

I. MANUAL DE ATUAÇÃO: INTERCEPTAÇÃO TELEMÁTICA

Na década de 60, nos Estados Unidos da América, começou a ser desenvolvido, com finalidade exclusivamente militar, um sistema de comunicação entre computadores, visando a garantir a possibilidade de coordenar um contra-ataque eficaz contra o inimigo de então, a União Soviética. Com o fim da Guerra Fria, o uso militar daquele projeto perdeu o sentido. Viu-se então o desenvolvimento do que todos nós conhecemos hoje como Internet, provocando significativas mudanças no mundo.

A revolução digital proporcionou maior facilidade de acesso ao universo dos computadores, à Internet e a outras novas tecnologias que surgiram com o avanço das ciências eletrônicas. A acessibilidade a estes novos equipamentos trouxe para a sociedade diversos impactos, principalmente na área do Direito. Antigos conceitos legais tiveram de ser reformulados, revestindo-se de uma roupagem mais moderna, de forma que pudessem se enquadrar à nova realidade. Surgiram também novas situações jurídicas, que exigem dos profissionais do Direito tratamento diferenciado, além de conhecimentos mais específicos sobre as matérias informáticas. É impossível, diante dessa nova realidade, pensar que o Direito possa permanecer estático, ignorando as mudanças que ocorrem no mundo todo.

A Internet é um lugar propenso ao desenvolvimento de fraudes, devido, sobretudo, ao anonimato que oferece aos seus usuários e à “imperfeição” dos programas de computadores utilizados para o acesso a ela e seu desenvolvimento.

Na medida em que os computadores são mais populares, nada mais lógico que haja o aumento da atividade criminal dentro dessa área. A Internet é um paraíso de informações, e, pelo fato de estas serem

riquezas, inevitavelmente atraem o crime. Onde há riqueza há crime. Constatamos a fragilidade dessa riqueza quando percebemos que sinais digitais, representando vastas quantias de dinheiro, podem ser interceptados e “furtados”. Em vez de pistolas automáticas e metralhadoras, os ladrões de banco podem agora usar uma rede de computadores e sofisticados programas para cometer crimes. O risco da empreitada criminosa foi substituído pela praticidade e facilidades concedidas pela Internet.

É necessário que antes de se pensar na edição de normas incriminadoras, que a sociedade como um todo, e os operadores de Direito em especial, volte seus olhos para os princípios gerais que merecem ser alterados diante das mudanças ocorridas no mundo nas últimas décadas.

O rápido crescimento da Internet, aliado ao fato de ela oferecer cada vez mais oportunidades para a aquisição de bens de consumo, evidenciam a potencialidade de materialização de crimes, o que culmina na necessidade da implementação de sua segurança e a de seus usuários.

Por meio da interceptação de e-mails pode-se descobrir a prática de um crime através da Internet, como o estelionato, fraude etc, como também pode servir de apoio para uma investigação criminal, auxiliando na localização do autor de algum crime que esteja foragido. Quando não houver a constatação do crime, as mensagens interceptadas servirão como meio de prova, para o êxito da investigação criminal.

“Interceptar é interromper o curso originário, impedir a passagem, sendo que na lei tem o sentido de captar a comunicação, conhecer seu conteúdo. Interceptar é ter contato com teor da comunicação, não impedindo que ela chegue ao seu destinatário.”¹

^{1,2} ARAÚJO DE CASTRO. Carla Rodrigues. *Crimes de Informática e seus aspectos processuais*. Rio de Janeiro: Editora Lúmen Júris, 2001. Págs. 111 e 112.

“A telemática é uma ciência que trata da manipulação de dados e informações, conjugando o computador, sistemas de informática, com os meios de comunicação, telefônicas ou não. Assim, qualquer comunicação feita através de sistema de informática é protegida pela lei; a título de exemplo, citamos as comunicações feitas na Internet.”²

A interceptação poderá ser feita nas comunicações telemáticas desde que preenchidos os requisitos enumerados na lei nº 9.296/96. Inicialmente, exige-se indícios razoáveis da autoria ou da participação em infração penal, assim, alguma prova deve embasar a medida, podendo ser a oitiva de uma testemunha, um documento etc. O segundo requisito refere-se à ausência de outro modo para demonstrar o fato apurado. A interceptação só será concedida quando for o único meio para provar a conduta delituosa. Por fim, é cabível apenas nos crimes punidos com reclusão.

Com a interceptação, as mensagens do e-mail grampeado são recebidas on-line pelo receptor. Através do grampo, pode-se descobrir o IP do usuário, e conseqüentemente identificar a máquina utilizada para enviar os e-mails. Sabendo qual a máquina utilizada, há como realizar a leitura de seu disco rígido (HD), e desta maneira conhecer os textos e documentos contidos na máquina e que foram enviados e/ou recebidos por e-mail.

Através dos provedores de Internet pode-se obter nos logs de acesso discado: o número do telefone utilizado para realizar a conexão; o tempo de conexão; data e hora de início e término da conexão; o IP (Internet protocol), instrumento para identificar a máquina utilizada.

O armazenamento dos logs pelos provedores é de no mínimo 30 (trinta) dias, e em alguns casos chegam a até 5 (cinco) anos. Trata-se dos documentos enviados e recebidos pelo usuário.

Por intermédio das informações cadastrais do usuário podem ser obtidos o nome do cliente, RG, CPF, endereço completo, telefones para contato e conta de e-mail.

Para os serviços de banda larga oferecidos via tv a cabo, além dos dados cadastrais, pode ser fornecido apenas o IP utilizado. Em relação aos usuários dos serviços de banda larga ADSL, são obtidos apenas os dados cadastrais.

Tendo em vista as diversas e importantes informações que podem ser obtidas através dos provedores, estes se tornam de extrema importância para a investigação criminal. Desta maneira, devem os agentes da justiça requisitar tais informações, que devem ser prontamente fornecidas pelos provedores.

II. PROVEDORES NACIONAIS:

O Ministério Público do Estado de Santa Catarina, considerando a Lei nº 9.296, de 24 de julho de 1996, que regulamentou o art. 5º, inciso XII da Constituição Federal, sobre a interceptação telefônica, requisitou dos provedores nacionais as seguintes informações: Quais são as informações contidas nos logs de acesso? Qual é a política de armazenamento desses logs? (Período armazenado e tipos de dados). Quais são as informações cadastrais requeridas do usuário?

Em resposta foi informado que:

<i>PROVEDORES</i>	<i>RESPOSTA</i>
<ul style="list-style-type: none"> -Formatto Net -Melim Informática LTDA -C&K Consultoria em Informática -New Age Internet -Conect Informática LTDA -Terra 	<p>Login, data de início da conexão, hora de início da conexão, data de término da conexão, hora de término da conexão, tempo que ficou conectado, quantidade de bytes enviados, quantidade de bytes recebidos, telefone que originou a conexão, IP que recebeu na conexão.</p> <p>Código de cadastro, nome do cliente, endereço, bairro, cidade,</p>

	Cep, estado, número do documento, data de cadastro, telefone de contato, plano solicitado, login de acesso, senha de acesso, conta de e-mail.
<p>-Formatto Net *</p> <p>-Melim Informática LTDA **</p> <p>-C&K Consultoria em Informática ***</p> <p>-New Age Internet ****</p> <p>-Conect Informática LTDA *</p> <p>-Terra *****</p>	<p>*Armazenamento por 30 dias nos softwares de origem e por 6 meses em aplicativos próprios.</p> <p>**Em condições normais por, no mínimo, trinta e seis (36) meses.</p> <p>***Tempo de armazenamento em disco e backup será de 05 anos.</p> <p>****Os logs são eliminados mensalmente.</p> <p>*****São armazenados por 12 meses</p>

III. ALGUNS PROVEDORES DE MAIOR UTILIZAÇÃO NO BRASIL:

- *Banco do Brasil:*

Responsável: Marcos Oswaldo Barcellos Chaves

Endereço: Setor Bancário Sul – SBS – Edifício Sede III, 19,
70073-901 – Brasília – DF

Telefone: (61) 310-3547

- *POP:*

Responsável: Adriano Campos

Endereço: caixa Postal, 19556, 80231-970 – Curitiba – PR

Telefone: (41) 3025-2000

- *IBest:*

Responsável: Marco Antônio Gonçalvez

Endereço: Rua Goethe, 06, Botafogo, 22281-020 – Rio de
Janeiro – RJ

Telefone: (21) 2537-3371

- *Click 21 Embratel:*

Responsável: Gerência Click 21

Endereço: Rua Regente Feijó, 166, 14º andar, 20060-060 –
Rio de Janeiro – RJ

Telefone: (21) 2121-8182

- *IG:*

Responsável: Contato Administrativo

Endereço: Rua Amauri, 299, 01448-000 – São Paulo – SP

Telefone: (11) 3065-000

- *BOL:*

Responsável: Victor Fernando Ribeiro

Endereço: Avenida Paulista, 1294, 2º Andar, 01310-915 – São Paulo – SP

Telefone: (11) 3266-3877

- *ITelefônica:*

Responsável: Alexandre Bonfim de Azevedo

Endereço: Avenida Brigadeiro Faria Lima, 3015, 16º andar, 01452-000 – São Paulo – SP

Telefone: (11) 3167-8701

- *Tutopia:*

Responsável: Departamento de Registro de Domínios

Endereço: Avenida das Nações Unidas, 13797, bl 3, 20º andar, 04794-000 – São Paulo – SP

Telefone: (11) 3365-5870

- *Yahoo:*

Responsável: Atendimento ao Usuário

Endereço: Rua Fidêncio Ramos, 195, 12º andar, 04551-010 – São Paulo – SP

Telefone: (11) 3054-5241

- *To Ligado:*

Responsável: Gian Carlo Salvati

Endereço: Rua Lauro Linhares, 2123, sala 307, bl B, 88036-003 – Florianópolis – SC

Telefone: (48) 233-0441

IV. PROVEDOR ESTRANGEIRO:

No caso de o e-mail ser oriundo de provedor estrangeiro, deve-se proceder da seguinte maneira, seguindo o exemplo da empresa provedora de e-mail gratuito, Hotmail (MICROSOFT):

Para a interceptação das mensagens, é necessária a solicitação através de uma ordem específica emanada do Poder Judiciário Norte-Americano, nos termos da legislação daquele país, mais especificamente o *Electronic Communications Privacy Act of 1986*, (legislação que protege os interesses privados de usuários de serviços de comunicação eletrônica).

O Brasil é signatário de um tratado para cooperação judicial (*Mutual Legal Assistance Treaty*), através do qual poderá solicitar tal requisição. O Brasil ainda faz parte do grupo conhecido como *network for computer crime matters* (Rede para Assuntos de Crime de Informática) e, de acordo com o documento firmado entre os países signatários, o contato no Brasil é o setor de Crimes de Informática da Polícia Federal, pelos telefones 55.61.311.9360 e 55.61.311.9383.

Para contatar o serviço do governo norte-americano criado para atender a este tratado deve-se buscar o **Departamento de Justiça (DOJ)**, ligar para os telefones **(1) 202-514-1026 ou 202-514-5000 (CCIPS – Computer Crime and Intellectual Property Section)**. Esse contato é feito pela Polícia Federal.

A despeito de ser o procedimento acima descrito necessário para que se tenha acesso ao conteúdo das mensagens enviadas pelo

Hotmail, a Microsoft Corporation mantém, por prazo limitado, informações sobre os IP logs e o registro dos usuários que utilizam seu serviço. Os referidos dados, em razão do disposto na legislação norte-americana antes citada, podem ser enviados mediante solicitação de autoridades estrangeiras, independente de decisão da justiça daquele país. Entretanto, tais informações devem ser solicitadas por meio de ofício endereçado à **Microsoft Corporation, One Microsoft Way, Redmond, State of Washington, 98052-6399, USA**. Caso haja interesse de em obter tais informações (IP Logs e Registro), o CCR entra em contato com o Departamento Jurídico da Microsoft Informática Ltda. Pelo telefone (11) 5504-2543.

Assim, para a obtenção da interceptação telemática de provedor estrangeiro deve-se seguir os seguintes procedimentos:

Solicitação de Assistência Judiciária em Matéria Penal à Polícia Federal:

- 1) **Destinatário (Para):** Departamento de Justiça dos Estados Unidos da América;
- 2) **Remetente (De):** Secretaria Nacional de Justiça do Ministério da Justiça do Brasil – Autoridade Central;
- 3) **Assunto:** Requerimento de assistência judiciária em matéria penal para Interceptação Telemática em razão de investigação criminal;
- 4) **Referência:** Identificação Nominal do Caso para facilitar sua identificação nos arquivos. (por exemplo: Caso TRT de São Paulo; Caso Nicolau Santos, etc.);
- 5) **Sumário:** Breve resumo dos dados de localização do órgão e autoridade responsável pela condução da investigação, do inquérito policial ou da ação penal em curso, assim como o nº do procedimento, a qualificação completa do(a) investigado(a) e a referência aos dispositivos legais das infrações perpetradas.

- 6) **Fatos:** Narrativa clara, objetiva e completa de todos os fatos, para apresentar o nexo de causalidade entre a investigação em curso, os suspeitos e o pedido de assistência formulado – se já houver denúncia oferecida, deverá ser utilizada como base para a descrição;
- 7) **Transcrição dos dispositivos legais:** Referência e cópia literal e integral dos dispositivos legais previstos em legislação esparsa, infraconstitucional ou constitucional nos quais estejam supostamente incursos os suspeitos ou que embasem o pedido de oitiva de testemunhas, se for este o caso. Finalidade: demonstrar ao país requerido a legislação vigente no país requerente, ou seja, no Brasil;
- 8) **Descrição das assistências solicitadas e rol dos quesitos para sua obtenção:** Informar o tipo de assistência desejada (interceptação telemática), com o nome e endereço completo do(o) réu(ré), e apresentar os quesitos para sua prestação, que devem ser claros e objetivos.
- 9) **Objetivos da Solicitação:** O processo criminal instaurado somente terá andamento uma vez consumada a citação do réu, ato através do qual tomará conhecimento da acusação contra ele (ela) formulada, e mediante o interrogatório judicial do(a) réu (ré), em audiência a ser designada, quando poderá ele (ela) confessar ou negar os crimes que lhe são atribuídos. Na mesma audiência, o (a) réu (ré) deverá indicar, se for da sua vontade, advogado (a) que possa promover sua defesa.
- 10) **Procedimentos a serem observados:** Observações importantes sobre a importância do sigilo, sobre o direito constitucional reservado ao(à) interrogado(a) de permanecer em silêncio durante o interrogatório; entre outras “dicas” relevantes sobre o funcionamento do processo penal brasileiro quanto à obtenção e manuseio das informações e (ou) documentos relativos ao pedido de assistência.

Preenchidas as exigências acima, a Polícia Federal encaminhará aos EUA a solicitação de interceptação nos retornando quando da ordem.

V. MODELOS DE PEÇAS PROCESSUAIS:

- I) Petição inicial de pedido de interceptação telemática
- II) Pedido de interceptação telemática
- III) Pedido de reconsideração de interceptação de e-mail
- IV) Alvará
- V) Pedido de busca e apreensão de computadores (HD) utilizados para o envio das mensagens interceptadas
- VI) Pedido de informações sobre usuários aos provedores

I - Petição Inicial de pedido de interceptação telemática:

EXCELENTÍSSIMO SENHOR DOUTOR JUIZ DE DIREITO DA COMARCA
DE _____.

O MINISTÉRIO PÚBLICO, por seu representante abaixo
subscrito, no uso de suas atribuições constitucionais e institucionais, vem,
com fulcro na Lei nº 9.296, de 24 de julho de 1996, formular o presente
pedido de **INTERCEPTAÇÃO DE COMUNICAÇÕES TELEMÁTICAS**
expondo e ao final requerendo o que segue:

1 - Dos Fatos

Chegou ao conhecimento do Ministério Público, denúncia anônima, bem como documento encaminhado pelo comando da Xª Companhia do XXº Batalhão da Polícia Militar do Estado de SC (docs. anexos), que pessoas estariam associadas nesta cidade e comarca, para o aliciamento de adolescentes, submetendo-os a sessões fotográficas e/ou publicações em cenas de sexo explícito e pornografia, razão pela qual foi requerida a interceptação telefônica de alguns aparelhos móveis e celulares, medida esta já deferida por Vossa Excelência, e que foi realizado pelo Centro de Investigações Especiais do Ministério Público (CIE).

Através de tais interceptações, o CIE constatou a ocorrência do comércio ilícito de entorpecentes na comarca. E, ao que consta, em grande escala, inclusive com ramificação fora do estado e do país.

Verificou o CIE, também, através de tais interceptações telefônicas, que as coordenadas para o efetivo comércio ilegal, com o transporte e entrega do material entorpecente, seria passado por via eletrônica.

Em razão das investigações descobriu-se endereços de e-mail.

Sabe-se que existem vários outros integrantes do grupo, porém ainda não foi possível a identificação de todos.

Assim, diante das evidências da corporação criminosa para a prática de crimes de tráfico de entorpecentes, torna-se necessário levantar as conversações realizadas via e-mail por **nome** através dos endereços eletrônicos ____@____ e ____@____, a fim de se apurar não somente a extensão do empreendimento criminoso, mas as mutantes formas de operação do grupo, motivo pelo qual formula-se este pedido de interceptação telemática dos endereços acima transcritos.

2 - Do Direito

2.1 - Da Lei

É de notório conhecimento que a Constituição Federal preserva a inviolabilidade das comunicações telefônicas, não obstante autorize a interceptação de tais comunicações, quando se tratar de meio para a investigação criminal ou instrução processual penal, *in verbis*:

"Art. 5º [...]

...

*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;***"(grifo não original).

Com efeito, regulamentando este dispositivo constitucional, sobreveio a Lei nº 9.296, de 24 de julho de 1996, que estabeleceu, em seu artigo 1º que “ *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.*

Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática”.
(Original sem grifo).

Do dicionário aurélio extrai-se a seguinte interpretação do significado da palavra telemática: **Verbetes: telemática**

[De tele(comunicação) + (infor)mática.]S. f.

1. Ciência que trata da manipulação e utilização da informação através do uso combinado de computador e meios de telecomunicação.

A interceptação que se pretende, portanto, é perfeitamente possível, uma vez que prevista como uma espécie de interceptação telefônica, mas que se passa por meio de computador, prevista esta hipótese taxativamente no parágrafo único da Lei 9296/96, pois o e-mail nada mais é do que um fluxo de comunicação em sistemas e informática e telemática.

Ademais, o presente pedido preenche os requisitos de admissibilidade do artigo 2º, quais sejam:

"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."

Em contrário senso, verifica-se que os requisitos necessários à concessão da medida são: a) a existência de indícios razoáveis de autoria ou participação em infração penal; b) necessidade da prova a ser obtida através da interceptação; c) a infração penal investigada deve ser punida com reclusão.

O primeiro requisito encontra-se satisfeito consoante documentam os elementos juntados, resultantes de investigações judicialmente deferidas.

No tocante ao segundo inciso, urge ressaltar a impossibilidade probatória por meio diverso da interceptação de telemática de ser descoberta a extensão da rede criminosa, que pode envolver inúmeros indivíduos que têm na comunicação via e-mail o meio de controle das operações de compra e distribuição de drogas, armas e agendamento do extermínio de pessoas “prejudiciais aos seus negócios”.

Quanto ao terceiro inciso, que reclama o apenamento mediante reclusão do crime imputado ao interceptado, não paira qualquer dúvida, vez que a capitulação prevista para o crime de tráfico praticado por organização criminosa, prevê penas de reclusão.

Assim, a pretensão ora formulada amolda-se perfeitamente à previsão legal. Acrescentando-se, ainda, a possibilidade de existência de organização criminosa, incidente os seus autores e partícipes na norma do artigo 288, do Código Penal, crime este punido também com **reclusão**, de 1 a 3 anos.

Portanto, não há óbice algum que impeça a admissão do pedido de interceptação dos seguintes endereços eletrônicos:

- _____@_____
- _____@_____

2.2 - Da Doutrina.

A permissão Constitucional e legal de interceptação das comunicações telefônicas para fins de investigação criminal ou instrução processual penal, evidencia o propósito da sociedade, concretizada pelo legislador, de assegurar os meios necessários ao Judiciário, para a efetiva punição dos delinqüentes, mormente os delitos de grande repercussão social, conhecido como macrocriminalidade.

Neste diapasão, é o escólio do laborioso Lênio Luiz Streck:

"Há que se compreender, no mínimo, que a nova lei se constitui em instrumento destinado a enfrentar, primordialmente, com eficácia, a "pós-modernidade" criminal, representada por crimes do tipo "colarinho branco", etc."

E percucientemente arremata:

"...é perfeitamente razoável afirmarmos que o "legislador", ao excluir apenas os crimes ou infrações penais apenados no máximo com detenção do alcance da Lei, expressou seu desejo - ainda que tardio - de combater a macrocriminalidade, como a sonegação de impostos, a corrupção, etc., e não cinicamente a micricriminalidade..." (In As Interceptações Telefônicas e os Direitos Fundamentais. Ed. Livraria do Advogado. Porto Alegre. 1997. p. 58.).

Ora, a hipótese vislumbrada pelo autor reflete o caso dos autos, posto que na medida que os agentes além de gerenciarem o tráfico de drogas e a distribuição aos usuários pela internet, estão envolvidos com a prática planejada uma grande rede de tráfico de entorpecentes.

Ademais, pela forma como se organizam e continuam atuando, os meios que utilizam e outras características, há evidências de que se trata mesmo de crime organizado, com participação de mais inúmeros autores

delituosos, o que reclama imediata ação da Justiça em prol da segurança da sociedade.

2.3 - Da Jurisprudência

A jurisprudência não discrepa quanto à admissibilidade da prova obtida por meio de interceptação no processo penal.

"Escuta Telefônica. Prova da autoria. A escuta telefônica é expressamente autorizada na CF, art. 5º inc. XII, em casos especiais e deferida pelo Juiz. Preliminar de nulidade rejeitada. Prova da autoria manifesta" (In RJTJRGs 166/52).

E mais:

"PRODUÇÃO DE PROVA CONSISTENTE EM GRAVAÇÃO DE COMUNICAÇÃO TELEFÔNICA – Admissibilidade. Moralmente ilícito é a interferência de terceiro. Cumpre ao Juiz apreciar o valor do documento, se necessário, através de perícia." (TJSP – AI 171.084-1/0 – 1ª CC – Rel. Des. Euclides de Oliveira – J. 24.03.92) (RJ 181/72)

Já no âmbito na Augustina Corte, com o advento da Lei 9.296, de 24 de julho de 1996, regulamentadora do artigo 5º, XII, da Lei Maior, concluiu-se pela legítima possibilidade da prova penal obtida através de interceptação telefônica, quando satisfeitos os requisitos insculpidos no artigo 2.º do referido Diploma Legal.

Neste diapasão:

"Habeas corpus (...) Improcedência da alegação de nulidade do processo em decorrência de escuta telefônica ilegal. Habeas corpus indeferido". (HC-78098 / SC - Relator Ministro MOREIRA ALVES. Publicado

no DJU - Seção 1, de 06-08-99, p. 07 - Julgamento em 01/12/1998 - Primeira Turma Votação: Unânime).

No mesmo sentido: STF: (HC 74.678, 1ª Turma, 10-6-97).

3 - Das Provas

Os documentos que instruem esta petição, apresentados em sigilo diante da gravidade dos fatos demonstram a veracidade de todo o alegado, constituindo suporte probatório bastante para autorizar a admissão a pretensão ministerial.

4 - Do Pedido

Assim sendo, o Ministério Público do Estado de Santa Catarina, requer a Vossa Excelência a expedição de alvará para que possa ser realizada a **interceptação dos e-mails** ____@____ e ____@____, **ambos utilizados por (nome), CPF** _____, **com endereço na Rua** _____ - _____, **nesta Comarca, no prazo de 15 (quinze) dias, renováveis por igual período**, consoante preceitua o artigo 5º da Lei 9.296/96, bem como que **seja determinado ao provedor que informe o conteúdo das comunicações ocorridas nos últimos 30 dias, bem como os IP's de acesso da conta do hotmail, e dos e-mails que entram em contato com esse e-mail, além de eventual uso de outras funcionalidades prestadas pela Microsoft, como o messenger.**

Para cumprimento da decisão, pode-se notificar a Microsoft Informática Ltda, na pessoa de seu responsável no Brasil, _____ no seguinte endereço: Avenida das Nações, 12901 – 27, 28 e 29 andares, Bairro Itaim Bibi – São Paulo – CEP 04.578-000 – telefone (011) 5504-2505.

Nestes Termos,

Espera Deferimento.

_____, ____ de _____ de 200____.

Promotor de Justiça

II – Pedido de interceptação telemática:

Excelentíssimo Senhor Doutor Juiz de Direito da Vara Criminal da Comarca de _____

O Ministério Público, por seu Promotor de Justiça signatário, amparado no art. 127 da Constituição Federal e art. 1º, § único, e 3º, II, da Lei n. 9.296/96, alicerçado nas peças indiciárias extraídas do IP n. _____._____._____-__, requer a Vossa Excelência a decretação da quebra do sigilo do fluxo de comunicações em sistemas de informática e telemática recebidas e geradas através do e-mail _____@_____, bem como a identificação do titular da Caixa Postal _____ – _____ – _____ - _____ - _____ – _____, pelas razões e fatos que passa a expor.

Cuida-se de inquérito policial instaurado em ____ de ____ do corrente, a partir de *notitia criminis* apresentada pela suposta vítima, através da qual imputa a prática de condutas criminosas a **nome** que, atuando no mesmo ramo da vítima, isto é, na _____, vem distribuindo, via internet, a partir do endereço eletrônico _____@_____, mensagens falsas, caluniosas e difamatórias, em formato de revista, as quais distribui aos síndicos e condomínios residenciais da Grande Florianópolis, com a finalidade de desqualificar os serviços prestados pelo seu suposto concorrente, no caso a _____.

Da peça representativa consta, por igual, que o suspeito também teria cometido fatos que, em tese, subsumem-se à conduta paradigmática definidora do crime de extorsão, segundo se infere das declarações colhidas pela autoridade policial e da mensagem eletrônica de fl. ____, e bem assim de concorrência desleal tipificada no art. 195, I, da Lei n. 9279/96, cuja conduta paradigmática tem a seguinte dicção:

“publica, por qualquer meio, falsa afirmação, em detrimento de concorrente, com o fim de obter vantagem.”

Consta que o suposto autor das mensagens criminosas utilizava-se da seguinte caixa postal: _____ - _____ - _____ - _____ E-mail: _____@_____, conforme se infere do documento de fl.____.

Acontece que, orientando a investigação pelos métodos tradicionais, vale dizer, tão-somente com a inquirição de testemunhas, a autoridade policial não logrou identificar o (s) autor (es) dos fatos, daí a sua representação a fl. ____, sugerindo a expedição de ordem judicial, com a finalidade de compelir a Empresa Brasileira de Correios e Telégrafos a fornecer o nome, CPF, Identidade, e o endereço do titular da Caixa Postal acima referida.

Bem de ver-se, pois, que se trata de atuação criminosa perpetrada com o emprego de recursos da telemática, cujo autor (es) mantém-se no anonimato, valendo-se, para tanto, do sigilo constitucional da correspondência e das comunicações telemáticas.

Neste ponto, convém sublinhar que a possibilidade de quebra do sigilo do fluxo de comunicações é perfeitamente possível. De fato, no artigo 1º da Lei n. 9.296/96 o legislador teve o cuidado de prever a

interceptação para comunicações telefônicas **de qualquer natureza**, estendendo a medida expressamente para as comunicações feitas através da informática e telemática.

Na hipótese, tem-se o confronto do interesse público de um lado, e, de outro, a intimidade protegida pelos direitos fundamentais. Aquele, no entanto, deve prevalecer, pois, com efeito, tem Poder Judiciário legítimo interesse de identificar o autor das condutas supostamente criminosas, cuja tarefa lhe cabe com exclusividade como aplicador do Direito Penal, cuja finalidade precípua é a defesa da sociedade em face daqueles que ofendem bens jurídicos relevantes.

A identificação do titular da caixa postal utilizada para enviar matérias de conteúdo falso não acarreta a violação do sigilo da correspondência. É que a autorização judicial visa apenas identificar a pessoa que contratou o serviço com a Empresa Brasileira de Correios e Telégrafos e não o conteúdo da correspondência porventura guardado na referida caixa postal.

No caso em foco, é de se lamentar o fato de a autoridade policial não haver tomado as declarações da testemunha **nome**, cuja inquirição, segundo admitiu no relatório de fls. ____/____, afigura-se de grande relevância para o esclarecimento dos fatos.

Ora, ao exame acurado do caderno indiciário, nele não é possível identificar nenhum ato formal, a indicar a intimação da referida testemunha para depor. Aliás, segundo a sistemática adotada pelo Código de Processo Penal, ressalvadas as hipóteses da dispensa legal (art. 206 e 207), a testemunha não poderá eximir-se da obrigação de depor, sob pena de incidir no crime de falso testemunho previsto no art. 342 do Código Penal.

Neste particular, consta do Auto de Transcrição da fita cassete entregue pela suposta vítima (em anexo), extenso diálogo havido entre o representante legal da vítima e do seu ex-funcionário, cuja gravação ambiental era, segundo aquele, de conhecimento de ambos interlocutores, daí a necessidade de se intimar e inquirir a testemunha em questão que, negando-se a comparecer perante a autoridade policial, poderá dar ensejo à sua condução forçada, mediante ordem judicial.

Assim, à míngua de outros meios de provas capazes de desvendar a autoria dos crimes sob investigação, demonstrado o *fumus boni juri e o periculum in mora* (indispensabilidade da prova), impõe-se seja decretada a quebra do sigilo ora almejado.

Estabelece o art. 129, I, da Constituição Federal, que compete, privativamente, ao Ministério Público, promover a ação penal pública.

Para exercer tão relevante atribuição, a atuação ministerial encontra limites no próprio texto constitucional, sujeitando-se a persecução penal do agente do crime ao devido processo legal, com a observância de princípios como a ampla defesa, o contraditório, a inocência, etc. De outra parte, o próprio processo penal fica subordinado aos princípios da utilidade e efetividade.

Assim, orientando-se pela diretriz constitucional, o legislador ordinário armou o titular da ação penal de ferramentas indispensáveis ao fiel cumprimento de sua destinação constitucional, inserindo-se neste contexto a lei n. 9.296/96, *verbis*:

“Art. 1º A interpretação 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 sigredo de justiça.” (grifei)

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

Por fim, cabe destacar que, em se tratando de repressão de ações criminosas muito provavelmente praticadas por quadrilha ou bando, a Lei n. 9.034/95 prevê expressamente a possibilidade, inclusive por iniciativa do Juízo da causa, de acesso a documentos e informações sigilosas dos acusados, dispondo:

“Art. 2º. Em qualquer fase de persecução criminal que verse sobre ação praticada por organizações criminosas são permitidos, além dos já previstos na lei, os seguintes procedimentos de investigação e formação de provas:

(...)

III - o acesso a dados, documentos e informações fiscais, bancárias, financeiras e eleitorais.”

Ademais, a decretação da medida almejada, tendo-se em conta a reiteração criminosa e as graves conseqüências, inclusive em desfavor de uma plêiade de consumidores, está em perfeita consonância com o princípio da proporcionalidade, assim traduzida por Jellineck, ao acentuar que “O Estado somente pode limitar com legitimidade a liberdade

do indivíduo na medida em que isso for necessário à liberdade e segurança de todos.”

Ante o exposto, com amparo nos art. 1º, § único, e 3º,II, da Lei n.9.296/96 requer-se:

1. seja decretado o sigilo do fluxo de comunicações em sistemas de informática e telemática, mediante oficiamento ao diretor da _____, sediada na _____, requisitando-lhe as seguintes informações, a serem remetidas a este juízo no prazo de 10 (dez) dias.

1.1 – os números do IP’s (internet protocol) de todas as conexões feitas através do seguinte e-mail: _____@_____;

1.2 – nome completo do titular daquele e-mail, informando todos os seus dados cadastrais, como data de nascimento, filiação, Identidade, CPF, endereço completo, etc.

1.3– replicar e remeter a este juízo, no mesmo prazo, todas as mensagens geradas e recebidas pelo e-mail _____@_____;

1.4 - caso não seja a _____ a provedora do e-mail _____@_____, deverá a empresa requisitada informar, por escrito e no mesmo prazo, o nome completo e endereço de quem o seja;

2. oficiar à Empresa Brasileira de Correios e Telégrafos de Florianópolis, requisitando ao seu diretor, no prazo de 5 (cinco) dias, o

nome, CPF, identidade e demais dados cadastrais do titular da caixa postal _____ . Caso tenha havido mudança dos titulares da referida caixa postal, informar a relação de seus usuários desde meados de fevereiro de 2002 até a presente data, indicando as respectivas datas de vigência dos contratos e a qualificação completa dos contratantes.

3. Nos termos do art. 8º da Lei n.9.2296/96, requer-se a autuação do presente pedido em autos apartados.

Termos em que espera deferimento.

_____, ____ de _____ de 200____.

Promotor de Justiça

III – Pedido de reconsideração de interceptação de e-mail:

Autos nº _____._____._____- __/____

MM. Juiz.

Cuida-se de pedido de quebra do fluxo de comunicações em sistemas de informática e telemática aforado pelo Ministério Público em ___ de _____ do corrente, objetivando o acesso a informações protegidas pelo sigilo constitucional, dada a existência de inquérito policial que, lamentavelmente, não logrou esclarecer a prática de diversos delitos imputados a **nome**, notadamente porque as diligências policiais basearam-se exclusivamente na coleta de prova testemunhal, embora estivesse a autoridade policial ciente de que o autor vem empregando métodos sofisticados para atingir os seus objetivos criminosos.

Assim é que, muito embora o procedimento tramitasse paralelamente ao inquérito policial, em ___ de _____ de ____ houve um primeiro despacho deste juízo, determinando a juntada da representação da vítima (fl.____).

Prontamente corrigida a omissão, segundo se infere da promoção de fl. ____, sobreveio novo despacho, desta vez por outro magistrado que, deixando de ingressar no mérito do pedido, pede novas explicações ao Ministério Público, pois, com efeito, somente conseguiu identificar uma única conduta imputada ao suposto autor dos delitos que, pela pena aplicada, ficaria fora da abrangência da Lei n. 9.296/96.

Ora, em que pese constar do 2º e 3º §§ do pedido de quebra a descrição dos fatos objeto da investigação policial, bem como a sua adequação típica às condutas paradigmáticas a que se subsumem, vale dizer, calúnias, difamações e mensagens falsas, que configuram em tese falsidade ideológica, tipificada no art. 299 do CP; extorsão, art. 158 do CP, e, por último, o delito de concorrência desleal, tem-se que o Juiz substituto apegou-se unicamente ao delito de concorrência desleal, talvez porque a conduta correspondente estava transcrita e capitulada.

Como é cediço, o acusado defende-se dos fatos que lhe são imputados e não da capitulação. Além disso, ao juiz é dado conhecer o direito, decorrendo daí que, expostos os fundamentos fáticos e jurídicos, a aplicação da norma, do direito positivo é função do magistrado, traduzida nos aforismos *da mihi factum, dabo tibi jus*” (dá-me os fatos e te darei o direito).

Neste compasso, é importante anotar que o segundo despacho judicial data do dia ____ de _____, tendo o feito permanecido em Cartório por mais 14 (catorze) dias, tempo bem acima do legal e de qualquer juízo de razoabilidade.

Por ser assim, e enfatizando mais uma vez a urgência que o caso requer, dada a reiteração criminosa do suposto autor, recentemente

alvo da grande imprensa televisionada, requer-se a reconsideração do despacho de fls. ____, deferindo a quebra almejada.

_____, ____ de _____ de 200____.

Promotor de Justiça

IV – Alvará Judicial:

ESTADO DE SANTA CATARINA

PODER JUDICIÁRIO

Comarca de _____

_____ Vara

ALVARÁ JUDICIAL – VALIDADE 15 DIAS

O Doutor _____, Juiz de Direito da ____ Vara, da Comarca de _____, na forma da lei, etc.

AUTORIZA a realização de interceptação dos e-mails _____@_____ e _____@_____ ambos utilizados por **nome**, CPF _____, com endereço _____, em _____, pelo prazo de 15 dias, renováveis por mais 15 dias, conforme preceitua o Artigo 5º da Lei 9.296/96, bem como que seja determinado ao provedor que informe o conteúdo das comunicações ocorridas nos últimos 30 dias, bem como os IP

´s de acesso da conta do _____, além de eventual uso de outras funcionalidades prestadas pela _____.

Eu, _____, o digitei, e o subscrevi. Comarca de _____, ____ de _____ de 200____.

Juiz de Direito

V - Pedido de busca e apreensão de computadores (HD) utilizados para o envio das mensagens interceptadas:

EXCELENTÍSSIMO SENHOR JUIZ DE DIREITO DA COMARCA DE _____.

O MINISTÉRIO PÚBLICO DO ESTADO DE SANTA CATARINA, por seu Promotor de Justiça em exercício neste juízo, no uso de suas atribuições institucionais, vem, com fundamento no artigo 242 do Código de Processo Penal, requerer BUSCA E APREENSÃO em face de (nome), residente na Rua _____, n. __, centro, _____/SC, pelas das seguintes razões fático-jurídicas:

Chegou ao conhecimento deste órgão de execução, através de informações obtidas por meio de mensagens eletrônicas interceptadas por ordem judicial que o **nome** estaria envolvido na prática do crime de _____, sendo necessário a apreensão de _____ computadores na residência do mesmo, que contêm em seu disco rígido (HD, mais informações e provas sobre o crime acima mencionado.

Tal conduta, se constatada, pode implicar na configuração do crime descrito no artigo ____ do Código Penal, e deve por isso sujeitar seus responsáveis às penalidades legais.

Perfaz-se, assim, de extrema importância o deferimento da providência acauteladora em questão ainda nesta fase inquisitória, não só à comprovação da materialidade da infração, como também, e precipuamente, para que se possa posteriormente estabelecer a autoria do delito, perquirindo-se a responsabilidade do proprietário dos computadores.

Com efeito, a busca domiciliar, enquanto meio de prova tipificado no Código de Processo Penal, visa assegurar de forma direta a materialidade da infração penal, e diante de sua essencialidade à futura relação jurídico-punitiva, pode ser decretada inclusive na fase das investigações preliminares por requerimento do Ministério Público e até mesmo de ofício (artigo 242 do Código de Processo Penal).

Neste sentido, ensina o mestre Tourinho Filho:

“Insta acentuar que, muito embora as buscas e apreensões possam ser realizadas na fase de instrução criminal, elas se verificam mais amiúde na fase pré-processual, durante o desenrolar da primeira etapa da *persecutio criminis*, vale dizer, durante a feitura do inquérito policial, não só porque a Polícia dispõe de meios rápidos e elementos mais eficazes para assegurar o seu bom êxito, com também porque, de regra, essas diligências se não forem levadas a cabo durante a fase do inquérito perderão a sua oportunidade”.³

De acordo com o artigo 240, §1º, alíneas “d”, “e” e “h”, do Código de Processo Penal, a diligência tem limites claros, e se destina à busca e apreensão, genericamente, de qualquer elemento de

³ TOURINHO FILHO. Fernando da Costa. *Processo Penal*: Vol.. 3. 21 ed. rev. e atual. São Paulo: Editora Saraiva, 1999. Pág. 352.

convicção à futura ação penal, mormente quando se trata, como no presente caso, de instrumentos da infração penal, importantes à sua comprovação em juízo.

Em face do exposto, REQUER este órgão de execução seja determinada a BUSCA E APREENSÃO de todos os computadores presentes na residência do requerido _____, no endereço supra mencionado, com a observância das cautelas, em sua execução, previstas no artigo 245 do Código de Processo Penal e no inciso XI, do artigo 5º, da Constituição Federal.

_____, ____ de _____ de 200 ____.

Promotor de Justiça

VI - Pedido de informações sobre usuários aos provedores:

Senhor Representante Legal,

O Ministério Público do Estado de Santa Catarina, por seu Promotor de Justiça firmatário, no uso de suas atribuições constitucionais estabelecidas no art. 129 da Constituição Federal, assim como no art. 26, I, “b” da Lei 8.625/93 e art. 83, I, “b”, da Lei Complementar nº 197/2000;

Considerando que a Lei nº 9.296, de 24 de julho de 1996, regulamentando o art. 5º, inciso XII da Constituição Federal, regulamentando a interceptação telefônica, disciplinou expressamente no parágrafo único de seu artigo 1º que o disposto na referida Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática; e

Considerando a possibilidade de implementação de mecanismos que possibilitem o controle, repressão e combate à criminalidade, requisita o envio, no prazo de 10 dias a partir do recebimento deste, das seguintes informações, referentes ao cliente do e-mail _____@_____:

1. Nome completo, endereço completo, CPF, RG e telefones para contato;
2. Número do IP nos dias _____, telefone que originou a conexão, data e hora de início e término da conexão nos dias _____;

3. Logs do cliente entre os dias _____ e _____.

Atenciosamente,

Promotor de Justiça