

Histórico, implementação e uso do Sistema Guardiãõ® de interceptação de dados de informática e telemática nas garantias do cidadão

Miguel Ângelo Duarte Ticom

Comissário de Polícia, Diretor-Geral da Busca Eletrônica da Subsecretaria de Inteligência da Secretaria de Estado de Polícia Civil

Wanderson de Freitas Pereira Neto

Perito Criminal Oficial, Doutor em Física de Reatores Nucleares, Coordenador de Pesquisa e Desenvolvimento de Software da Diretoria-Geral de Busca Eletrônica da Subsecretaria de Inteligência da Secretaria de Estado de Polícia Civil

Silde Monteiro de Albuquerque

Oficial de Cartório, Estatístico e Bacharel em Direito, Coordenador da Inteligência de Interceptação de Telefonia e Telemática da Diretoria-Geral de Busca Eletrônica da Subsecretaria de Inteligência da Secretaria de Estado de Polícia Civil

Israel Carbone de Carvalho

Inspetor de Polícia, Economista, Coordenador da Inteligência Cibernética da Diretoria-Geral de Busca Eletrônica da Subsecretaria de Inteligência da Secretaria de Estado de Polícia Civil

Arnaldo Rosa da Silva Jr.

Inspetor de Polícia, Analista de Redes, Coordenador da Inteligência de Fontes Abertas da Diretoria-Geral de Busca Eletrônica da Subsecretaria de Inteligência da Secretaria de Estado de Polícia Civil

Resumo

Este estudo tem como finalidade demonstrar a relevância da interceptação telefônica como meio de obtenção de prova no processo penal, constituindo exceção à tutela constitucional de inviolabilidade ao sigilo das comunicações. Com a elaboração deste trabalho é possível verificar os pontos de maior relevância acerca da interceptação telefônica e a sua operacionalização pela polícia judiciária do estado do Rio de Janeiro, que, atualmente, atravessa uma nova fase, baseada em planejamento estratégico e inteligência policial. Ainda, podemos verificar que por meio das auditorias realizadas no sistema de interceptação telefônica e de dados Guardiãõ®, da empresa nacional Dígito, ficam garantidos o direito do cidadão ao sigilo das comunicações telefônicas previsto na Constituição Federal, no art. 5º, inciso XII, e quaisquer outras violações, além de excepcional, previstos na Lei nº 9.296/1996.

Palavras-chave

Interceptação telefônica, Sistema Guardiãõ®, sigilo telefônico.

As opiniões e análises contidas nos artigos publicados pela revista Cadernos de Segurança Pública são de inteira responsabilidade de seus autores, não representando, necessariamente, a posição do Instituto de Segurança Pública.

Introdução

Interceptação telefônica é o desvio e o acesso a todos os dados gerados por voz oriundos de um terminal telefônico, podendo ser de rádio, linha fixa e/ou móvel. Apesar de a interceptação telefônica ser, de forma usual, denominada como “escuta telefônica”, a seguir verificaremos que são conceitos distintos. A interceptação telefônica pode ser realizada com o conhecimento ou não de um ou de ambos interlocutores, e é hoje um instrumento de acesso a informações que vão protagonizar, em muitas ações jurídicas, o meio principal de prova de fatos ilícitos e delituosos.

A Justiça, que detém a competência exclusiva para o deferimento das interceptações telefônicas, acata a representação da autoridade policial ou do membro do Ministério Público responsável pela investigação quando verificados os requisitos da lei, uma vez que a interceptação telefônica somente é autorizada para a investigação de determinados crimes e em circunstâncias especiais.

Em 2007, por conta dos Jogos Pan-Americanos, a extinta Secretaria de Estado de Segurança do Rio de Janeiro adquiriu o sistema de interceptação telefônica Guardião®. A partir daquele momento o Rio de Janeiro passou a utilizar um sistema técnico e especializado, que inaugurou uma nova era na área da inteligência policial e no combate à criminalidade.

O trabalho com essa nova ferramenta consistiu em um grande desafio para a Polícia Civil do Estado do Rio de Janeiro, uma vez que as interceptações telefônicas eram antes realizadas diretamente pelas unidades de polícia judiciária – delegacias distritais e especializadas – e que naquele momento passaram a ser concentradas na Subsecretaria de Inteligência (SSINTE), que integrava a estrutura da extinta Secretaria de Estado de Segurança do Rio de Janeiro (SESEG). Atualmente, a SSINTE integra a Secretaria de Estado de Polícia Civil¹.

Essa centralização permitiu não somente uma abordagem técnica das interceptações telefônicas, mas também o controle de todas as operações e sua adequação aos limites legais impostos pela Lei nº 9.296/1996², a qual regula o tema.

A interceptação telefônica é tratada na Lei nº 9.296/1996, que veio regulamentar a parte final do inciso XII, do art. 5º da Constituição Federal de 1988, que cuida da quebra do sigilo telefônico e cuja uniformização foi concretizada por meio das resoluções nº 59 e nº 84 editadas pelo Conselho Nacional de Justiça, em 2008 e 2009, respectivamente.

É importante destacar que a interceptação telefônica entrou em uma nova fase com o advento da expansão dos sistemas de telefonia. Na década de 1960 os sistemas de telefonia evoluíram e, mais tarde, com o advento do celular, os meios de comunicação alcançaram um desenvolvimento jamais visto.

Neste mesmo sentido, o crime também evoluiu e, aproveitando toda a tecnologia, os criminosos passaram a utilizar os meios de comunicação

1 - Com o Decreto nº 46.544/2019, de 1º janeiro de 2019, o então governador do estado do Rio de Janeiro, Wilson Witte, recém empossado, extinguiu a Secretaria de Estado de Segurança do Rio de Janeiro, criando assim duas outras secretarias de estado, uma sendo a Secretaria de Estado de Polícia Civil (SEPOL) e a outra sendo a Secretaria de Estado de Polícia Militar (SEPM).

2 - Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/19296.htm>. Último acesso em fevereiro de 2020.

em favor da criminalidade. Atualmente, verifica-se que nenhum crime é cometido sem que haja comunicação, mínima que seja, entre os envolvidos. Não bastasse isso, o crime organizado se utiliza dos meios de comunicação, principalmente os de telefonia, para controlar e comandar ações, mesmo de dentro de presídios.

Assim, por via de consequência, a investigação passou a demandar uma forma mais efetiva de combate às novas modalidades criminosas praticadas com o auxílio dos meios de comunicação, criando a necessidade de regulamentação legal para as ações investigativas nesta seara. Surgiu, então, a necessidade de determinação das hipóteses de incidência que ensejariam a quebra do sigilo constitucionalmente tutelado e as limitações da atuação do poder público, a fim de garantir tanto a efetividade da persecução penal como o respeito aos direitos e garantias dos indivíduos.

Antes da aquisição do Sistema Guardiã® pela Polícia Civil do Estado do Rio de Janeiro, poucas unidades policiais distritais ou especializadas realizavam suas interceptações por meio do uso de computadores que ficavam sob o controle direto da autoridade policial. O trabalho de interceptação de comunicações telefônicas da forma como era realizado pela polícia judiciária não permitia nenhum tipo de controle interno ou externo, bem como não produzia informações para a instituição, pois não havia armazenamento em banco de dados, nem havia a produção de estatísticas que demonstrassem a quantidade de operações realizadas, os alvos sob investigação, ou os resultados obtidos por meio dos desvios.

Assim, o amadorismo e a falta de processos e técnicas na realização das interceptações telefônicas traziam prejuízos para a instituição policial não só no âmbito da investigação criminal em si, mas também em âmbito administrativo, uma vez que a ausência de auditoria e de formação de banco de dados sobre as operações e procedimentos investigativos que envolviam interceptações telefônicas prejudicavam o planejamento e o controle das ações policiais no estado. Sem controle, não havia uma resposta exata, e muito menos rápida, quando dados acerca das interceptações telefônicas eram necessários para pautar qualquer ação institucional de inteligência.

Estas foram, portanto, as principais demandas que exigiram que a Polícia Civil do Estado do Rio de Janeiro desse novo tratamento à questão da interceptação telefônica, iniciando uma busca por excelência, para transformar o trabalho empírico e quase artesanal produzido até então em um processo técnico, composto por diversas etapas, com controle institucional e jurisdicional, com formação de banco de dados, com acesso restrito por senha, com análise de dados e de vínculos e com registros estatísticos, demandando qualificação profissional dos servidores da segurança pública vinculados aos setores de inteligência policial.

Assim, em março de 2007, a SESEG adquiriu o Sistema Guardiã®, que, no âmbito da Polícia Civil, naquele momento, era operado pela Coordenadoria de Inteligência (CINPOL, agora extinta), inaugurando um novo modelo de trabalho para a realização das interceptações telefônicas no estado, que passaram a ser operadas por meio da utilização desta ferramenta,

que não só otimiza o trabalho policial, mas permite a produção legal de meios de prova para garantir a efetividade da persecução penal pelo poder judiciário.

Cabe ressaltar que, no panorama atual da Secretaria de Estado de Polícia Civil do Rio de Janeiro, a CINPOL foi extinta e os servidores que eram lotados nesta coordenadoria foram transferidos para a Subsecretaria de Inteligência (SSINTE) da atual secretaria.

O direito constitucional à inviolabilidade das comunicações e a Lei nº 9.296/1996

Abaixo o trecho da Constituição da República Federativa do Brasil de 1988 sobre os direitos e garantias fundamentais dos cidadãos.

TÍTULO II

Dos Direitos e Garantias Fundamentais

Art. 5º - Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...)

XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Vide Lei nº 9.296, de 1996)³.

Da leitura do texto constitucional acima transcrito, verifica-se que a garantia à inviolabilidade e ao sigilo das comunicações não é absoluta, mas relativa, sendo admitidas exceções legítimas no próprio plano do ordenamento legal.

Tanto quanto a tutela à inviolabilidade e ao sigilo das comunicações telefônicas, o direito fundamental ao contraditório e à ampla defesa, previsto no inciso LV do art. 5º da Constituição Federal, tem pertinência no estudo e na consecução das interceptações telefônicas.

LV - aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, com os meios e recursos a ela inerentes⁴.

Ainda que se trate de diligência possível como exceção constitucional e regulamentação legal, a interceptação telefônica, por sua natureza, corre em sigilo com o total desconhecimento dos alvos investigados, os quais não têm, em princípio, a oportunidade sequer de exercer o contraditório e a ampla defesa durante a sua execução.

³ - Disponível em: <http://www.planalto.gov.br/ccivil_03/constitucao/constitucao.htm>. Último acesso em julho de 2019.

⁴ - *Idem*.

Certo é que o magistrado não pode levar a cabo uma condenação penal baseando seu convencimento nas provas colhidas exclusivamente na fase do inquérito policial. De fato, pelo princípio do livre convencimento motivado, o juiz é livre para apreciar a prova, mas, ao decidir, deve fundamentar sua decisão com base nas provas produzidas nos autos, conforme previsão no art. 93, inciso IX, da Constituição Federal.

Art. 93 - Lei complementar, de iniciativa do Supremo Tribunal Federal, disporá sobre o Estatuto da Magistratura, observados os seguintes princípios: (...)

IX - todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação; (Redação dada pela Emenda Constitucional nº 45, de 2004)⁵.

Por sua vez, sendo a prova o meio pelo qual se demonstra a verdade de algo, é intuitivo que a sua produção carece do contraditório e de ampla defesa, sem os quais há franca violação ao Estado Democrático de Direito e ao consagrado no art. 5º, inciso LV, da Constituição Federal.

Em que pese ser a inquisitorialidade uma das principais características do inquérito, o que afasta a ampla defesa do acusado, é evidente que isso não significa total ausência de direitos e a consideração do acusado como “objeto” da investigação, sendo ele pessoa e, portanto, titular de todos os direitos e garantias assegurados pela Constituição e pelas leis. Entre eles, o de ser considerado, e consequentemente tratado, como inocente até a condenação penal definitiva.

Neste sentido, o fundamento da condenação necessita de demonstração cabal de autoria e materialidade, o que só é alcançável, no Estado Democrático de Direito, mediante o contraditório e a ampla defesa.

Embora a Lei nº 9.296/1996 regulamente a interceptação telefônica, seu art. 1º, parágrafo único, diz que “o disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática”. Ou seja, fica claro que esta lei contempla a interceptação de qualquer tipo de dado, seja ele telefônico ou oriundo de qualquer fonte ou sistema eletrônico, desde que devidamente autorizado, conforme normatizado no trecho transcrito abaixo.

LEI Nº 9.296, DE 24 DE JULHO DE 1996

Regulamenta o inciso XII, parte final, do artigo 5º da Constituição Federal.

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 sigilo de justiça.

5 - *Idem.*

Parágrafo único - O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

Art. 2º - Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:

I - não houver indícios razoáveis da autoria ou participação em infração penal; II - a prova puder ser feita por outros meios disponíveis;

III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção. Parágrafo único - Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.

Art. 3º - A interceptação das comunicações telefônicas poderá ser determinada pelo Juiz, de ofício ou a requerimento:

I - da autoridade policial, na investigação criminal;

II - do representante do Ministério Público, na investigação criminal e na instrução processual penal.

Art. 4º - O pedido de interceptação de comunicação telefônica conterà a demonstração de que a sua realização é necessária à apuração de infração penal, com indicação dos meios a serem empregados (...)º.

Interceptação telefônica, escuta telefônica e gravação clandestina

As interceptações telefônicas legalmente disciplinadas e efetuadas com obediência aos requisitos impostos no ordenamento jurídico são aceitas como provas lícitas, sendo admissível seu resultado como fonte de prova no processo penal. Surge, então, a necessidade de diferenciação entre os institutos da interceptação telefônica, da escuta telefônica e da gravação clandestina, que são frequentemente tratadas com enorme imprecisão, com consequências relevantes, uma vez que desafiam disciplinas legais distintas.

Qualquer interceptação pressupõe, necessariamente, três protagonistas: dois interlocutores e um interceptador, que capta a conversação sem o consentimento daqueles ou com o consentimento de um deles. Quando a captação é feita pelo terceiro por meio de um gravador e entre presentes, estamos diante da interceptação ambiental. Já a escuta telefônica consiste na captação da conversa pelo interceptador quando um dos interlocutores tem conhecimento da interceptação.

Na gravação clandestina ou ilícita há só dois comunicadores, sendo que um deles grava a própria conversa com o outro, telefônica ou não, sem o conhecimento de seu interlocutor. Trata-se de gravação de conversa própria, que, embora não se enquadre na tutela do sigilo das comunicações (art. 5º, inciso XII, da CF), relaciona-se com a proteção à intimidade (art. 5º, inciso X, da CF).

Vale ressaltar que inexistente tipo penal que incrimine a gravação clandestina ou ambiental com base na premissa de que, em um processo de comunicação, tanto o emissor como o receptor são titulares da mensagem, de modo que o sigilo só existe em relação a terceiros, os quais estão liberados para gravar

6 - *Idem.*

o conteúdo da mensagem. Entretanto, a divulgação desta mensagem, sem justa causa, poderá ser considerada ilícita, subsumindo-se a conduta ao tipo previsto no art. 153 do Código Penal, que trata da Divulgação de Segredo.

O Sistema Guardiã[®]

O Sistema Guardiã[®] é um conjunto de *software* e *hardware* fabricado pela empresa Dígito, sediada em Florianópolis, Santa Catarina, que desenvolveu tecnologia própria. É um sistema capaz de realizar interceptação de voz e dados, disponibilizar acessos simultâneos e gravar ao mesmo tempo centenas de ligações, além de oferecer recursos avançados de análise de áudio.

O Guardiã[®] é adquirido pelas polícias estaduais e federal e o Ministério Público de acordo com suas demandas. Cada sistema é dimensionado de acordo com a necessidade de cada cliente, sendo, portanto, flexível e modular, com interface 100% *web*, permitindo ao analista acessar o sistema de qualquer lugar de forma segura, transformando-se hoje na ferramenta de maior utilização no combate ao crime organizado no Brasil.

O Guardiã[®] é um sistema que possibilita o acompanhamento em tempo real de todos os áudios, permitindo a marcação de sua relevância, sendo o acesso às informações condicionado a uma senha. Esta senha é a garantia da auditoria do sistema e permite que todos os profissionais da Subsecretaria de Inteligência (SSINTE) que estiverem diretamente ligados à operação como administradores do sistema tenham acesso aos áudios e dados desviados. Esta senha também é gerada para as autoridades policiais, membros do Ministério Público, juízes, bem como para policiais por eles indicados.

O acesso ao sistema é feito por meio de teclado virtual com utilização de *token* (primeira versão) e as senhas são assinaturas eletrônicas, que garantem a restrição e o controle de acesso. Na versão atual não é feito o uso do *token* para o acesso ao sistema.

Após a autorização judicial, que é a materializada por meio de ofícios dirigidos às operadoras de telefonia, inicia-se a operação, que é o efetivo trabalho de interceptação de alvos, com o cadastramento das linhas telefônicas que serão interceptadas no sistema e seus respectivos desvios.

Os desvios – Discagem Direta Ramal (DDR) – são os números telefônicos que são encaminhados às operadoras de telefonia para que sejam cadastrados junto aos alvos. Para cada alvo existe um desvio, funcionando o Sistema Guardiã[®] como um grande gravador com ferramentas de busca. Portanto, é possível concluir que o Guardiã[®] não intercepta, por si só, as linhas autorizadas judicialmente, tendo em vista a necessidade de efetiva participação das operadoras para que os dados de voz sejam desviados para o sistema e gravados.

Toda a difusão do conhecimento pode ser feita de forma criptografada, sem riscos de ser decifrada, garantindo o acesso somente às pessoas

autorizadas. Assim, o Guardiã® favorece a segurança das informações, com recursos para a realização de auditorias, permitindo que verificações periódicas sejam feitas, com o controle simultâneo de todas as operações efetivadas. Os dados e a voz referentes ao alvo (telefone monitorado) são desviados para o Guardiã®, que procede à gravação e ao armazenamento. Ainda, o sistema gerencia todos os prazos previamente cadastrados no sistema, os alvarás de interceptação emitidos pelos juízes e as DDRs, que significam canais onde os áudios dos alvos são gravados.

O Guardiã® permite auditar todos os acessos e consultas ao sistema. O cadastramento da operação no sistema é seguido de um processo que funciona da seguinte forma: obedece a um processo vinculado à SSINTE, que administra e cria acesso para os servidores autorizados pelas autoridades policiais ou pelos membros do Ministério Público. Desta forma, somente o agente cadastrado consegue visualizar a sua operação.

O Guardiã® também registra os *logs* de acesso, que podem ser solicitados a qualquer momento pela autoridade responsável pela investigação/interceptação. Por fim, é por meio dos *logs* de acesso que a auditoria pode ser realizada.

O Sistema Guardiã® no estado do Rio de Janeiro

As unidades policiais – delegacias distritais e especializadas – faziam as interceptações telefônicas em suas próprias sedes e em equipamentos que, muitas vezes, sequer eram fornecidos pela administração pública para esta finalidade. Entretanto, com a implementação do Sistema Guardiã® a partir de 2007, tornou-se possível a operacionalização técnica das interceptações telefônicas realizadas no âmbito da polícia judiciária do estado, com registro de acesso aos áudios e identificação dos responsáveis pelas gravações, além do controle das operações por meio de senhas, as quais são exigidas para a obtenção do conteúdo dos áudios gravados, que são criptografados e ficam restritos aos servidores responsáveis pelo procedimento de interceptação e pelo judiciário.

A adoção desse sistema pela instituição policial também demandou capacitação dos profissionais lotados na SSINTE, naquela época vinculada à extinta SESEG, assim como daqueles lotados no setor de inteligência da Polícia Civil, uma vez que a nova tecnologia, além de exigir conhecimento da ferramenta, requer constante atualização acerca das modificações periódicas do *software*. Além disso, passou-se a exigir total conhecimento dos limites legais de atuação e das determinações procedimentais para a realização da diligência, de modo a garantir sua finalidade como prova instrutória de investigações criminais, dando subsídios para o oferecimento da denúncia pelo Ministério Público e para a entrega da prestação jurisdicional pelo poder judiciário.

Atualmente, a utilização do Sistema Guardiã® garante o respeito aos direitos individuais, isto porque, como já visto, o sigilo das comunicações

telefônicas tem proteção na Constituição Federal, no art. 5º, inciso XII, e qualquer violação, além de excepcional, sofre limitação legal, neste caso pela Lei nº 9.296/1996.

Portanto, são inibidas todas as formas de acesso e divulgação de áudios, mesmo quando autorizados pela justiça, eis que o vazamento é condenável e passível de punição, tanto na esfera administrativa como na esfera penal. A tutela aos direitos e garantias individuais também é reforçada pelo rígido controle exercido atualmente pelas corregedorias internas e pelo controle externo exercido pelo poder judiciário e pelo Conselho Nacional de Justiça.

A instituição policial, pautada nos princípios que norteiam a administração pública, em especial a legalidade, a moralidade e a eficiência, mantém estreita observância às limitações constitucionais e às determinações legais, principalmente por conta da possibilidade de auditar todos os processos.

O Sistema Guardião® sofre, ainda, dupla conferência, por parte da SSINTE e das operadoras de telefonia, no tocante ao desvio de áudios, uma vez que a interceptação telefônica somente é levada a efeito depois da confirmação das linhas objeto de autorização judicial junto aos responsáveis pelas operações em cada instituição, diminuindo a margem de erro. Isto é feito a fim de evitar a violação da intimidade de um alvo equivocadamente, o que, como já visto, constitui violação de grande gravidade e com consequências institucionais e pessoais.

Considerações finais

Atualmente vivemos um momento em que os setores de inteligência das forças de segurança do estado do Rio de Janeiro vêm norteando as ações estratégicas, por meio da integração de bases e bancos de dados, criando um novo conceito em análise de informações e de atuação policial.

Essa nova visão vem respaldar o processo de substituição gradativa da polícia repressiva pela polícia preventiva, norteada por um conceito de inteligência policial voltado para o estudo da criminalidade, baseada em fontes de dados concretos extraídos da realidade, além de planejamento, estratégias, ações e análise de resultados.

Essa noção vem sendo cada vez mais disseminada entre os órgãos responsáveis pela segurança pública, os quais, mesmo quando diretamente ligados a atividades de repressão e enfrentamento direto do crime, têm sua atuação pautada pela legalidade que funda e mantém o Estado Democrático de Direito.

Uma gestão de segurança pública inspirada na inteligência e na utilização de informações como principal ferramenta de trabalho resulta na prevenção e na antecipação de prováveis ações criminosas, diminuindo índices de criminalidade e os impactos negativos originados pelas políticas de enfrentamento direto. Neste sentido, a modernização tecnológica é imprescindível para o acompanhamento do fenômeno criminal e para o

aparelhamento da sociedade para enfrentar a criminalidade.

A aquisição e a efetiva implantação do Sistema Guardiã® para a operacionalização das interceptações telefônicas realizadas no estado do Rio de Janeiro, por meio da Secretaria de Estado de Polícia Civil, demonstra que o trabalho de investigação pode estar aliado integralmente à legalidade e à transparência, os quais são imprescindíveis para o desempenho positivo da atividade, para o alcance de resultados concretos e para a promoção da tranquilidade e da paz social.

Referências bibliográficas

LIMA, P. A. M. **A interceptação telefônica no tráfico de drogas: técnica de investigação e ausência de defesa.** Dissertação (Mestrado em Direito) – Universidade Federal de Goiás, Goiás, 115 f. 2005.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, [2016]. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Último acesso em julho de 2019.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Último acesso em julho de 2019.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, 77 do art. 5º da Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/19296.htm>. Último acesso em julho de 2019.

GRECO FILHO, V. **Interceptações Telefônicas** – considerações sobre a Lei nº 9.296 de 24 de julho de 1996. 1ª ed., São Paulo: Saraiva, 1996.

LENZA, P. **Direito Constitucional Esquematizado.** 14ª ed., São Paulo: Saraiva, 2010.

