes, vez que será necessária criação de senha pessoal e intransferível.

sair da Central de Polícia Judiciária, ligou para seu contador, que estava em viagem, e disse: "a Polícia veio atrás de mim, preciso ir logo até seu escritório e tirar a arma e aquele livro de lá antes que os policiais consigam um mandado de busca".

Diante dos indícios de autoria e da imprescindibilidade da medida para as investigações, a autoridade policial confeccionou, em caráter de urgência, representação visando prisão temporária deste investigado.

A investigação, utilizando-se de **senhas de consulta a dados cadastrais**[8], conseguiu obter a completa **qualificação**[9] do referido contador, tornando conhecida também a localização de seu escritório.

Montada então campana policial próxima ao referido escritório, tão logo saiu de lá, o sócio investigado foi abordado e sofreu busca pessoal sob o fundamento de trazer consigo elemento de descoberta imprescindível para formação de conjunto probatório. Na pasta do sócio estava depositada arma de fogo que, conforme Laudo elaborado pelo médico legista do Instituto Médico-Legal, possuía calibre idêntico a do armamento utilizado para o crime. Não só, ali estava o livro referido na ligação telefônica, em que se continha registros de desvio de grande monta de dinheiro, que estava sendo realizado pelo investigado, com auxílio de seu contador, contra as vítimas.

Com o principal suspeito preso temporariamente, a autoridade policial confeccionou, então, representação de busca e

8. Ferramenta de maior importância nas investigações por interceptação telefônica, é imprescindível que o ofício judicial contenha a determinação para criação de senhas de acesso a dados cadastrais e registros de ligações, com monitoramento de deslocamento em tempo real, de investigados e pessoas a eles relacionadas, abrangente, inclusive, de período pretérito razoável. Sem ordem com tais termos, a investigação estará às cegas.

9. Dados identificadores pessoais.

apreensão a ser cumprida no escritório em que se tinha dado a reunião entre as partes, local este que se presumia como de ocorrência dos disparos que vitimaram o casal.

A perícia técnica foi realizada por perito criminal oficial e exitosa quanto ao encontro de resquícios de pólvora e sangue humano, ocasião pela qual, obteve-se elemento novo apto a justificar pedido de prorrogação da prisão temporária do suspeito.

Conhecendo da prisão de seu cliente, o contador, temendo ser preso para apuração de sua participação no crime, evadiu-se para local desconhecido, ocasião pela qual a autoridade policial representou por sua prisão temporária, pedido este, acatado pelo juízo prevento.

Ato VII – Prorrogação

Havendo necessidade de aprofundamento nas investigações, estando-se próximo ao final do primeiro período de interceptação telefônica (exíguo iter de 15 dias), os agentes policiais confeccionaram **auto circunstanciado**[10] em que narraram as ações empreendidas e indicaram a necessidade de **prorrogação da autorização de interceptação telefônica**[11], nela inclusa a linha telefônica do contador.

Realizada nova **representação** pela autoridade policial e encaminhada, acompanhada do **auto circunstanciado**, em envelope

10. Peça de Polícia Judiciária confeccionada por dois agentes policiais, com curso superior, e responsáveis pelo acompanhamento das interceptações em que se narrará as diligências realizadas e será degravado, isto é, transcritas e identificadas, as ligações e mensagens que formarem conjunto probatório.

11. A fim de evitar solução de continuidade, o auto circunstanciado e a nova representação deverão estar depositadas no juízo local no penúltimo dia do período de interceptação. Note que, por conta disso, a investigação sempre sofrerá prejuízo de 2 dias em período investigativo, contudo, a prática revela que apenas assim há tempo hábil para expedição de nova ordem judicial e implementação das interceptações pelas operadoras de telefonia.

fechado, ao juízo prevento, foi emitida nova **ordem judicial** contenedora da determinação de prorrogação das **senhas de consulta a dados cadastrais, registros telefônicos e localização de linhas alvo relacionadas aos investigados**, bem como de **continuidade das interceptações telefônicas**.

Ato VIII – Investigação Telemática

Ciente da possibilidade de estar sob interceptação telefônica, o contador desfez-se de sua linha. Não só, decidiu por não realizar nenhum contato por ligação telefônica com seus familiares, já que anteviu a possibilidade de interceptação também de tais pessoas.

Diante da falta de utilização da linha interceptada, os agentes, novamente em uso das **senhas de acesso restritas**, obtiveram o **IMEI - *International Mobile Equipment Identity* (Identificação Internacional de Equipamento Móvel) do aparelho utilizado pelo contador foragido.**

Confeccionaram, então, novo relatório de serviço em que solicitaram à autoridade policial a expedição de nova representação, desta vez direcionada ao ***Google*** e ***WhatsApp*** com o fito de que juízo local emitisse nova **ordem judicial** para que tais empresas fornecessem o ***e-mail***[12] vinculado ao IMEI do aparelho do investigado, fornecendo também, em seguida, os **registros de pesquisa no *Google*, *logs* de acesso do *WhatsApp***[13] e **dados de mídia armazenados em nuvem**[14].

Expedida **ordem judicial** nos termos técnicos indicados pela autoridade policial em sua **representação**, a equipe policial

12. A identificação da conta do usuário é indispensável para o acesso aos seus dados.
13. Registros de conexão que listarão IPs aptos a indicar a localização do buscado.
14. Dados de mídia encaminhados à nuvem em ***backups*** realizados pelo sistema *Android*.

a encaminhou ao ***Google*** e ***WhatsApp***, por seus portais de ***Law Enforcement***[15].

Tão logo aportaram na Delegacia de Polícia as informações requisitadas àquelas empresas, a investigação pôde constatar que, 2 dias antes da data do crime, a conta de *e-mail* do contador foragido registrou **pesquisa** no ***Google*** nos termos "melhor forma de eliminar vestígios", "micro-ondas do crime", "sem corpo, sem crime".

Por sua vez, nos dados armazenados na **nuvem** da mesma conta, havia **imagem** com recente *upload*, datada do dia anterior ao recebimento dos dados, que retratava famosa queda d'água localizada na divisa territorial do Brasil com país vizinho.

Os ***logs* de acesso**, por seu turno, revelaram lista de IPs – *Internet Protocols* – em que determinado sequencial era recorrente a partir da fuga. Selecionados e identificados os provedores de internet fornecedores de tais IPs, a equipe investigativa emitiu novo **auto circunstanciado** contendo o produto de tais dados, ocasião pela qual a autoridade policial emitiu **ofício requisitório de dados cadastrais** ao principal provedor de internet.

Recebidos os dados cadastrais do usuário vinculado ao *internet protocol* recorrente, a equipe policial tomou conhecimento de que se relacionava a determinada hospedaria localizada na divisa do país.

Ato IX – Desfecho

De posse do conhecimento da provável localização do contador foragido, a equipe policial se deslocou, em viaturas descaracterizadas, à região, permanecendo em campana nos arredores até que, no segundo dia de espera, foram exitosos em flagrar o procurado pela Justiça caminhando até uma farmácia nas proximidades da hospedaria.

15. Ambas as empresas, assim como o ***Facebook***, possuem portais para submissão de ordens legais.

Estando os suspeitos presos, o trabalho investigativo foi encerrado com produção de **auto circunstanciado** contendo o produto do período final de interceptação e **relatório de serviço**[16] tratando das diligências finais realizadas.

A autoridade policial, tendo recebido o **relatório final de investigação**, confeccionou **relatório final de inquérito policial**[17]**,** em que tratou dos fatos, da primeira à última diligência, elencando todos os elementos informativos, coligidos aos autos, aptos a demonstrar indícios de autoria e materialidade, de forma objetiva, bem como a fundar o despacho de **indiciamento** e subsidiar a **acusação** penal pelo *Parquet*.

• PROCEDIMENTOS INICIAIS DE IMPLEMENTAÇÃO E ACESSO A FERRAMENTAS INVESTIGATIVAS

A seguir serão trazidos os procedimentos iniciais de implementação e acesso às ferramentas investigativas em interceptação telefônica. Serão tecidas breves explicações acerca das etapas principais a serem cumpridas com as principais operadoras de telefonia, principais redes sociais e aplicativos de troca de mensagens por telemática.

Serão exibidas imagens disponíveis em sítios de livre acesso e passadas orientações de solicitação de criação de usuário e senha. Cada sistema de monitoramento pode conter peculiaridades que apenas podem ser reveladas pela leitura de manuais sigilosos a que o agente operacional terá acesso após realizar seu devido cadastramento e enviar ordem legal.

16. Nesta peça deverá haver referência e transcrição dos elementos indispensáveis à prova de autoria e materialidade.

17. A remessa final do inquérito policial deverá ser acompanhada do envio, em mídia gravada, do produto integral das interceptações telefônicas e telemáticas.

Em capítulo específico desta obra, intitulado "Modelos de Peças", o leitor encontrará modelos de todos os ofícios, autos circunstanciados, relatórios de serviço e representações citadas ao longo da obra.

• ASPECTOS PRÁTICOS CONFORME AS PECULIARIDADES DAS PRINCIPAIS OPERADORAS DE TELEFONIA

• VIVO/TELEFÔNICA – SA

Endereços e telefones úteis:

VIVO/TELEFÔNICA
Divisão de Serviços Especiais – D.S.E.
Rua Doutor Fausto Ferraz, 172 - 3º andar - Bela Vista
São Paulo/SP
Vigia Vivo: https://vigia.vivo.com.br/login.html
Portal Jud Vivo: https://portaljud.vivo.com.br/portaljud/login.jsf
Telefone: 0800 770 8486

A autoridade policial ou representante do Ministério Público deverá confeccionar e enviar um **ofício requisitório de criação de usuário e senha** à empresa Telefônica/Vivo.

No corpo de referido ofício, a autoridade deverá solicitar a criação de usuário e senha de acesso ao **Portal Jud Vivo** e ao sistema **Vigia Vivo**, plataformas fornecidas pela operadora a fim de procedimentalizar os trabalhos.

Os documentos oficiais deverão ser encaminhados para a respectiva operadora por dois canais, a saber, o Portal Jud Vivo, para aqueles que já possuam cadastro, ou e-mail ordens.sigilo.br@tefefonica.com, para usuários ainda não cadastrados. É relevante fazer recordar que o serviço de fax foi desativado em 31/12/2019.

Transcorrido certo lapso temporal, cerca de trinta minutos, a operadora enviará resposta para o e-mail constante nos ofícios.

Caso tal não ocorra, deverá o agente entrar em contato com a operadora pelo telefone 0800 770 8486, ocasião em que serão disponibilizadas duas opções, sendo elas, 1- atendimento; 2- dúvidas relacionadas ao envio de ofícios.

Aqui, caberá ao interessado pleitear tais medidas, sempre tendo em mãos o número do ofício e nome da autoridade signatária.

Ao receber atendimento, os agentes responsáveis pelo acompanhamento das interceptações, cujos nomes deverão constar, acompanhados de e-mail institucional, cargo e cadastro de pessoa física – CPF –, na ordem judicial ou ofício de criação de usuário e senha, devem transmitir, por voz, dados pessoais ao atendente desta operadora.

Completa a criação de usuário e senha de acesso aos portais Vigia Vivo e Portal Jud Vivo, o operacional receberá em seu e-mail institucional um arquivo compactado contendo seu usuário e senha de acesso. A abertura deste arquivo protegido será feita mediante digitação da sequência numeral **8486**, seguida do acionamento da tecla *enter*.

Antes de passar à exploração das ferramentas Portal Jud Vivo e Vigia Vivo, o operacional deverá solicitar o cadastramento de uma senha de voz, a qual deverá ser anunciada ao atendente nas ligações futuras a fim de possibilitar realização de pesquisas de históricos de chamadas originadas ou recebidas por números e IMEIs não interceptados, além de extratos de conexão de dados móveis, requisições estas que apenas poderão ser feitas por este último meio de chamada de voz ao 0800 770 8486.

Note-se que tal acesso por voz é o único meio de acesso a registros telefônicos de outros investigados que não o alvo interceptado. Por óbvio, tais investigados deverão guardar estrita relação com o alvo interceptado e/ou o objeto da investigação.

VIGIA VIVO

O Sistema Vigia Vivo é acessível por sítio eletrônico e possibilitará ao operacional o acesso aos dados e registros telefônicos e telemáticos do alvo interceptado, como seu registro de ligações[18] efetuadas e recebidas, conexões, deslocamentos por ERBs, troca de mensagens, rastreio em tempo real e extratos diversos ligados, sempre, ao indivíduo alvo da investigação.

Ao acessar a plataforma fornecida pela Vivo/Telefônica, deverá ser inserido o *login* e senha fornecidas pela operadora e encaminhadas ao operacional em seu e-mail institucional.

No primeiro acesso o usuário deverá cadastrar uma nova senha, obrigatoriamente composta por ao menos duas letras maiúsculas, duas minúsculas, dois números e dois caracteres não alfanuméricos, as quais deverão ser substituídas, em média, a cada trinta dias ou quando a operadora assim o determinar. "EXemplo./2019" retrata uma senha que atende aos requisitos exigidos.

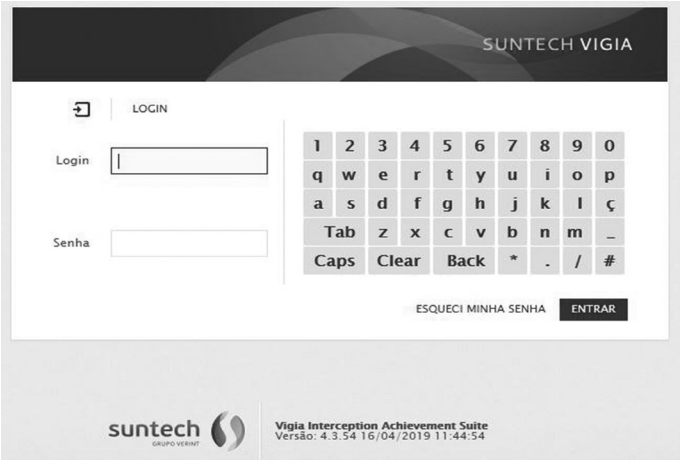

Figura 1 - Interface do Vigia Vivo

18. O registro de ligações é tratado no meio policial como bilhetagem ou régua.

Providenciada pela *Suntech*, a plataforma Vigia é a principal ferramenta de monitoramento de um alvo interceptado da investigação.

Uma vez conectado, o acesso às ferramentas internas do Vigia Vivo será acessível mediante inserção de código no campo "nome da operação", seguido de aplicação de senha específica, também fornecida pela operadora quando há implementação de uma interceptação telefônica.

Vale salientar que as operações poderão ser individualizadas por um único alvo ou conter mais de um número/IMEI em um mesmo crachá de acesso. A utilização é feita por intermédio da inserção dos dados através das senhas enviadas ao seu e-mail, permitindo acesso, individualmente, a cada alvo.

Por tratar-se de objeto protegido legalmente, não poderão ser fornecidas nesta obra telas e funcionalidade por funcionalidade desta plataforma. Para tanto, após regularmente cadastrado, o operacional deverá clicar o ícone "ajuda", comumente localizado no canto superior direito da tela, para realizar o *download* de um manual das localizações e funcionalidades dentro do dispositivo.

PORTAL JUD VIVO

Nos mesmos moldes do Vigia Vivo, a plataforma é acessível por sítio eletrônico em que o operacional deverá utilizar o *login* fornecido pela operadora e cadastrar uma senha com letras maiúsculas, minúsculas e números.

No Portal Jud Vivo, é possível submeter, como via alternativa ao fax, ofícios e outros documentos mediante acionamento da aba "enviar documentos".

A principal funcionalidade do Portal Jud Vivo, no entanto, é outra. Esta é a plataforma de consulta a dados cadastrais da opera-

dora Vivo. Nela é possível realizar pesquisas por dados cadastrais ligados a nomes, CPF, CNPJ, e número de telefone[19].

Figura 2 - Página inicial do Portal Jud Vivo

O Portal Jud Vivo é a principal ferramenta de consulta a dados cadastrais da operadora Vivo. Sua interface permite baixar um manual explicativo para o primeiro acesso.

Uma vez inseridos os dados de acesso, o Portal Jud Vivo exigirá a inserção de um sequencial de segurança contido em um cartão de segurança enviado ao e-mail institucional do operacional quando de seu cadastramento.

No interior do dispositivo é possível selecionar um ofício ativo, previamente enviado para cadastramento, que permitirá a realização de pesquisas. Ponto salutar é indicar que a caixa comando para inserção de elementos de pesquisa é sempre feita em

19. Os números de linhas telefônicas deverão ser sempre precedidos de ***DDD*** – discagem direta à distância.

janela extra, daí haver necessidade de não estarem vedados os *pop-ups* afeitos a este sítio eletrônico.

Tal janela de pesquisas possui *slots* para preenchimento apenas em sua parte inferior, devendo o operacional manobrar a barra de rolagem para os acessar.

• CLARO/EMBRATEL

Endereços e telefones úteis:

Setor de Ofícios da Claro
Rua Flórida, 1.970, Brooklin Novo
São Paulo-SP
Vigia Claro: https://vigia.claro.com.br/login.html
Telefone: (11) 3579 6700
E-mails: oficios.juridico@claro.com.br & oficios.doc@claro.com.br

A operadora Claro viabiliza a plataforma Vigia Claro para procedimentalizar a interceptação telefônica e seu acompanhamento. Aglutina, portanto, ferramentas em um mesmo sistema, o que dá pragmaticidade ao trabalho do operacional.

No primeiro acesso deverá ser feito envio de **ofício requisitório de criação de usuário e senha de acesso ao Vigia Claro**. A própria autoridade que preside o procedimento investigativo deverá confeccionar tal ofício e fazer sua remissão à operadora por meio de seus e-mails indicados supra.

O ofício, nos mesmos moldes das outras operadoras, deverá conter nome, CPF, cargo e e-mail institucional do operacional. Após seu envio, a operadora enviará *login* e senha de acesso, que deverá ser trocada no primeiro ingresso no sistema, ao e-mail institucional do operador. A nova senha deverá conter obrigatoriamente ao menos duas letras maiúsculas, duas minúsculas, dois

números e dois caracteres não alfanuméricos, as quais deverão ser substituídas, em média, a cada trinta dias ou quando a operadora assim o determinar. "EXemplo./2019" retrata uma senha que atende aos requisitos exigidos.

VIGIA CLARO

Ao acessar o Vigia Claro será possível clicar no botão "ajuda", geralmente situado no canto direito superior da tela, mediante o qual será possível obter um manual de acesso e localização das funcionalidades disponíveis.

O Vigia Claro permite a abertura de operação mediante inserção de um sequencial e senha para monitoramento de alvo interceptado junto à operadora. Por este meio é possível obter registro de ligações efetuadas e recebidas, mensagens trocadas, conexões, deslocamentos e rastreio em tempo real.

Há ainda outra aba acessível mediante clique no botão "senhas". Tal funcionalidade depende da existência de um ofício judicial válido, previamente enviado para cadastro para o e-mail **oficios.juridico@claro.com.br**, e permitirá o acesso à pesquisa de dados cadastrais e registros telefônicos de outros números, IMEIs e CPFs não interceptados, mas relacionados ao objeto da investigação e ao alvo interceptado.

Esta última ferramenta é acessível conforme conteúdo trazido no ofício judicial emitido pelo juiz do feito, daí ser de fundamental importância que a representação conste os exatos termos técnicos necessários à investigação.

Por motivos de sigilo, não poderão ser trazidas imagens e maiores detalhes do acionamento de cada funcionalidade, contudo, como dito acima, após realização de cadastro e obtenção de acesso, é possível acessar o manual fornecido pelo administrador da plataforma.

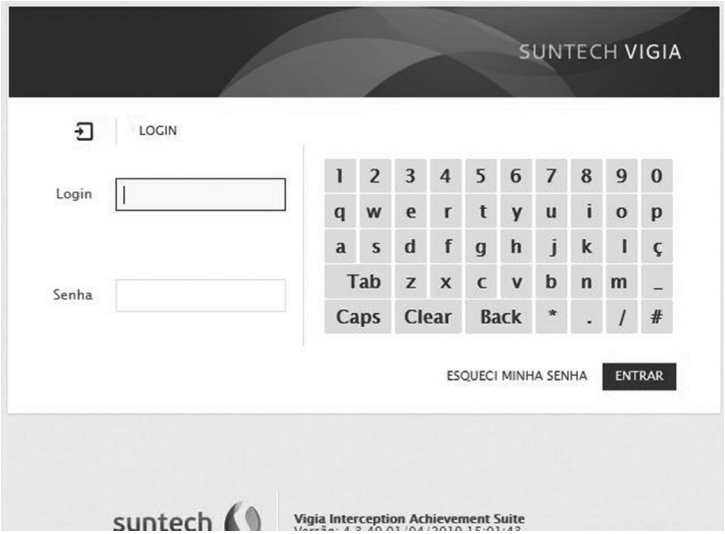

Figura 3 - Interface do Vigia Claro

A tela inicial da plataforma é semelhante nas principais operadoras, diferindo apenas quanto às funcionalidades disponíveis em cada sistema.

- **TIM**

Endereços e telefones úteis:

GRAOP
Avenida Alexandre Gusmão, Bloco C, 29, Vila Homero Thon
Santo André-SP
Vigia Tim: https://poarg.timbrasil.com.br/login.html
Infoguard Tim: https://infoguard.timbrasil.com.br/login.html
Telefone: (11) 4251 6633
E-mails: graop_oficios@timbrasil.com.br /
graop@timbrasil.com.br

A operadora Tim deverá ser acionada, para o primeiro acesso, por meio do envio de **ofício requisitório de criação de usuário**

e senha de acesso ao Vigia Tim e **Infoguard** a ser encaminhado ao **graop_oficios@timbrasil.com.br**.

O interessado deverá acessar a plataforma do Inforguard, clicar em cadastre-se, ocasião em que se abrirá um campo a ser preenchido com o número do CPF do solicitante, em seguida, haverá redirecionamento a outra tela denominada "FORMULÁRIO DE CADASTRO PARA NOVOS USUÁRIOS DO SISTEMA INFOGUARD", tela em que o operacional deverá preencher os dados pessoais e encaminhar à operadora.

Dados do operacional, como nome, CPF, cargo e e-mail institucional do operacional são obrigatórios. Após seu envio, a operadora enviará *login* e senha de acesso, que deverá ser trocada no primeiro ingresso no sistema, ao e-mail institucional do operador do Vigia e do Infoguard, obrigatoriamente composta por ao menos duas letras maiúsculas, duas minúsculas, dois números e dois caracteres não alfanuméricos, as quais deverão ser substituídas, em média, a cada trinta dias ou quando a operadora assim o determinar. "EXemplo./2019" retrata uma senha que atende aos requisitos exigidos.

Tal qual a operadora Vivo, a operadora Tim trabalha com duas plataformas, servindo, o Vigia, para monitoramento das linhas alvo interceptadas junto à operadora, por onde será possível ter acesso aos registros de ligações, mensagens, conexões, movimentação e rastreio em tempo real do investigado.

O Infoguard, por sua vez, é a plataforma fornecida pela operadora que possibilita o envio de documentos, tais quais ofícios requisitórios de dados cadastrais e ordens judiciais.

Esta última plataforma é também o meio adequado para realização de pesquisas referentes a dados cadastrais e registros telefônicos de linhas não interceptadas. Por meio de consultas relacionadas a IMEIs, linhas e CPFs é possível acessar registros de utilização de aparelho celular e obter registro de ERBs sob as quais o investigado se deslocou.

A régua de pesquisas possíveis no Infoguard dependerá do conteúdo da decisão judicial remetida, sendo, em especial nesta operadora de telefonia, indispensável a exata definição dos meios de pesquisa a serem colocados à disposição da investigação.

VIGIA TIM

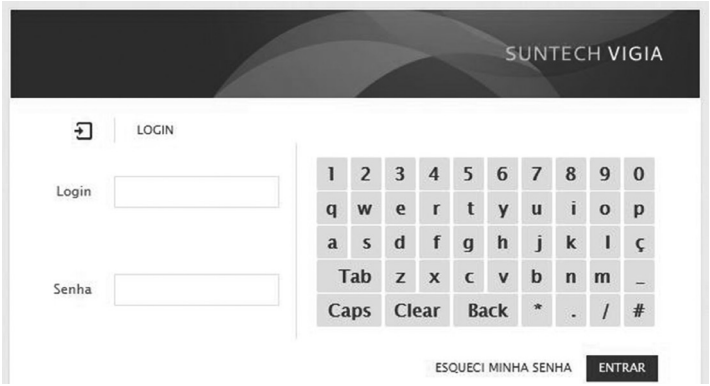

Figura 4 - Interface do Vigia Tim

O Vigia Tim é de funcionamento semelhante ao disponibilizado pela operadora Vivo, contendo, igualmente, a possibilidade de acessar um manual de funcionalidades na aba "ajuda" contida no quanto superior direito da tela.

INFOGUARD TIM

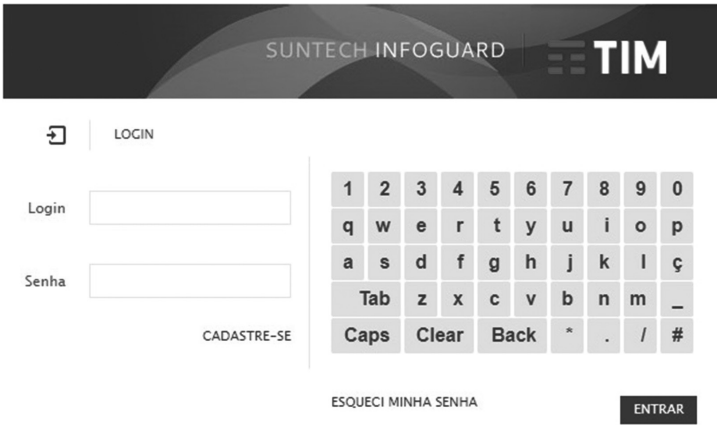

Figura 5 - Infoguard Tim

O Infoguard tem funcionamento semelhante ao Portal Jud Vivo e possui uma aba específica para envio de documentos, substituindo o *e-mail* da operadora para a implementação de interceptação ou ativação de senha autorizativa.

Há também uma aba para realização de "solicitações", isto é, especificação dos termos de pesquisa com remessa de pedido que, em média, é respondido dentro de poucas horas após a requisição. Os arquivos de resposta estarão compactados e necessitarão da inserção da senha composta pela sigla **TBGR** seguida, sem espaço, do **ano** em que é feita a requisição. Ex. TBGR2019.

• OI

Endereços e telefones úteis:

Ações Restritas
Avenida Presidente Vargas, 914, 8º andar, Centro Rio de Janeiro-RJ
Vigia Oi: https://ilc.oiloja.com.br
Telefones: 0800 031 7053
E-mails: pp-acoesrestritasplantao@oi.net.br & qsoi@oi.net.br

A operadora de telefonia Oi utiliza dois sistemas distintos, um para o monitoramento das comunicações telefônicas dos investigados interceptados, a plataforma Vigia, e outro para envio de documentos, obtenção de extratos de chamadas, dados cadastrais e rastreio de estações rádio base de investigados não interceptados junto à operadora.

O acesso aos dados telefônicos de investigado não interceptado junto à operadora se faz por meio de envio de solicitação ao e-mail pp-acoesrestritasplantao@oi.net.br.

SOLICITAÇÕES AO PLANTÃO AÇÕES RESTRITAS

Tal funcionalidade depende de cadastro prévio do operacional. Para tanto, deverá o agente componente da equipe investigativa ligar para o número **0800 031 7053**, digitar opção 3, e solicitar ao atendente um pré-cadastro, fornecendo seu e-mail institucional.

Na sequência, usando o e-mail funcional informado, o operacional deverá enviar um ofício, assinado por seu superior imediato, caso houver, endereçando o documento ao e-mail eletrônico **qsoi@oi.net.br**. Tal correspondência eletrônica deverá ter como assunto **"Cadastro Oi"** seguido de um código que será fornecido pela operadora.

Como conteúdo, tal e-mail deverá conter, em forma de ofício, dados de qualificação profissional e pessoal, incluso telefone celular para contato, de quem solicita acesso. Em até um dia útil, o operacional receberá um e-mail contendo um formulário para preenchimento, e no celular informado, um SMS com o código de validação.

Caso se verifique alguma falha no processo de cadastramento, deverá o servidor manter contato pelo número 0800 031 7053, digitar a opção 2 e solicitar ao atendente nova realização dos procedimentos.

Por procedimento, apenas serão aceitos e-mails institucionais para envio de documentos sigilosos, vedado o uso de e-mails pessoais particulares. Somente será habilitado um usuário para cada e-mail institucional informado.

Uma vez que esteja devidamente cadastrado, o operacional deverá enviar ofício judicial autorizativo ao e-mail **pp-acoesrestritasplantao@oi.net.br**. Tão logo reconhecida e cadastrada a ordem legal, o servidor receberá um código pessoal e intransferível que deverá utilizar para encaminhar, àquele mesmo endereço eletrônico, solicitações que se fizerem necessárias no curso da investigação.