GUIDO ÍCARO FRITSCH

A PRÁTICA PROCESSUAL NO DIREITO CIBERNÉTICO

www.crimesinternet.com.br

Monografia final do Curso de Graduação em Direito objetivando a aprovação no componente curricular Monografia.
UNIJUI - Universidade Regional do Noroeste do Estado do Rio Grande do Sul.
DEJ - Departamento de Estudos Jurídicos.

Orientador (a): BUSNELLO, César.

Ijuí (RS)
2012

Dedico este trabalho a todos que de uma forma ou outra me auxiliaram e ampararam-me durante estes anos da minha caminhada acadêmica.

AGRADECIMENTOS

A Deus, acima de tudo, pela vida, força e coragem.

A meu orientador tal e tal pela sua dedicação e disponibilidade.

A todos que colaboraram de uma maneira ou outra durante a trajetória de construção deste trabalho, minha muito obrigada!

“Se ler será um prazer, se não ler será um favor.”

Autor Desconhecido

RESUMO

O presente trabalho orienta na prática como proceder diante de atos ilícitos praticados com uso da internet. São toneladas de materiais sintetizados com enfoque simples, claro e objetivo. O conteúdo orienta como: Investigar e coletar evidências em websites, blogs, e-mails, redes sociais, e outros meios eletrônicos; Preservar e conferir validade jurídica às provas obtidas na internet; Localizar o autor do delito e responsável por websites, blogs, e-mails, perfis em rede sociais; Rastrear o numero de IP; Procedimentos junto aos provedores como notificações e quebra do sigilo telemático, incluído modelo de peças; Competência territorial e jurisdicional no ciberespaço; Atribuir responsabilidade civil aos provedores na internet. E demais procedimentos inerentes da prática forense.

Palavras-chave: Cyber Crime. Direito Eletrônico e Tecnologia da Informação. Coleta de Provas na Internet. PL2126/11.Comentários ao Marco Civil da internet. Preservar e Dar Validade Jurídica às Provas Obtidas na Internet Aspectos Jurídicos na Internet. Informática Jurídica. Direito Digital. Forense Digital. Delitos Informáticos. Crimes Praticados por Meios Eletrônicos. Manual Prático de Direito Cibernético. Como Atribuir Responsabilidade Civil a Provedores na Internet. Competência Territorial e Jurisdicional em Crimes Praticados por Meio da Internet. Localizar o Autor do Delito e Responsável por Websites, Blogs, E-mails, Perfis em Rede Sociais. Rastreamento do Numero de IP. Procedimentos Junto aos Provedores como Notificações e Quebra do Sigilo Telemático.

ABSTRACT

The present study guides in practice how to proceed in the face of unlawful acts committed with the use of the internet. Are tons of materials synthesized with simple, clear and objective approach. Content guides as: Investigate and collect evidence on websites, blogs, emails, social networking, and other electronic media; Preserve and give legal validity to the evidence obtained on the internet; Locate the offender responsible for websites, blogs, emails, social networking profiles; Trace the IP number; Procedures with the providers as telematic notifications and breaking confidentiality, included parts model; Territorial and jurisdictional competence in cyberspace; Assign liability to providers on the internet. And other procedures involved in forensic practice.

Keywords: Cyber Crime. Electronic and information technology law. Collecting Evidence on the Internet. PL2126/11. Marco Civil da internet. Preserve and Give legal validity to evidence obtained in Internet legal issues on the Internet. Legal Informatics. Digital Law. Digital Forensics. Computer Crimes. Crimes committed by electronic means. Practical Manual of Cyber Law. How to assign Liability to Providers on the Internet. Territorial and jurisdictional competence in Crimes committed through the Internet. Locate the offender responsible for Websites, Blogs, Emails, Social Networking Profiles. Tracking of IP number. Procedures with the Providers as Telematic notifications and breaking Confidentiality.

SUMARIO

INTRODUÇÃO

Este trabalho é uma tentativa modesta de orientar na prática como proceder diante de atos ilícitos praticados por intermédio da internet. Aborda o tema de forma sintética e clara, para que pessoas sem pleno conhecimento da matéria possam tomar providências.

Menciona, em um primeiro momento, como coletar as evidências na internet, como manter preservadas e atribuir validade jurídica às provas obtidas na internet, com o intuito de serem apresentadas futuramente em juízo sem problemas.

Faz referencia a notificação previa dos provedores que tem o condão de retirar conteúdo do ar, resguardar as evidências, atribuir responsabilidade solidaria do provedor pelo dano e condenação ao pagamento de custas processuais em uma futura ação judicial.

Expõe como identificar o responsável pelo conteúdo de um *site*, e-mail ou qualquer aplicação de internet, como entrar em contato com o provedor, descobrir seu endereço físico, a fim de requerer os registros de acesso aplicações de internet.

Alude ainda, como identificar o provedor de acesso responsável pelo endereço IP na conexão à internet, a fim de requerer os registros de conexão e subsequentemente obter informações referentes ao usuário vinculado a determinado endereço IP.

Por fim, traz conhecimentos atinentes à competência territorial e jurisdicional no ciberespaço e anexos com modelos de peças e endereços uteis de delegacias e demais entidades que por ventura sejam necessárias entrar em contato.

O roteiro do procedimento adotado em caso de litígios por intermédio da internet é basicamente assim:

Ato ilícito

Identificação dos meios/ análise dos fatos/ coleta de evidências

Necessária Ata Notarial?

Fato Crime

Sim

Não

Boletim de ocorrência

Ata Notarial

Medidas judiciais e extrajudiciais preliminares

Notificação do provedor (retirada do conteúdo do serviço, preservação das provas)	**Cautelar para guarda e coleta de dados ou busca e apreensão**

Medidas judiciais

Justiça Civil

Justiça Criminal

Justiça Trabalhista

1 COLETA E VALIDADE JURÍDICA DAS PROVAS

A produção de provas, em um processo cujo litígio foi instaurado através da internet, é algo novo para nossos tribunais. Este capítulo tem a finalidade de nortear práticas forenses na coleta e apresentação das evidências digitais com validade probatória em juízo.

Tendo em vista que a fase de instrução do processo, ou seja, quando as provas serão colhidas para comprovar a existência do fato é uma etapa fundamental para influenciar o convencimento do magistrado.

1.1 Investigando e coletando evidencias na internet

Os crimes e danos cometidos no ambiente virtual são semelhantes aos cometidos no mundo real, ou seja, deixam "rastros" vestígios. Ao longo desse capitulo serão expostas técnicas para investigar e coletar evidências no ambiente digital.

As evidências possuem algumas caraterísticas peculiares elas são voláteis podem ser apagadas, alteradas, perdidas facilmente, por isso se faz necessário agir com extrema urgência, com algumas medidas cautelares.

Por obvio, nossa legislação contempla inúmeras formas de prova, contudo aqui serão exibidas formas de prova irrefutáveis e simples que estão sendo usadas na prática com sucesso. A fim de garantir maior celeridade e economia processual.

"Há outras possibilidades de prova também, como solicitar ao provedor que veja, pelo seu histórico, se aquele tipo de informação estava no ar ou não. O provedor consegue descobrir isso **mesmo se o site retirar a informação do ar**." (PINHEIRO, 2006, grifo nosso).

Além das provas que confirmam o fato, a evidência mais importante é o **endereço IP (***Internet Protocol*). Basicamente é uma identificação que todo computador que acessa a rede recebe em cada conexão. **O endereço IP deve estar acompanhado da data de comunicação e o horário indicando o fuso horário utilizado - UTC ou GMT.**

Esses dados são imprescindíveis para futuramente efetuar a requisição judicial dos registros junto aos provedores de serviço e provedores de acesso a fim de obter dados do usuário, e assim, tentar identificar o autor do ato ilícito.

É importante salientar que o apropriado é buscar imediatamente o auxilio de um perito ou advogado especializado para dar auxilio, no entanto, diante da volatilidade das evidências determinadas providências podem e devem ser prontamente tomadas.

1.1.1 Websites/blogs/redes sociais (aplicações de internet)

No presente titulo será exposto como coletar evidências de forma solida e irrefutável em Websites/blogs/redes sociais, chamados de provedores de serviços ou aplicações de internet pelo PL 2126/11.

"VII – aplicações de Internet: conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet;". (BRASIL, 2011, Art. 5°, VII).

O Ministério Público Federal (2006, p. 18) aponta que somente o endereço URL (exemplo: www.sitelivro.com.br) não é suficiente para iniciar uma investigação, pois, como exposto anteriormente, as evidências eletrônicas são voláteis e podem ser apagadas ou modificadas a qualquer tempo.

Portanto, deve-se, providenciar rapidamente a impressão do *website* ou, melhor ainda, o *download* de seu conteúdo**. Lembrando que a impressão deve ser feita por um tabelião, com a respectiva ata notarial para que tenham validade jurídica.**

De nada adianta você mesmo capturar a imagem da tela "***Print Screen***" ou imprimir o conteúdo do *website* e anexar no processo, dessa maneira não terá validade, pois podem ser facilmente adulteradas e por consequência serão impugnadas pela defesa.

Com exceção das tecnologias que garantem validade jurídica a documentos eletrônicos, um exemplo é o Certificado Digital ou Assinatura Digital.

> **Validade Jurídica -** Garantida pelo artigo 10 da MP nº 2.200-2, que instituiu a Infraestrutura de Chaves Públicas Brasileiras - ICP-Brasil, conferindo presunção de veracidade jurídica em relação aos signatários nas declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil. (PORTAL NACIONAL DO DOCUMENTO ELETRÔNICO, 2012).

As demais provas documentais precisam estar amparadas com instrumentos que lhe deem presunção de veracidade. Para maior esclarecimento veja abaixo o trecho de uma entrevista, realizada pela revista Consultor Jurídico a advogada Patrícia Peck Pinheiro, especialista em Direito Digital.

> **ConJur** — Como são produzidas as provas do crime no mundo virtual? A impressão da página de uma comunidade racista do Orkut, por exemplo, é considerada prova?
> **Patrícia Peck** — A impressão é uma evidência. Tem de ser feita a ata notarial no cartório de notas **[o cartório faz um relatório do site, imprime a página e o código fonte]** para a prova ser inequívoca. A mera impressão do site é evidência para um boletim de ocorrência, mas pode não ser suficiente para sustentar uma condenação. Há outras possibilidades de prova também, como solicitar ao provedor que veja, pelo seu histórico, se aquele tipo de informação estava no ar ou não. O provedor consegue descobrir isso mesmo se o site retirar a informação do ar. A Justiça pode pedir acesso aos dados de IP das pessoas que acessaram a informação. A capacidade de perícia no ambiente eletrônico é muito grande, mas o momento da coleta da prova é importante porque é nessa hora que ela pode ser preparada para ter maior ou menor força jurídica. (PINHEIRO, 2006, grifo nosso).

Segundo o Ministério Público Federal (2006, p. 19) existem aplicativos que permitem salvar o conteúdo de um *site* inteiro, feito o *download* podem ser os arquivos encaminhados para o órgão competente através de e - mail ou um dispositivo móvel de memória como Pen Drive.

Menciona também o Ministério Público Federal (2006, p. 20) que se possível seja encaminhadas em um dispositivo não regravável (CD-R), para garantir a autenticidade das evidências (Esses *softwares* abaixo estão especificados em um tópico especifico).

Um exemplo de software capaz de fazer o download total de um site é o *HTTrack*, que também gera um arquivo de *log* (hts_log) registrando a data , hora e endereço do site salvo. Essas informações serão importantes para definir o tempo do crime.

Também existe para outros sistemas operacionais (exemplo: Linux) o software livre *Wget.* O programa Gwget serve de interface gráfica para o Wget. As informações acima são provenientes do Ministério Público Federal (2006, p. 19).

1.1.2 E-mails

Segundo o Ministério Público Federal (2006, p. 28) quando a evidência for um e-mail é preciso, além de preservar o conteúdo da mensagem aparente e anexo, **identificar o cabeçalho do e-mail,** ou seja**,** a parte que informa os dados do remetente e destinatário.

Imprimir e salvar o cabeçalho, para obter informações relevantes como o **endereço IP, data e hora da transmissão e a referencia à hora GMT.** Para obter o cabeçalho do e-mail nos webmails mais populares estão abaixo uma serie de passos. De acordo com o site Crimes pela Internet (2011).

> Webmails:
> **Gmail**
> • Acesse a sua conta do Gmail.
> • Abra a mensagem com os cabeçalhos que você deseja visualizar.
> • Clique na seta para baixo próxima a Responder, no canto superior direito da mensagem.
> • Selecione Mostrar original.
> Os cabeçalhos completos serão exibidos em uma nova janela.
> **Hotmail**
> • Faça login na sua conta do Hotmail.
> • Selecione Caixa de Entrada no menu à esquerda.
> • Clique com o botão direito do mouse na mensagem cujos cabeçalhos você deseja visualizar e selecione Exibir código-fonte da mensagem.
> Os cabeçalhos completos serão exibidos em uma nova janela.
> **Yahoo!**
> • Faça login na sua conta de e-mail do Yahoo!
> • Selecione a mensagem cujos cabeçalhos você deseja visualizar.
> • Clique no menu suspenso Ações e selecione Exibir cabeçalho completo.
> Os cabeçalhos completos serão exibidos em uma nova janela.
> Gerenciadores de e-mails locais:
> **Mozilla**
> • Abra o Mozilla.
> • Abra a mensagem com os cabeçalhos que você deseja visualizar.
> • Clique no menu View (Exibir) e selecione Message Source (Origem da mensagem).
> Os cabeçalhos completos serão exibidos em uma nova janela.
> **Outlook**
> • Abra o Outlook.

- Abra uma mensagem.
- Na guia Mensagem, no grupo Opções, clique na imagem do ícone Iniciador de Caixa de Diálogo.
- Na caixa de diálogo Opções de Mensagem, os cabeçalhos aparecem na caixa Cabeçalhos de Internet.

Em versões anteriores do Outlook:

1. Abra o Outlook.
2. Abra a mensagem com os cabeçalhos que você deseja visualizar.
3. Clique no menu Exibir e selecione Opções….

Os cabeçalhos completos serão exibidos em uma nova janela.

Outlook Express

- Abra o Outlook Express.
- Da sua caixa de entrada, localize a mensagem com os cabeçalhos que deseja visualizar.
- Clique com o botão direito do mouse na mensagem e selecione Propriedades.
- Abra a guia Detalhes na caixa de diálogo.

Os cabeçalhos completos serão exibidos na caixa de diálogo.

Opera

- Abra o Opera.
- Clique na mensagem com os cabeçalhos deseja visualizar para que sejam exibidos na janela abaixo da caixa de entrada.
- Clique em Exibir todos os cabeçalhos do lado oposto do campo Para.

Os cabeçalhos completos serão exibidos na janela a seguir.

IncrediMail

- Abra o IncrediMail.
- Usando sua caixa de entrada, localize a mensagem com os cabeçalhos que deseja visualizar.
- Clique com o botão direito do mouse na mensagem e selecione Propriedades.
- Abra a guia Detalhes na caixa de diálogo.

Os cabeçalhos completos serão exibidos na caixa de diálogo.

Veja abaixo no capitulo “2.4 Localizando o responsável por um e-mail” como analisar o cabeçalho (*header*) de um e-mail segundo o Ministério Público Federal (2006, p. 29).

> **7 - Vou encaminhar os e-mails difamatórios que recebi à Policia e ao perito digital. Estou correto?**
> Não! Ao encaminhar o e-mail de um crime na Internet você simplesmente está destruindo evidências sobrescrevendo o header (cabeçalho) da mensagem original por tags do seu provedor de e-mail SMTP. Recomenda-se efetivamente salvar o arquivo do e-mail (.eml) ou semelhantes ou até mesmo permitir ao perito a coleta do arquivo de banco de dados dos e-mails (.dbx, .pst ou similares). (MILAGRE, 2011).

Caso não exista a opção de visualizar o cabeçalho no seu serviço de e-mail procure um profissional na área para te ajudar.

1.2 Preservando e dando validade jurídica as evidências

No capitulo antecedente foram expostos meios de coletar as evidencias eletrônicas. Nesse capitulo veremos formas adequadas de preservar e dar validade jurídica às evidências para que possam ser apresentadas em juízo e evitar que sejam futuramente impugnadas pela outra parte.

1.2.1 Ata Notarial

Atualmente a Ata Notarial é um poderoso meio de preservar e atribuir validade jurídica a evidências voláteis e dinâmicas, perfeita para provar fatos ocorridos na internet, atribuindo-lhes fé pública para ter valor de prova em um processo.

"A escritura pública, lavrada em notas de tabelião, é documento dotado de fé pública, fazendo prova plena". (Código Civil, Art. 215).

"O documento público faz prova não só da sua formação, mas também dos fatos que o escrivão, o tabelião, ou o funcionário declarar que ocorreram em sua presença". (Código de Processo Civil, Art. 364).

"Não dependem de prova os fatos: (…) em cujo favor milita presunção legal de existência ou de veracidade". (Código de Processo Civil, Art. 334, IV).

Veja o conceito de Ata notarial segundo a Wikipédia (2012, grifo nosso)

> Ata notarial é um ato notarial por meio do qual o tabelião – a pedido de parte interessada – lavra um instrumento público formalizado pela narrativa fiel de tudo aquilo que verificou por seus próprios sentidos sem emissão de opinião, juízo de valor ou conclusão, **servindo a mesma de prova pré-constituída** para utilização nas esferas judicial, extrajudicial e administrativa, de modo que a verdade (juris tantum) dos fatos ali constatados, só pode ser atacada por incidente de falsidade através de sentença transitada em julgado.

Além da finalidade probatória serve também para dar celeridade ao processo, em vez de pericias morosas e custosas, podemos optar pela Ata notarial como meio prático para agilizar e reduzir o custo do processo.

A Ata Notarial comprova vários fatos na internet, abaixo estão alguns fatos autenticáveis, que os advogados e cidadãos podem se utilizar. Segundo a Wikipédia (2012):

> Alguns fatos autenticáveis, que os advogados e cidadãos podem se utilizar:
> - Diálogo telefônico em sistema de viva-voz;
> - Acontecimentos na Internet;
> - Uso e disponibilização indevida de música (MP3);
> - Existência de mensagens eletrônicas (e-mails, sms);
> - Transmissão e exibição de programa televisivo;
> - Existência de projeto sigiloso e atribuição de autoria (propriedade industrial);
> - Existência de documentários, filmes, propaganda, programas de computador e atribuição de autoria (propriedade intelectual);
> - Cópia e transferência de dados entre disco rígido (HD) como geração de hash;
> - Existência de arquivos eletrônicos;
> - Compra de produto em estabelecimento comercial, etc.

Podemos citar mais alguns fatos autenticáveis por meio da ata notarial. Segundo Crimes pela internet (2011):

> A ata notarial comprova inúmeros fatos na internet, dentre eles:
> - Prova o conteúdo divulgado em páginas da internet.
> - Prova o conteúdo da mensagem e o IP emissor.
> - Textos que contenham calúnia, injúria e/ou difamação;
> - Uso indevido de imagens, textos [livros], filmes, logotipos, marcas, nomes empresariais, músicas e infrações ao direito autoral e intelectual;
> - Concorrência desleal;
> - Consulta em páginas de busca;
> - Comunidades on-line que conecta pessoas através de uma rede de amigos;
> - Consulta do CPF no sítio da receita federal, etc.

Tanto no meio tangível com intangível, o tabelião relata fielmente tudo aquilo que presenciou. E o mais importante, além de certificar à veracidade e autenticidade, fixa a data e hora em que foi verificado o fato.

Por fim, constatamos que este importante ato, que pode ser obtido em qualquer Tabelionato de notas conforme dispõe o art. 6º e 7º da Lei Federal 8935/94, com o manto do art. 236 da Constituição Federal, é um importante aliado para resguardar direitos.

1.2.2 Softwares

Além da Ata Notarial existem outros meios para garantir a autenticidade e integridade de evidências eletrônicas. Quando não é possível armazenar os arquivos em mídia **não regravável** (CD-R) é importante que se faça uso de programas que garanta a integridade dos dados.

Segundo o Ministério Público Federal (2006, p. 20), *o MD5Sum7* é um exemplo de aplicativo que garante a integridade dos dados. Tecnicamente cria uma assinatura em forma de arquivo no momento da gravação, evitando que os dados que foram gravados no momento da produção da prova sofram alguma adulteração no trâmite do processo.

Como utilizar o aplicativo segundo o Ministério Público Federal (2006, p. 21)

> Como utilizar o MD5Sum?
> 1. Compacte seus arquivos para gerar somente um arquivo .ZIP (é mais fácil gerar a assinatura de um só arquivo do que de todos);
> 2. Rode o programa MD5Sum para esta cópia gerada;
> 3. Mande a cópia de seu arquivo zipado, junto com este arquivo adicional criado (assinatura) com extensão .MD5.
> 4. Com este arquivo (assinatura) o receptor de seu arquivo poderá a qualquer momento rodar o MD5Sum no arquivo recebido e comparar as assinaturas, se forem iguais, o arquivo é autêntico.

Existem outros programas responsáveis por funções semelhantes e até mais sofisticadas que o mencionado acima pode ser encontrado em materiais relacionados à perícia forense computacional, além disso, com a evolução frenética da computação no momento que você esta lendo isso pode ter sido inventado um programa superior aos que existem.

1.2.3 Boletim de Ocorrência

Lavrar Boletim de Ocorrência, de preferencialmente em uma Delegacia especializada, é um procedimento indispensável em caso de crimes cometidos por intermédio da internet. Até porque, como todos já sabem a autoridade policial que vai descobrir a autoria do crime.

Somente a titulo informativo serão expostas aqui algumas ciências a respeito.

> A vítima deve procurar uma Delegacia de Polícia e se no local existir computador com acesso a internet, solicitar que o escrivão de polícia visualize o conteúdo das ofensas e imprima as mesmas. Em seguida é necessário que o escrivão, **em razão de ter fé pública**, elabore uma certidão com os endereços que foram acessados (no caso de conteúdo ofensivo disponibilizado em sites ou redes sociais) e imprima cópia do conteúdo acessado.
> Se a ofensa estiver armazenada no e-mail da vítima o correto é que ela acesse o e-mail diante do escrivão de polícia, que deverá promover a impressão do conteúdo criminoso, não se esquecendo de clicar em ver cabeçalho completo (ou exibir código fonte da mensagem). Em seguida o referido policial civil deve elaborar certidão sobre o fato. Caso outro policial civil realize esta atividade ao final deverá elaborar um documento informando ao delegado de polícia os procedimentos adotados. Por exemplo, caso o policial seja um investigador de polícia ou outro funcionário que trabalhe diretamente com as atividades investigativas deverá elaborar um relatório de investigação.
> Também é possível registrar uma ata notarial em um cartório de notas. Nestes casos, o cartorário acessa e imprime o conteúdo ofensivo, nos mesmos moldes do escrivão de polícia, pois ambos possuem fé pública.
> Outro caminho que pode ser utilizado, caso não seja possível realizar as sugestões acima apresentadas, é que a própria vítima grave as informações em uma mídia não regravável e também as imprima e entregue na Delegacia de Polícia quando for elaborar o Boletim de Ocorrência. Nesta impressão deve constar o endereço (ou URL) aonde o conteúdo foi divulgado e nos casos de e-mails, o cabeçalho completo, além do conteúdo. Nos casos de ofensas em salas de bate papo os procedimentos são semelhantes, sendo necessário individualizar o nome da sala, seu endereço na internet e os nicknames envolvidos. Existem programas de computadores confiáveis e gratuitos capazes de permitir que o site seja integralmente copiado e que se constate a sua autenticidade, como por exemplo, o HTTrack Website Copier (cópia do site) e o Home of the MD5summer (verifica a integridade do arquivo). (JORGE, 2011, grifo nosso).

Soube de um caso em que foram postadas no *Facebook* informações com teor calunioso. A vítima procurou uma Delegacia de Policia e acessou com seu *notbook* a rede social e exibiu as ofensas, segundo a mesma que é advogada, foi lavrado flagrante da conduta do ofensor. Na sequencia foi encaminhado o inquérito até uma Delegacia especializada.

1.2.4 Busca e apreensão de computadores

Busca e apreensão de computadores, dispositivos de armazenamento de dados digitais e outros equipamentos, são uma excelente forma de comprovar a autoria e materialidade em crimes e demais atos antijurídicos.

A busca e apreensão esta arrolada no capitulo das provas, mas também pode ser utilizada como medida cautelar, estando presentes os requisitos de *periculum in mora* e *fumus boni iuris.* Conforme os art. 839 até 843 do Código de Processo Civil e também art. 13 da Lei do Software (lei 9.609/98).

Ela deve ser solicitada com cautela, mas quando é o único meio de prova deve ser providenciada rapidamente para que não ocorra a perda das evidências, devido à volatilidade das mesmas como explicado anteriormente.

Os art. 6° e 240 até 250 do Código de Processo Penal também ventila a busca e apreensão como medida imprescindível para que não desapareçam as provas do crime e relaciona as peculiaridades da busca e apreensão.

> **Art. 6º** - Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:
> I - dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais;
> II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais;
> III - colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias;
> (BRASIL. Decreto Lei nº 2.848 de 07 de Dezembro de 1940).
>
> **Art. 243** - O mandado de busca deverá:
> I - indicar, o mais precisamente possível, a casa em que será realizada a diligência e o nome do respectivo proprietário ou morador; ou, no caso de busca pessoal, o nome da pessoa que terá de sofrê-la ou os sinais que a identifiquem;
> II - mencionar o motivo e os fins da diligência;
> III - ser subscrito pelo escrivão e assinado pela autoridade que o fizer expedir.
> (BRASIL. Decreto Lei nº 2.848 de 07 de Dezembro de 1940).

Mais adiante nos próximos capítulos, será exposto como "I - indicar, o mais precisamente possível, a casa em que será realizada a diligência e o nome do respectivo proprietário ou morador; [...]" (BRASIL. Decreto Lei nº 2.848 de 07 de Dezembro de 1940).

Por enquanto vamos se concentrar nos detalhes da busca e apreensão. Leia com atenção as valiosas informações que o ilustre Delegado Mariano menciona abaixo.

> [...] Um computador pode se tornar alvo de uma busca ou apreensão por agentes da lei em qualquer uma destas situações: há uma causa provável para acreditar que o computador é o fruto de um crime, é a instrumentalidade de um crime, ou irá produzir provas de um crime.
> A qualquer tempo, quem for alvo de busca e apreensão, pode requerer o "backup" de arquivos ou cópia dos documentos apreendidos, sendo que a devolução de material equivocadamente apreendido será objeto de restituição imediata, mediante provocação, ou de ofício.
> Deve ser feito o backup do conteúdo dos discos rígidos dos computadores e de mídias encontradas (Cd's, DVD's, Cartões de memória, etc), e não sua apreensão, não se podendo desconhecer que existem programas que ocultam os arquivos do computador, e que, inclusive, há ferramenta do sistema operacional Windows que permite a ocultação mencionada, podendo, inclusive, haver perda de dados valiosos num backup.
> Caso seja necessária a remoção de equipamentos para fins de "backup" é medida adequada à comunicação ao Juiz que concedeu a busca e apreensão desta circunstância, formalizando-se tal ato e prevendo-se o tempo necessário para cópia de todo o material apreendido, o que evitará prejuízos a quem sofreu a busca e evitará constrangimento ilegal que poderá ser sanado em sede de "mandado de segurança".
> **É absolutamente imprescindível esclarecermos que, caso seja efetuada a busca e apreensão de computadores e mídias de armazenamento sem que ocorra a efetivação de cópia do conteúdo dos mesmos, na presença de testemunhas, utilizando-se programas que possam gerar um arquivo "hash" do conteúdo para comprovar não adulteração, o material apreendido pode e deve ser considerado "inútil" porque abrirá margem a alegação de adulteração do mesmo.** (MARIANO, 2010, grifo do autor).

Frisasse que é necessária atenção ao cumprimento desse mandado, que de preferencia deve ser efetuado com a ajuda de um perito na área de computação forense. Abaixo segue mais informações segundo o disposto no *Weblog* do ilustre Delegado Mariano.

> Enumeramos a seguir, regras básicas relacionadas à busca e apreensão, principalmente de computadores e equipamentos afim, baseadas em procedimentos internacionalmente reconhecidos.
> Em caso de busca e apreensão:
> Se, dentro dos limites de razoabilidade, você acreditar que o crime sob investigação possa envolver o uso de computadores, tome providências imediatas para preservar a evidência;
> Você tem bases legais para apreender este computador (plenamente visível, mandado de busca, consentimento, etc.);
> Não acesse quaisquer arquivos no computador. Se o computador estiver desligado, deixe-o desligado. Se estiver ligado, não comece a fazer qualquer busca nos arquivos;
> Se o computador estiver ligado, consulte as seções apropriadas deste guia quanto à maneira mais adequada de desligar o computador e prepará-lo para transporte como evidência;
> Se você acreditar que o computador esteja destruindo evidências, desligue-o imediatamente puxando o cabo de força da parte de trás do computador;

Se uma câmera estiver disponível e o computador estiver ligado, tire fotografias da tela. Se estiver desligado, tire fotografias do computador, da sua localização e de quaisquer mídias eletrônica ligadas ao computador;
Considerações legais especiais se aplicam (médico, advogado, religiosos, psiquiatra, jornais, editoras, etc.)?

1º)Computador Pessoal, Doméstico, Sem Rede: Siga os procedimentos abaixo na ordem de sua apresentação para assegurar a preservação de evidências.

a)Se estiver ligado em rede (ligado a um roteador e/ou modem), veja a instrução correspondente;
b)Não utilize nem faça buscas no computador.
c)Fotografe o computador de frente e de trás, juntamente com os cabos e aparelhos ligados ao computador, no estado em que foi encontrado. Fotografe as áreas em volta do computador antes de mover qualquer evidência;
c)Se o computador estiver desligado, não o ligue;
d)Se o computador estiver ligado e houver conteúdo na tela, fotografe a tela;
e)Se o computador estiver ligado e a tela em branco, mova o mouse ou aperte a barra de espaços (assim poderá mostrar a imagem ativa na tela) Depois que a imagem aparecer, fotografe a tela;
f)Desligue o cabo de força da parte de trás da torre;
g)Se um laptop não desligar ao desconectar o cabo de força, localize e remova a bateria. Normalmente, a bateria é localizada no fundo do computador, havendo normalmente um botão ou mecanismo que permite a remoção da bateria. Uma vez removida a bateria, não recoloque nem a guarde no laptop. A remoção da bateria evitará a possibilidade de ligar o laptop acidentalmente;
h)Faça um diagrama e etiquete os cabos para identificar posteriormente outros aparelhos ligados ao computador;
i)Desconecte todos os cabos e aparelhos ligados na torre;
j)Embrulhe os componentes e transporte/armazene-os como carga frágil;
k)Apreenda outros meios de armazenamento de dados;
l)Mantenha todos os aparelhos, incluindo a torre, longe de imas, transmissores de rádio e outros elementos potencialmente prejudiciais;
m)Recolha manuais de instrução, documentação e anotações;
n)Documente todos os passos envolvidos na apreensão de um computador e seus componentes.

2º)Computador Pessoal, Doméstico, Ligado em Rede: Siga os procedimentos abaixo na ordem de sua apresentação para assegurar a preservação de evidências.

a)Desconecte o cabo de força do roteador ou do modem;
b)Não utilize nem faça buscas de evidências no computador;
c)Fotografe o computador de frente e de trás, juntamente com os cabos e aparelhos ligados ao computador, no estado em que foi encontrado. Fotografe as áreas em volta do computador antes de remover qualquer evidência;
d) Se o computador estiver desligado, não o ligue;
e)Se o computador estiver ligado e houver conteúdo na tela, fotografe a tela;
f)Se o computador estiver ligado e a tela estiver em branco, mova o mouse ou aperte a barra de espaços (assim poderá mostrara imagem ativa na tela). Depois que a imagem aparecer, fotografe a tela;
g)Desligue o cabo de força da parte de trás da torre;

h)Faça um diagrama e etiquete os cabos para identificar posteriormente outros aparelhos ligados ao computador;
i)Dê atenção à criptografia e à coleta de dados voláteis (imagem de memória RAM e documentar processo em execução, abra conexões de rede. etc.);
j)Desconecte todos os cabos e aparelhos ligados na torre;
k)Embrulhe os componentes (incluindo roteador e modem) e transporte/armazene-os como carga frágil;
l)Apreenda outros meios de armazenamento de;
m)Mantenha todos os aparelhos, incluindo a torre, longe de imãs transmissores de rádio e outros elementos potencialmente prejudiciais;
n)Recolha manuais de instrução, documentação e anotações;
o)Documente todos os passos envolvidos na apreensão de um computador e seus componentes.

3º)Servidor de Rede/Rede Empresarial:
a)Consulte pessoas com maior experiência em busca de assistência mais aprofundada;
b)Assegure a segurança da cena e não permita que alguém toque nos equipamentos, a não ser policiais treinados para manusear sistemas em rede;
c)Não desligue qualquer cabo de força em hipótese alguma.
4º)Mídias de Armazenamento (Pen Drive, Cartões de Memória, CD, DVD, Disquete): A mídia de armazenamento é utilizada para armazenar dados a partir de aparelhos eletrônicos. Esses itens podem variar em termos de capacidade de memória.
a)Recolha manuais de instrução, documentação e anotações;
b)Documente todos os passos envolvidos na apreensão de mídias de armazenamento;
c)Mantenha o equipamento longe de imãs, transmissores de rádio e outros aparelhos potencialmente prejudiciais.
5º)PDA, Telefones Celular, MP'3, Câmeras Digitais: Estes equipamentos podem armazenar dados diretamente na sua memória interna ou em cartões removíveis. A seção seguinte detalha os procedimentos apropriados a serem seguidos na apreensão e preservação desses aparelhos e suas mídias removíveis.
a)Se o aparelho estivei desligado, não o ligue;
b)No caso de PDA's ou telefones celulares, se o aparelho estiver ligado deixe-o ligado. Desligar o aparelho pode ativar a senha e consequentemente, impedir acesso à evidência;
c)Fotografe o aparelho e sua tela (se houver);
d)Etiquete e recolha todos os cabos (incluindo a fonte de energia do mesmo) e transporte-os juntamente com o aparelho;
e)Se não for possível manter o aparelho carregado, deverá o mesmo ser encaminhado com prioridade para as providências cabíveis;
f)Apreenda outras mídias de armazenamento de dados (cartões de memória, "flash" compacto, etc.);
g)Documente todos os passos envolvidos na apreensão do aparelho e de seus componentes;
h) Mantenha o equipamento longe de imãs, transmissores de rádio e outros aparelhos potencialmente prejudiciais. (MARIANO, 2010).

Saliento que todo o cuidado é pouco no cumprimento desses mandados, pois é frequente a prestação equivocada dos registros de conexão "*logs*" por parte dos provedores de acesso, o que leva a um suspeito errado.

Por fim, quero deixar claro que o objetivo desse trabalho não é se aprofundar no campo da computação forense e procedimentos da pericia criminal. Mas sim, tecer a titulo informativo considerações para maior entrosamento.

2. CONTATO COM OS PROVEDORES E REQUISIÇÃO DOS REGISTROS

No presente capitulo será exibido como identificar o responsável pelo conteúdo de um *site*, e-mail ou qualquer aplicação de internet. Qual o provedor de serviços ou servidor que hospeda a pagina para requerer a retirada do conteúdo, preservação dos logs e demais dados necessários para identificação do usuário e comprovação do ato ilícito.

Apresenta como identificar o provedor de acesso responsável pelo endereço IP na conexão à internet, a fim de requerer os registros de conexão e subsequentemente obter informações referentes ao usuário vinculado a determinado endereço IP.

Menciona ainda, sobre a notificação previa dos provedores que tem o condão de resguardar as evidências, atribuir responsabilidade solidaria do provedor pelo dano e condenação ao pagamento de custas processuais em uma futura ação judicial.

2.1 Como se chega à autoria de um crime na Internet ?

Inicialmente, para maior entendimento e conexão, vamos esclarecer o que são Provedores de Acesso e Provedores de Serviço. Segundo especialistas da área. O esquema basilar de funcionamento da internet é resumidamente assim:

USUÁRIO → PROVEDOR DE ACESSO → PROVEDOR DE SERVIÇOS

Provedores de serviços são os que oferecem utilidades/serviços na Internet, remuneradas ou não, como hospedagem, e-commerce, serviços de e-mails, comunicadores, chats, jogos online, redes sociais, dentre outros. (MILAGRE, 2011).

Exemplos: Google; Facebook; MercadoLivre; Yahoo; Hotmail; etc. Definidos pelo PL 2126/2011 como **provedor de aplicações de internet**.

“VII – aplicações de Internet: conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet;”. (BRASIL, 2011, Art. 5°, VII).

Já **provedores de acesso**, são os que fornecem acesso de usuários à Rede Mundial de Computadores, sendo que estes, por sua vez, possuem o cadastro do usuário ou do titular do computador/internet utilizada para o crime. (MILAGRE, 2011).

Exemplos: Telefônica; Embratel; Net; GVT; Brasil Telecom; Claro; etc.

"Primeiramente, deve-se acionar o provedor de serviços, para que este informe os chamados dados de conexão **(ip, data, hora, gmt)** envolvendo um suposto ilícito. (Em alguns casos o provedor de serviços possui mais dados, que podem ser fornecidos)." (MILAGRE, 2011, grifo nosso).

"De posse destes dados, deve-se na sequência, acionar o provedor de acesso, para que este informe os dados físicos **(nome, rg, cpf, endereço, telefone, etc.)** do titular da conta de Internet que estava conectado nas exatas datas e horas identificadas pelo provedor de serviços." (MILAGRE, 2011,grifo nosso).

"É com esta correlação, envolvendo provedor de serviços e provedor de acesso, que se pode chegar à autoria de crimes na Internet." (MILAGRE, 2011).

2.2. Notificação previa dos Provedores

A notificação previa do provedor é um ato extrajudicial essencial. Trata-se de requerer junto ao servidor através de carta de notificação a retirada do conteúdo, preservação das provas e demais dados necessários para identificação do usuário e comprovação do ato ilícito.

Atualmente esse artifício é de suma seriedade, pois tem o condão de resguardar as evidências, atribuir responsabilidade solidária do provedor pelo dano e condenação ao pagamento de custas processuais em uma futura ação judicial.

"A notificação é importante para se demonstrar ao Juiz, na ação a ser proposta, que a ação só está sendo proposta porque extrajudicialmente houve a recusa do provedor em fornecer os dados." (MILAGRE, 2011).

“Na ação deve-se pedir a condenação do provedor ao pagamento de honorários e custas, por ter dado causa ao ajuizamento da medida.” (MILAGRE, 2011).

Segundo Milagre (2011) o provedor que mantem os serviços pelo qual foi praticado o ato ilícito, deve ser previamente notificado, de maneira formal e registrada, com o auxilio de um advogado e um perito computacional que coletou as informações.

Deve-se requerer basicamente por meio da notificação:

“1) Retirada imediata do conteúdo ilegal e/ou ofensivo do (serviço onde o material está hospedado, incluindo o(s) link(s) pertinentes), sob pena de ajuizamento da competente ação de responsabilidade.” (MINISTÉRIO PÚBLICO DO ESTADO DE RONDÔNIA, 2012).

“2) Preservação de todas as provas e evidências da materialidade do(s) crime(s) e todos os indícios de autoria, incluindo os logs e dados cadastrais e de acesso do(s) suspeito(s),[...].” (MINISTÉRIO PÚBLICO DO ESTADO DE RONDÔNIA, 2012).

Claro que na notificação devem constar outros detalhes, como denunciar o mau uso do serviço e solicitar o máximo possível de informações referentes ao usuário. Também é necessário anexar na notificação às evidências e demais provas do delito.

“Há outras possibilidades de prova também, como solicitar ao provedor que veja, pelo seu histórico, se aquele tipo de informação estava no ar ou não. O provedor consegue descobrir isso **mesmo se o site retirar a informação do ar**.” (PINHEIRO, 2006, grifo nosso).

Em anexo segue um modelo de notificação (Anexo A - **Modelo Carta ao Provedor denunciando abuso**) disponibilizada no site do Ministério Público do Estado de Rondônia (2012).

Abaixo seguem algumas recentes posições jurisprudenciais, que definem um prazo de 24 horas após a notificação, para a retirada da página com o conteúdo ilícito da internet, **sob pena do provedor responder solidariamente com o autor do dano.**

Terceira Turma fixa prazo de 24 horas para retirada de página com conteúdo ofensivo da internet

A Terceira Turma do Superior Tribunal de Justiça (STJ) definiu em 24 horas o prazo para que o provedor de internet retire do ar mensagens postadas em redes sociais e denunciadas como ofensivas, sob pena de responder solidariamente com o autor direto do dano. **O prazo deve ser contado a partir da notificação feita pelo usuário ofendido** e a retirada tem caráter provisório, até que seja analisada a veracidade da denúncia.

A decisão foi tomada no julgamento de recurso especial interposto pelo Google. Consta no processo que, após ter sido **notificado, por meio da ferramenta "denúncia de abusos"** (disponibilizada pelo próprio provedor aos usuários do Orkut), da existência de um perfil falso que vinha denegrindo a imagem de uma mulher, o Google demorou mais de dois meses para excluir a página do site.

Ao julgar a ação ajuizada pela ofendida, o juiz de primeira instância condenou o provedor ao pagamento de indenização por danos morais no valor de R$ 20 mil.

Na apelação, o Tribunal de Justiça do Rio de Janeiro (TJRJ) reconheceu a inércia do provedor no atendimento da reclamação. Apesar disso, deu parcial provimento ao recurso do Google, apenas para reduzir o valor da indenização para R$ 10 mil.

Milhares de pedidos

O provedor não negou os fatos, mas alegou que não houve omissão. Segundo ele, o intervalo de tempo entre o recebimento da notificação e a remoção do perfil foi razoável, visto que recebe diariamente "milhares de ordens judiciais e ordens de autoridades policiais, além de cartas, e-mails, notificações de pessoas físicas e jurídicas de todo o mundo".

Afirmou que cada pedido é analisado individualmente, com prioridade para as determinações judiciais e para os casos que demonstram uma "gravidade maior". No recurso especial direcionado ao STJ, o provedor alegou violação ao artigo 186 do Código Civil.

Ao analisar o pedido, a ministra Nancy Andrighi, relatora do recurso especial, considerou o interesse coletivo envolvido na questão, "não apenas pelo número de usuários que se utilizam desse tipo de serviço, mas sobretudo em virtude da sua enorme difusão não só no Brasil, mas em todo o planeta, e da sua crescente utilização como artifício para a consecução de atividades ilegais".

Prazo razoável

Ela mencionou que, no julgamento do recurso que firmou a posição atualmente adotada pela Terceira Turma (REsp 1.193.764) e nos outros sobre o tema, inclusive nos da Quarta Turma, não foi definido objetivamente qual seria o prazo razoável para que páginas de conteúdo ofensivo fossem retiradas do ar.

"Com efeito, a velocidade com que os dados circulam no meio virtual torna indispensável que medidas tendentes a coibir informações depreciativas e aviltantes sejam adotadas célere e enfaticamente", disse.

Ela explicou que, diante da inexigibilidade (reconhecida pelo próprio STJ) de o provedor controlar e fiscalizar previamente o que é postado em seu site, é impossível evitar a difusão de mensagens ofensivas na internet.

Entretanto, tal liberdade gera a necessidade de que as mensagens sejam excluídas rapidamente, para minimizar a disseminação do insulto e, consequentemente, os efeitos posteriores à veiculação.

Nancy Andrighi citou precedente de sua relatoria sobre o tema: "Se, por um lado, há notória impossibilidade prática de controle, pelo provedor de conteúdo, de toda a informação que transita em seu site; por outro lado, deve ele, ciente da existência de publicação de texto ilícito, removê-lo sem delongas" (REsp 1.186.616).

24 horas

Para a ministra, uma vez notificado de que determinado texto ou imagem possui conteúdo ilícito, é razoável que o provedor retire o material do ar no prazo de 24 horas, sob pena de responder solidariamente com o autor direto do dano, devido à omissão.

Apesar disso, ela considerou a afirmação feita pelo Google de que recebe diariamente enorme volume de pedidos e determinações de remoção de páginas.

Explicou que o provedor não tem a obrigação de analisar em tempo real o teor de cada denúncia recebida, mas de promover, em 24 horas, a suspensão preventiva da página, para depois apreciar a veracidade das alegações e, confirmando-as, excluir definitivamente o conteúdo ou, caso contrário, reestabelecer o livre acesso à página.

"Embora esse procedimento possa eventualmente violar direitos daqueles usuários cujas páginas venham a ser indevidamente suprimidas, ainda que em caráter temporário, essa violação deve ser confrontada com os danos advindos da divulgação de informações injuriosas, sendo certo que, sopesados os prejuízos envolvidos, o fiel da balança pende indiscutivelmente para o lado da proteção da dignidade e da honra dos que navegam na rede", afirmou Andrighi.

Isso não significa que o provedor poderá adiar por tempo indeterminado a análise do teor da denúncia, deixando o usuário, cujo perfil foi provisoriamente suspenso, sem explicação. Cabe a ele, o mais rápido possível, dar uma solução final para o caso.

Em relação à viabilidade técnica de excluir o conteúdo ofensivo, a ministra verificou que a própria empresa admite ter meios para excluir imediatamente a página, "sendo certo que, afastada a necessidade de, num primeiro momento, exercer qualquer juízo de valor sobre a procedência da denúncia, não subsistem as ressalvas quanto à análise individual de cada reclamação".

(SUPERIOR TRIBUNAL DE JUSTIÇA, 2012, grifo nosso). **Processo relacionado**: REsp 1323754

Abaixo segue outro texto retirado do site Migalhas (2012, grifo nosso), na qual o *Google* foi condenado a indenizar uma estudante porque se manteve inerte após a notificação.

Google indeniza estudante por perfil falso no Orkut

O Google foi condenado a indenizar em R$ 10 mil uma estudante da Zona da Mata mineira que teve perfil falso criado no Orkut. Na página, teria sido veiculado conteúdo ofensivo à honra da requerente. A decisão da 15ª câmara Cível do TJ/MG, que confirmou sentença anterior, proíbe ainda que a empresa divulgue conteúdo ofensivo sob pena de multa diária de R$ 1 mil. A multa, no entanto, foi limitada em R$ 20 mil.

A estudante tomou conhecimento da existência do perfil falso após ter sido procurada por mulheres que tiravam satisfação sobre o fato de seus companheiros serem aliciados por ela através do Orkut.

> Ela tentou denunciar o perfil falso, **solicitando a sua retirada, mas não obteve sucesso, tendo que recorreu então à Justiça pedindo a retirada do perfil e indenização por danos morais.**
> Em 1ª instância, o juízo da 1ª vara Cível, Criminal e de Execuções Criminais de Santos Dumont determinou que o Google providenciasse o imediato cancelamento do perfil, sob pena de multa diária de R$ 1 mil.
> Inconformado, o Google recorreu ao TJ/MG. O desembargador Tibúrcio Marques, relator do recurso, afirmou que "**a Google não se exime da responsabilidade de indenizar a autora**, na medida em que ficou cabalmente demonstrado que o serviço por ela prestado é falho, vez que não garante ao usuário a segurança necessária, permitindo a veiculação de mensagens de conteúdo extremamente ofensivo e desabonador, como no caso dos autos".
> Os desembargadores Tiago Pinto e Antônio Bispo concordaram com o relator.
> **Processo:** 0458286-13.2008.8.13.0607

Note que nos exemplos citados acima a **notificação foi feita por meio da ferramenta "denúncia de abusos"** (disponibilizada pelo próprio provedor aos usuários do Orkut). Praticamente todas as aplicações de internet tem uma ferramenta semelhante.

Para mais informações consulte os "**termos de uso"** da aplicação. É no termo de uso e política que encontramos os direitos e deveres do usuário, politica de uso dos dados, o que não é permitido e como denunciar os abusos.

Contudo, quando o PL 2126/2011 (Marco Civil da Internet) entrar em vigor com força de lei, em minha opinião, pode-se entender pela interpretação do texto legal, que essa notificação extrajudicial não terá força de responsabilizar civilmente o provedor.

> **Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros**
> **Art. 14.** O provedor de conexão à Internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.
> **Art. 15.** Com o intuito de assegurar a liberdade de expressão e evitar a censura, o **provedor de aplicações de Internet somente poderá ser responsabilizado civilmente** por danos decorrentes de conteúdo gerado por terceiros se, **após ordem judicial específica**, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.
> Parágrafo único. A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material. (BRASIL, 2011, art. 14 e 15, grifo nosso).

Note que o PL 2126/11 segue a lógica da atual jurisprudência, na qual o provedor de aplicações de internet somente poderá ser responsabilizado civilmente se após tomar conhecimento ou for avisado do conteúdo ilícito manter-se inerte.

Contudo, somente após ordem judicial, ou seja, a mera notificação feita por meio da ferramenta "denuncia de abusos" como costa no caso exposto acima "Google indeniza estudante por perfil falso no Orkut", não terá mais o condão de responsabilizar o provedor.

2.3 Contato com o provedor de serviços (aplicações de Internet)

Abaixo será exposto como entrar em contato com o provedor de serviços ou provedor de aplicações de internet, o mesmo procedimento é adotado para identificar o responsável pelo conteúdo de um *Website* ou *blog.*

Na hipótese de ser impossível entrar em contato com o responsável com informações disponíveis na própria página. Normalmente existe na página um campo (*link*) do tipo "contato", "webmaster" também se encontra canal de contato nos "termos de uso".

Para desvendarmos quem é o responsável pelo conteúdo de um site inicialmente precisamos descobrir qual é o **provedor de serviços** ou servidor que hospeda a pagina. Essa informação pode ser facilmente obtida através de sites de pesquisa de domínio que disponibilizam esse serviço.

Segue abaixo algumas sugestões:

- http://whois.domaintools.com/ ;

- http://www.registro.br. (Somente domínios nacionais terminados em .br).

Basta colar a *URL* do *site* no espaço indicado e acionar a pesquisa (com informação de contato) que varias informações importantes serão disponibilizadas como o responsável pelo domínio, contato para eventuais incidentes, provedor que hospeda o site e etc.

Existe um serviço na internet muito útil para descobrir endereços - www.apontador.com.br/local - basta digitar o nome da empresa/razão social (exemplo: Google Brasil, facebook) o resultado expõe o **endereço empresarial e telefone** da empresa.

De posse dessas informações teremos meios de entrar em contato, ou, na hipótese de uma medida pela via judicial, para onde o oficio deve ser encaminhado para a empresa responsável responder fornecendo os subsídios necessários.

2.3.1 Do requerimento dos registros de acesso a aplicações de Internet.

Atualmente, requer-se junto ao provedor através de carta de notificação previa, de regra, a retirada do conteúdo, preservação dos logs e demais dados necessários para identificação do usuário e comprovação do ato ilícito.

(Importante. Para mais informações e entendimento leia o tópico 2.2 notificação previa dos provedores).

Caso exista a **negativa dos provedores** em atender os requerimentos pela via extrajudicial, ficamos forçados a adotar medidas judicias para alcançar os objetivos. Entre elas a quebra do sigilo dos dados telemáticos.

> **4.1.6. Quebra do sigilo de dados telemáticos.**
> Feita a identificação do provedor que hospeda a página, qual a etapa seguinte? Depende: a) se o hospedeiro é um provedor conhecido, que hospeda, gratuita ou mediante remuneração, sites de terceiros (por exemplo,"HPG", "Geocities", "Terra"); b) se a página está registrada em nome de uma empresa não conhecida. Nessa última hipótese, seria preciso analisar o caso concreto, e verificar se é possível requerer a quebra do sigilo de dados telemáticos sem que o autor da página tome conhecimento disso.
> Se o provedor que hospeda a página for conhecido (e brasileiro), o investigador deverá requerer, judicialmente (ver modelo no anexo III), a **quebra de sigilo de dados telemáticos, para que o hospedeiro forneça uma cópia, em mídia não-regravável (CD-R), das páginas investigadas e também os logs, isto é, os registros de criação e alteração da página. É no log que encontramos as três informações que nos são necessárias para prosseguir: a) o número IP; b) a data e a hora da comunicação; e c) a referência ao horário, incluído o fuso horário GMT ou UTC.**
> No caso de páginas da Internet, é comum o provedor fornecer uma lista de IP's e datas. Esta lista indica todas as vezes em que a página foi modificada.

> Como é possível que mais de um computador tenha sido usado para alterar o conteúdo da página, aconselhamos que o investigador selecione quatro ou cinco "linhas" da lista para, em seguida, formular outro requerimento judicial, desta vez à operadora de telefonia ou cabo. **(**MINISTÉRIO PÚBLICO FEDERAL, 2006, p. 26, grifo nosso).

O modelo de quebra do sigilo dos dados telemáticos que se refere à citação acima esta em anexo neste trabalho. Os requisitos legais do requerimento, segundo o PL 2126/11 estão elencados abaixo.

> **Seção II**
> **Da Guarda de Registros**
> **Art. 10**. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet de que trata esta Lei devem atender à preservação da intimidade, vida privada, honra e imagem das partes direta ou indiretamente envolvidas.
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo.
>
> **Seção IV**
> **Da Requisição Judicial de Registros**
> **Art. 17**. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de Internet.
> Parágrafo único. Sem prejuízo dos demais requisitos legais**, o requerimento deverá conter, sob pena de inadmissibilidade:**
> **I –** fundados indícios da ocorrência do ilícito;
> **II –** justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
> **III –** período ao qual se referem os registros.
> (BRASIL, 2011, Art. 17, grifo nosso).

"VI - **registro de conexão :** conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;" (BRASIL, 2011, Art. 5°, VI).

VIII – **registros de acesso a aplicações de Internet:** conjunto de informações referentes à data e hora de uso de uma determinada aplicação de Internet a partir de um determinado endereço IP. (BRASIL, 2011, Art. 5°, VIII).

> Caso o site esteja hospedado no exterior, a competência da Justiça e da Polícia brasileiras só estará justificada (e executável) se houver algum vínculo com brasileiros. Por exemplo, há hoje sites racistas e nazistas feitos por brasileiros hospedados em provedores na Argentina e nos EUA. Nesse caso, entendemos que é possível a persecução penal no Brasil, remanescendo o problema da identificação da autoria.
> Se não houver vínculo algum do site com o Brasil (ou seja, ele não está hospedado em provedores nacionais e não há indícios da participação de brasileiros no delito) recomendamos que a notícia do fato criminoso seja encaminhada à INTERPOL. Ou, melhor, comunicada a um dos hotlines associados à INHOPE - International Association of Internet Hotlines (www.inhope.org), pois a associação filiada se encarregará de informar rapidamente a polícia local. (MINISTÉRIO PÚBLICO FEDERAL, 2006, p. 25).

Vencida essa batalha, de posse **do endereço IP acompanhado da data de comunicação e o horário indicando o fuso horário utilizado - UTC ou GMT.** O próximo passo e formular um novo requerimento judicial, dessa vez junto ao provedor de acesso á internet (ver tópico 2.5).

Porém, o PL2126/11 vem trazendo um **aparente retrocesso** na guarda de registros de acesso a aplicações de internet. A palavra "Provisão" foi muito bem empregada. Provisão é sinônimo de guarnição, aprovisionamento, munição. Veja abaixo.

> **Da Guarda de Registros de Acesso a Aplicações de Internet**
> **Art. 12**. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de Internet.
> **Art. 13. Na provisão de aplicações de Internet é facultada a guarda dos registros de acesso a estas**, respeitado o disposto no art. 7º.
> § 1º A opção por não guardar os registros de acesso a aplicações de Internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.
> § 2º Ordem judicial poderá obrigar, por tempo certo, a guarda de registros de acesso a aplicações de Internet, desde que se tratem de registros relativos a fatos específicos em período determinado, ficando o fornecimento das informações submetido ao disposto na Seção IV deste Capítulo.
> § 3º Observado o disposto no § 2º, a autoridade policial ou administrativa poderá requerer cautelarmente que os registros de aplicações de Internet sejam guardados, observados o procedimento e os prazos previstos nos §§ 3º e 4º do art. 11. (BRASIL, 2011, Art. VI, grifo nosso).

Acredito que seja essencial a revisão do ponto referente à faculdade a guarda dos registros de acesso a aplicações de internet. Do contrário, a insegurança jurídica e impunidade vão reinar em um território que já é considerado sem lei.

2.4 Localizando o responsável por um e-mail

Antes de prosseguir com o processo de investigação tradicional vale apena consultar o endereço < http://www.spokeo.com/ >. Basta colar o e-mail no campo indicado que o serviço aponta o dono do e-mail, é incrível, funciona na maioria dos casos.

Para localizar o responsável por um e-mail é realmente muito fácil, basta verificar o cabeçalho (*header*) e identificar o endereço IP da primeira maquina que originou a mensagem, ou seja, o ultimo "*received*".

Veja abaixo como analisar o cabeçalho de um e-mail segundo o Ministério Público Federal (2006, p. 29).

4.2.3. Analisando o cabeçalho de um e-mail.
A análise do cabeçalho de um *e-mail* é bastante complexa, mas é graças a ela que é possível identificar o remetente da mensagem. É comum um cabeçalho possuir várias linhas que começam com a palavra "*received*". A palavra marca por quantas estações (ou servidores) a mensagem passou antes de chegar ao destinatário. O parágrafo que interessa é sempre o **último "*received*"** (os "received" estão em ordem decrescente, ou seja, o primeiro "received" mostrará a máquina mais recente por onde sua mensagem passou) é ele quem indica a primeira máquina que originou a mensagem, isto é, o computador do remetente..
Abaixo um exemplo de cabeçalho de e-mail com endereço falso (típico de estação infectada com vírus), mas contendo o IP verdadeiro do remetente. Observe também a data e o horário (incluindo o fuso horário) que o e-mail foi encaminhado:

```
Received: from pppp.mmm.gov.br
        ([200.158.14.238])
        by pprr.www.mmm.gov.br; Wed, 03 Mar 2004 07:49:53 -0300
From: pifkdjkgab@ifpp.gov.br
To: fulano@pppp.mmm.gov.br
Subject: Re: Your archive
Date: Wed, 3 Mar 2004 07:46:27 -0300
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0003_000052ED.00002596"
X-Priority: 3
X-MSMail-Priority: Normal

This is a multi-part message in MIME format.

------=_NextPart_000_0003_000052ED.00002596
Content-Type: text/plain;
        charset="Windows-1252"
Content-Transfer-Encoding: 7bit
```

Obtida a informação do **endereço IP, a data da comunicação, e o horário indicando o fuso horário utilizado – GMT ou UTC.** Na sequencia é só localizar a quem pertence o endereço IP (ver tópico 2.5 deste capitulo), entrar em contato com o provedor e requisitar as informações.

Segundo o Ministério Público Federal (2006, p. 31). Caso não seja possível identificar o **numero ip, data, hora, gmt,** mas consta o endereço eletrônico do remetente (exemplo: joaodasilva@terra.com.br).

A autoridade policial ou o membro do Ministério Público podem requerer judicialmente a quebra do sigilo de dados telemáticos para que o provedor do e-mail (no exemplo, o Terra) forneça o endereço IP da máquina que autenticou esta conta, na data e horário do e-mail remetido.

2.5 Contato com provedor de acesso e requisição dos registros de conexão

Abaixo segue exposto como identificar o provedor de acesso responsável pelo endereço IP na conexão à internet, a fim de requerer os registros de conexão e subsequentemente obter informações referentes ao usuário vinculado a determinado endereço IP.

O endereço IP (internet protocol) é como se fosse um CPF, é uma identificação que todo computador que acessa a rede possui. Existe o **IP estático**, ou seja, não muda permanece sempre o mesmo endereço IP e existe também o **IP dinâmico** que muda toda vez que o computador se conecta à internet.

“IV - endereço IP - código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;”. (BRASIL, 2011, Art. 5°, IV).

Normalmente os provedores de acesso, por motivos de segurança, utilizam a tecnologia do IP dinâmico, portanto cada vez que o usuário se conecta na rede receba um numero de IP diferente, **é por isso que é tão importante coletar a data, hora e fuso horário, junto com o endereço IP.**

> Como a Internet é uma rede *mundial* de computadores, os registros indicam a hora local (05:41:12, no exemplo) e a referência à hora GMT (no caso - 08:00). Às vezes, é feita apenas a menção à hora GMT (por exemplo, "Tue, 09 Mar 2004 00:24:28 GMT"). **Nos pedidos feitos aos provedores de acesso e às companhias telefônicas, é imprescindível que haja, no mínimo, a menção a esses três indicadores: a) o número IP; b) a data da comunicação; e c) o horário indicando o fuso horário utilizado – GMT ou UTC. Sem eles, não será possível fazer a quebra do sigilo de dados telemáticos. (**MINISTÉRIO PÚBLICO FEDERAL, 2006, p. 15).

A partir do endereço IP descobriremos o provedor de acesso (ISP, "Internet Service Provider) que é uma empresa, normalmente companhias telefônicas, que fornece acesso à internet em determinada região geográfica.

Contudo, não existe qualquer conexão entre a localização geográfica do provedor de acesso e do usuário, uma vez que um internauta pode, por exemplo, usar um provedor chinês e terá um IP na china independente de sua localização. Porém, às vezes, descobrimos a localização aproximada do usuário, caso utilize um provedor de sua região.

Para descobrir informações e dados cadastrais do usuário vinculado ao endereço IP, se faz necessário um novo pedido de quebra dos dados telemáticos (modelo em anexo), dessa vez junto ao provedor de acesso (ISP, "Internet Service Provider).

Para encontrar informações sobre o provedor de acesso é muito simples, basta procurar na internet por *sites* que ofereçam serviços de localização ou rastreamento de IP, como por exemplo:

- http://whois.domaintools.com/

- http://www.maxmind.com/app/lookup_city

Basta inserir o endereço IP no campo indicado e o *site* trará informações relevantes sobre do endereço IP pesquisado, como:

- Organização (nome da empresa responsável pelo serviço).
- ISP (Provedor de Acesso);

- País;
- Estado;
- Cidade;
- Latitude e longitude;

(Para descobrir dados complementares, como Rua, Bairro, e etc. Basta copiar a longitude e latitude e colar no *GOOGLE MAPS*).

Existe um serviço na internet muito útil para descobrir endereços - www.apontador.com.br/local - basta digitar o nome da empresa/razão social (exemplo: Google Brasil, facebook) o resultado expõe o **endereço empresarial e telefone** da empresa.

De posse dessas informações sabemos para onde o oficio judicial deve ser encaminhado e a empresa responsável devera responder fornecendo os registros de conexão e subsídios necessários para localização e identificação do indivíduo.

> **Seção IV**
> **Da Requisição Judicial de Registros**
> **Art. 17**. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de **registros de conexão** ou de registros de acesso a aplicações de Internet.
> Parágrafo único. Sem prejuízo dos demais requisitos legais**,** o requerimento deverá conter, sob pena de inadmissibilidade:
> I – fundados indícios da ocorrência do ilícito;
> II – justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
> III – período ao qual se referem os registros.
> (BRASIL, 2011, Art. 17, grifo nosso).

"VI - **registro de conexão:** conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;" (BRASIL, 2011, Art. 5°, VI).

Veja que o PL 2126/11 traz em seu texto o dever guardar os registros de conexão pelo prazo de um ano, o que vai ao desencontro do prazo prescricional de varias condutas delituosas contempladas pela nossa legislação.

> **Da Guarda de Registros de Conexão**
> **Art. 11**. Na provisão de conexão à Internet, cabe ao administrador do sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, **pelo prazo de um ano**, nos termos do regulamento.
> § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
> § 2º A autoridade policial ou administrativa poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.
> § 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de sessenta dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.
> § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º. (BRASIL, 2011, art. 11, grifo nosso).

Diante disto, reforço mais uma vez a necessidade de agir com extrema urgência em casos de litígios instaurados por meio da internet.

2.5.1 Servidores Proxy

Como foi exposto anteriormente, o endereço IP é fundamental para a identificação do usuário, porem existe formas indiretas de acesso à internet, na qual um servidor serve de " intermediário" na conexão.

USUÁRIO → SERVIDOR PROXY → INTERNET

Chamados servidores *PROXY* (PROXY significa procuração em inglês), cuja função é filtrar conteúdo, **providenciar anonimato**, e outras finalidades.

"Um ***proxy* anônimo** é uma ferramenta que se esforça para fazer atividades na Internet sem vestígios: acessa a Internet a favor do usuário, protegendo as informações pessoais ao ocultar a informação de identificação do computador de origem." (WINKIPEDIA, 2012).

Além disso, é possível usar uma cadeia de servidores *proxyes* diferentes. Se um servidor da cadeia não armazenar as informações dos usuários, torna-se praticamente impossível identificar o usuário através do endereço IP.

Portanto, a identificação do usuário depende da colaboração dos servidores *proxy* envolvidos. Alguns incluem o registro de *logs* e também enviam cabeçalhos contendo o endereço IP original do usuário, para evitar problemas legais. No entanto a legislação ainda e fraca nessa questão.

2.6 Requisições de dados cadastrais pela autoridade policial independente de autorização judicial.

Com a entrada em vigor da Lei n° 12.683, de 9 de julho de 2012, que alterou a Lei n° 9.613, de 3 de março de 1998, para tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro.

A autoridade policial ganhou reforço para requisitar dados cadastrais **diretamente** junto à companhias telefônicas e provedores de internet, independentemente de autorização judicial.

De acordo com a Lei nº 12.683, de 9 de julho de 2012 (grifo nosso).

> Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, **independentemente de autorização judicial**, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito.

Esse dispositivo de natureza processual penal trouxe uma importante inovação de natureza pratica, agilizando de forma considerável o processo.

“Outrora, estes órgãos quando perquiridos exigiam uma ordem judicial, o que acabava levando a investigação a uma verdadeira teia burocrática que em muito contribuía para o insucesso” (Delegado Mariano, 2012).

Há que diga que isso seria inconstitucional por violar a privacidade e intimidade do individuo, contudo existem posicionamentos mais lúcidos sobre o caso.

De acordo com o Delegado Mariano (2012)

> [...] Este tipo de informação não revela quaisquer aspectos da vida privada ou da intimidade do indivíduo, até porque é esperado que todos possuam tais elementos identificadores, os quais por se tratarem de dados objetivos, não permitem qualquer juízo de valor sobre uma pessoa.
> O S.T.F. já se posicionou sobre o assunto, no sentido de que a proteção constitucional a inviolabilidade das comunicações se refere à comunicação de dados e não aos dados em si, conforme extensa ementa abaixo parcialmente transcrita, além do fato de que conceito de "dados" contido no preceito constitucional é diverso do conceito de dados cadastrais:
>
> *EMENTA: (...) IV – Proteção constitucional ao sigilo das comunicações de dados – art. 5º, XVII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada – o ter sido o microcomputador apreendido sem ordem judicial e a conseqüente ofensa da garantia da inviolabilidade do domicílio da empresa – este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação do art. 5º. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve "quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial". 4. A proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação "de dados" e não dos "dados em si mesmos", ainda quando armazenados em computador. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira – RTJ 179/225, 270). V – Prescrição pela pena concretizada: declaração, de ofício, da prescrição da pretensão punitiva do fato quanto ao delito de frustração de direito assegurado por lei trabalhista (C. Penal, arts. 203; 107, IV; 109, VI; 110, § 2º e 114, II; e Súmula 497 do Supremo Tribunal).*
>
> Cumpre ainda destacarmos que informações cadastrais de correntistas de instituições financeiras não estão sujeitas ao chamado "sigilo bancário", pois não sendo os dados cadastrais bancários protegidos pelo sigilo bancário não há em nosso ordenamento jurídico qualquer previsão no sentido da necessidade de ordem judicial para o acesso a este tipo de dados cadastrais, o que implica na aplicabilidade do poder geral de polícia (art. 6, III do CPP) no que diga respeito à requisição destes.

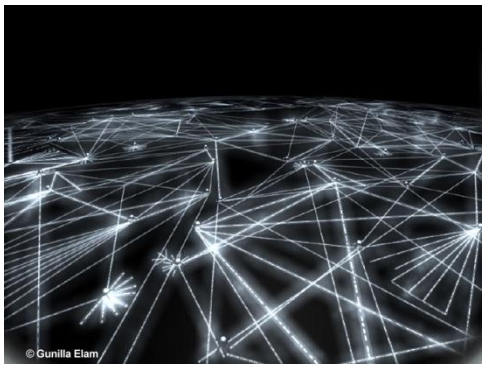
> Desta forma, tendo a Autoridade Policial conhecimento que determinada conta bancária é utilizada para fins ilícitos pode requisitar ao banco os dados cadastrais do titular da mesma.
> Por outro lado, a alteração legislativa em comento veio para deixar assentado que a Autoridade Policial pode requisitar "dados cadastrais telefônicos", informações mínimas sobre o proprietário da linha telefônica, com a finalidade de especificar qual é o consumidor do serviço e cujo acesso não depende de nenhum tipo de autorização judicial.
> Com o advento da alteração legislativa, certo é que o descumprimento de requisição de dados cadastrais solicitados por Autoridade Policial amolda-se perfeitamente ao delito de desobediência, constante no artigo 330 do Código Penal, por se tratar de ordem legal advinda de funcionário público uma vez que tal prerrogativa requisitória encontra-se amparada pela norma constante no artigo 6º, III do CPP.
> E mais: a Lei 8.078/90, em seu artigo 43, §4º, estabelece que os bancos de dados e cadastros relativos a consumidores são considerados entidades de caráter público, o que reforça ainda mais a possibilidade de requisição de dados cadastrais pela Autoridade Policial através do poder geral de polícia, inclusive anteriormente a edição da Lei 12.683, de 9.7.2012, a qual veio apenas consagrar este tipo de posicionamento[...].

Note que o PL 2126/11 também traz em seu texto de forma expressa o poder da autoridade policial ou administrativa requerer cautelarmente que os registros de conexão sejam guardados, porém terá acesso somente com autorização judicial.

> **Da Guarda de Registros de Conexão**
> **Art. 11**. Na provisão de conexão à Internet, cabe ao administrador do sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, **pelo prazo de um ano**, nos termos do regulamento.
> § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
> **§ 2º A autoridade policial ou administrativa poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.**
> § 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de sessenta dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.
> § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º. (BRASIL, 2011, art. 11, grifo nosso).

Por fim se destaca a incongruência entre as duas leis. Não tenho conhecimento suficiente para saber o que acontecerá se o for aprovado o PL 2126/011 com essa redação. Contudo segundo os princípios gerais do direito, a lei nova revoga ou torna sem efeito a anterior.

3 COMPETÊNCIA TERRITORIAL E JURISDICIONAL NO CIBERESPAÇO



(GOOGLE, 2012)

A internet é uma rede parecida com uma teia de aranha que se espraia a nível mundial sem fronteiras territoriais, *www* significa teia mundial em português. E é exatamente por isso, que a questão da competência territorial e jurisdicional no ciberespaço é tão controvertida.

"A Internet é o maior conglomerado de redes de comunicações em escala mundial e dispõe milhões de computadores interligados pelo protocolo de comunicação TCP/IP que permite o acesso a informações e todo tipo de transferência de dados." (WIKIPÉDIA, 2012).

Ainda não existe legislação especifica sobre o assunto e as teorias são muitas, portanto, o que se pode fazer por enquanto é analisar o contexto de cada caso individualmente e na duvida nos basear em jurisprudências para sanar divergências a respeito da matéria.

Abaixo seguem alguns julgados recentes dos tribunais, sobre questões controvertidas até pouco tempo.

> CONFLITO NEGATIVO DE COMPETÊNCIA. CRIME DE INJÚRIA PRATICADO POR MEIO DA INTERNET, NAS REDES SOCIAIS DENOMINADAS ORKUT E TWITTER. AUSÊNCIA DAS HIPÓTESES DO ART. 109, INCISOS IV E V, DA CF. OFENSAS DE CARÁTER EXCLUSIVAMENTE PESSOAL. COMPETÊNCIA DA JUSTIÇA ESTADUAL.
> 1 - O simples fato de o suposto delito ter sido cometido por meio da rede mundial de computadores, ainda que em páginas eletrônicas internacionais, tais como as redes sociais "Orkut" e "Twitter", não atrai, por si só, a competência da Justiça Federal.
> 2 - É preciso que o crime ofenda a bens, serviços ou interesses da União ou

esteja previsto em tratado ou convenção internacional em que o Brasil se comprometeu a combater, como por exemplo, mensagens que veiculassem pornografia infantil, racismo, xenofobia, dentre outros, conforme preceitua o art. 109, incisos IV e V, da Constituição Federal.
3 - Verificando-se que as ofensas possuem caráter exclusivamente pessoal, as quais foram praticadas pela ex-namorada da vítima, não se subsumindo, portanto, a ação delituosa a nenhuma das hipóteses do dispositivo constitucional, a competência para processar e julgar o feito será da Justiça Estadual.
4 - Conflito conhecido para declarar a competência do Juízo de Direito do Juizado Especial Cível e Criminal de São Cristóvão/SE, o suscitado. (BRASIL,2012).

CONFLITO DE COMPETÊNCIA. DIREITO PROCESSUAL PENAL. ARTIGO 241, CAPUT, DA LEI Nº 8.069/90. DIVULGAÇÃO. CRIME PRATICADO NO TERRITÓRIO NACIONAL POR MEIO DE PROGRAMA DE COMUNICAÇÃO ELETRÔNICA ENTRE DUAS PESSOAS. COMPETÊNCIA DA JUSTIÇA ESTADUAL.
1. "Aos juízes federais compete processar e julgar: os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente." (Constituição Federal, artigo 109, inciso V).
2. Em se evidenciando que os crimes de divulgação de fotografias e filmes pornográficos ou de cenas de sexo explícito envolvendo crianças e adolescentes não se deram além das fronteiras nacionais, restringindo-se a uma comunicação eletrônica entre duas pessoas residentes no Brasil, não há como afirmar a competência da Justiça Federal para o processo e julgamento do feito.
3. Conflito conhecido, para declarar competente o Juízo Estadual suscitante.
(BRASIL, 2008).

CONFLITO NEGATIVO DE COMPETÊNCIA. QUEIXA-CRIME. CALÚNIA PRATICADA, EM TESE, POR JORNALISTA. CARTA PUBLICADA EM BLOG. LEI DE IMPRENSA.
NORMA NÃO RECEPCIONADA PELA CONSTITUIÇÃO DE 1988. ART. 70 DO CÓDIGO DE PROCESSO PENAL. COMPETÊNCIA DO JUÍZO SUSCITADO.
1. Não recepcionada a Lei n. 5.250/1967 pela nova ordem constitucional (ADPF n. 130/DF), às causas decorrentes das relações de imprensa devem ser aplicadas as normas da legislação comum, inclusive, quanto à competência, o disposto no art. 70 do Código de Processo Penal.
2. O crime de calúnia (art. 138, caput, do Código Penal) consuma-se no momento em que os fatos "veiculados chegam ao conhecimento de terceiros" (CC n. 107.088/DF, Relatora Ministra Maria Thereza de Assis Moura, DJe de 4/6/2010).
3. Tratando-se de queixa-crime que imputa a prática do crime de calúnia em razão da divulgação de carta em blog, na internet, o foro para processamento e julgamento da ação é o do lugar de onde partiu a publicação do texto tido por calunioso.
4. In casu, como o blog em questão está hospedado em servidor de internet sediado na cidade de São Paulo, é do Juízo da 13ª Vara Criminal dessa comarca a competência para atuar no feito.
5. Conflito conhecido para declarar competente o suscitado.
(BRASIL, 2011).

CONFLITO DE COMPETÊNCIA. PENAL. JUÍZOS ESTADUAIS. EXTORSAO VIA MENSAGENS ELETRÔNICAS PELA INTERNET. DELITO FORMAL. MOMENTO CONSUMATIVO. PRESENÇA DOS ELEMENTOS CONSTITUTIVOS DO TIPO. LOCAL DO RECEBIMENTO DOS E-MAILS.

Na hipótese dos autos, houve o momento consumativo perpetrado pelo agente ao praticar o ato de constrangimento (envio dos e-mails de conteúdo extorsivo), e o das vítimas que se sentiram ameaçadas e intimidadas com o ato constrangedor, o que ocasionou a busca da Justiça.

Consumação do lugar do recebimento das mensagens eletrônicas.

Conflito conhecido, declarando-se a competência do Juízo de Direito da 2ª Vara Criminal de Guarapuava/PR.

(BRASIL, 2004, apud AGUIAR, 2006).

CONCLUSÃO

A internet é algo muito recente e presente, apresenta progresso explosivo e esta mudando inegavelmente o âmbito social. Como consequência o ordenamento jurídico deve acompanhar o avanço da sociedade a fim de tutelar as relações jurídicas.

Tendo em vista o crescimento exponencial da internet e que as empresas relações sociais, hábitos de consumo, e demais relações jurídicas estão migrando para o ambiente ciberespaço, por consequência, as demandas judiciais tem a tendência de aumentar cada vez mais.

E com este cenário, precisamos de cursos de Direito atualizados, profissionais capacitados e acima de tudo juízes com pleno conhecimento acerca da matéria, além é claro, da legislação ser adequada à nova realidade social.

No entanto, por ser a internet algo inédito, a legislação ainda é extremamente carente nesse sentido, existem lacunas, nem todas as condutas se enquadram em nossos códigos e se encontram dificuldades para buscar interpretações análogas.

Diante disto, os estudantes e profissionais do Direito mostram insuficiência de conhecimento acerca do tema, por ser um assunto dinâmico e intricado. Com novas tecnologias surgindo a cada segundo o conhecimento acumulado se torna obsoleto muito rápido.

REFERÊNCIAS

BRASIL. Decreto Lei nº 2.848 de 07 de Dezembro de 1940.

BRASIL. Lei n° 10.406 de 10 de janeiro de 2002.

BRASIL. Lei nº 12.683, de 9 de julho de 2012.

BRASIL. PROJETO DE LEI 2126/2011.

BRASIL. Superior Tribunal de Justiça. CC 121.431/SE, Rel. Ministro Marco Aurélio Bellizze, Terceira Seção, julgado em 11/04/2012, DJe 07/05/2012**.** Disponível em: < http://br.vlex.com/vid/-369233178>. Acesso em: 20 ago. 2012.

BRASIL. Superior Tribunal de Justiça. CC 40.569/SP, Rel. Ministro José Arnaldo da Fonseca, Terceira Seção, julgado em 10/03/2004, DJ 05/04/2004, p. 201. In: AGUIAR, Rebeca Novaes. Competência territorial para apurar crimes na internet: **Revista Âmbito Jurídico,** Rio Grande, 31, 31 jul. 2006. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=1225>. Acesso em: 20 ago. 2012.

BRASIL. Superior Tribunal de Justiça. CC 57.411/RJ, Rel. Ministro Hamilton Carvalhido, Terceira Seção, julgado em 13.02.2008, DJ 30.06.2008 p.1. Disponível em: < http://br.vlex.com/vid/-41196239>. Acesso em: 20 ago. 2012.

BRASIL. Superior Tribunal de Justiça**.** CC 97.201/RJ, Rel. Ministro Celso Limongi (Desembargador Convocado do TJ/SP), Terceira Seção, julgado em 13/04/2011, DJe 10/02/2012**.** Disponível em: <http://br.vlex.com/vid/-351203390>. Acesso em: 20 ago. 2012. Acesso em: 20 ago. 2012.

CRIMES PELA INTERNET. **Como denunciar crimes digitais.** Postado em 18 de outubro de 2011. Disponível em: < http://www.crimespelainternet.com.br/como-denunciar-crimes-digitais/>. Acesso em: 29 de jul. 2012.

CRIMES PELA INTERNET. **Como identificar a origem de um e-mail que recebi.** Postado em 27 de novembro de 2011. Disponível em: < http://www.crimespelainternet.com.br/como-identificar-a-origem-de-um-e-mail-que-recebi/>. Acesso em: 29 de jul. 2012.

GOOGLE Imagens. **Trabalhando na rede mundial de computadores**. 800 X 600|109.7KB jpeg. Disponível em: <http://images.search.conduit.com/ImagePreview/?q=rede%20mundial%20de%20computadores&ctid=CT2851643&searchsource=48&start=0&pos=0>. Acesso em: 20 ago. 2012.

HEREDIA. Carlos Américo Ramos. Hipotesis Acusatoria. La Evidencia Digital. 25 mai. 2011. 200 X 200 | 24.6KB gif. Disponível em: <http://hipotesis-acusatoria.blogia.com/2011/052601-la-evidencia-digital.php>. Acesso em: 12 set. 2012.

JORGE. Higor Vinicius Nogueira. Cyberbullyng e investigação de crimes cibernéticos. **Segurança da Informação e Crimes Cibernéticos**, 19 jun. 2011. Disponível em: <http://www.crimesciberneticos.net/2011/06/cyberbullyng-e-investigacao-de-crimes.html>. Acesso em: 17 set. 2012.

MARIANO, Delegado**.** Busca e apreensão de computadores**. Cyber Crimes – Delegado Mariano,** 29 jan. 2010. Disponível em: <http://mariano.delegadodepolicia.com/busca-e-apreensao-de-computadores/>. Acesso em: 29 ago. 2012.

MARIANO, Delegado**.** Lei 12.683, de 9.7.2012: reforço ao poder de requisitar dados cadastrais pela Autoridade Policial**. Cyber Crimes – Delegado Mariano,** 17 jul. 2012. Disponível em: <http://mariano.delegadodepolicia.com/lei-12-683-de-9-7-2012-reforco-ao-poder-de-requisitar-dados-cadastrais-por-parte-da-autoridade-policial/>. Acesso em: 20 jul. 2012.

MIGALHAS. **Google indeniza estudante por perfil falso no Orkut,** 15 jun. 2012. Disponível em: <http://www.migalhas.com.br/Quentes/17,MI157619,21048Google+indeniza+estudante+por+perfil+falso+no+Orkut>. Acesso em: 14 ago. 2012.

MILAGRE, José Antonio. F.A.Q do Cybercrime: O que fazer e como agir em casos de crimes na Internet. **Legaltech Consultoria,** Versão 2, 30 abr. 2011. Disponível em: <http://www.legaltech.com.br/faq_do_cybercrime.php>. Acesso em: 14 ago. 2012.

MINISTÉRIO PÚBLICO DO ESTADO DE RONDÔNIA. Coordenadoria Estadual de Combate aos Crimes Cibernéticos. **Modelo Carta ao Provedor denunciando abuso**. 2012. Disponível em: <http://www.mp.ro.gov.br/web/ccc/arquivos/carta-ao-provedor>. Acesso em: 20 ago. 2012.

MINISTÉRIO PÚBLICO FEDERAL. Procuradoria da República no Estado de SP. Grupo de Combate aos Crimes Cibernéticos. **Crimes Cibernéticos:** Manual Prático de Investigação. Abril de 2006. Disponível em: <http://www.mpdft.gov.br/portal/pdf/unidades/promotorias/pdij/TAC/Manual_de_Crimes_de__Inform%C3%A1tica_-_vers%C3%A3o_final2.pdf>. Acesso em: 26 jul. 2012.

PINHEIRO Aline. A internet e a lei - Conteúdo que está no seu computador é público. **Consultor Jurídico**, 03 set. 2006. Disponível em: <http://www.fraudes.org/clipread.asp?CdClip=614>. Acesso em: 07 set. 2012.

PORTAL NACIONAL DO DOCUMENTO ELETRÔNICO. Documentos Eletrônicos. **Assinatura digital**. Disponível em: <http://www.documentoeletronico.com.br/assinatura-digital.asp>. Acesso em: 12 de set 2012.

SUPERIOR TRIBUNAL DE JUSTIÇA. Terceira Turma fixa prazo de 24 horas para retirada de página com conteúdo ofensivo da internet. **Sala de Notícias**, 22 jun. 2012. Disponível em: <http://www.stj.jus.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=106174>. Acesso em: 12 set. 2012.

WIKIPÉDIA. Desenvolvido pela Wikimedia Foundation. Apresenta conteúdo Enciclopédico. Disponível em: <http://pt.wikipedia.org/wiki/Ata_notarial>. Acesso em: 05 ago. 2012.

WIKIPÉDIA. Desenvolvido pela Wikimedia Foundation. Apresenta conteúdo Enciclopédico. Disponível em: <http://pt.wikipedia.org/wiki/Internet>. Acesso em: 20 ago. 2012.

Anexo A

Modelo carta ao provedor denunciando abuso. (MINISTÉRIO PÚBLICO DO ESTADO DE RONDÔNIA, 2012).

Carta-Modelo

Cidade , (DATA)

Ao Senhor(a) Diretor(a) da (Nome da Empresa prestadora de serviço responsável por hospedar o conteúdo ilegal e/ou ofensivo)

Prezado Senhor,

(Nome do interessado), (Nacionalidade), (Profissão), (Estado Civil), portador da Carteira de Identidade nº (xxx), inscrito no CPF sob o nº (xxx), residente e domiciliado à Rua (xxx), nº (xxx), Bairro (xxx), Cidade (xxx), Cep. (xxx), no Estado de (xxx), com fundamento na Constituição da República, art. 5º, X, dispositivo este que assegura a todo cidadão o direito a inviolabilidade da "intimidade, vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente da sua violação", vem notificar o que se segue para, ao final, pleitear as providências cabíveis e expressamente indicadas:

DOS FATOS

(Aqui, narrar em detalhes o fato que enseja a busca pelo direito pretendido)

DO DIREITO

Como se depreende dos fatos supranarrados, o requerente tem sido vítima do crime de

Escolha o(s) crime(s):

Crime de Ameaça

Art. 147 - Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave:

Pena - detenção, de um a seis meses, ou multa.

Parágrafo único - Somente se procede mediante representação.

Crime de Falsa Identidade

Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:

Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

Crime de Calúnia

Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:

Pena - detenção, de seis meses a dois anos, e multa.

§ 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.

§ 2º - É punível a calúnia contra os mortos.

Exceção da verdade

§ 3º - Admite-se a prova da verdade, salvo:

I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;

II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;

III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.

Crime de Difamação

Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:

Pena - detenção, de três meses a um ano, e multa.

Exceção da verdade

Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.

Crime de Injúria

Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:

Pena - detenção, de um a seis meses, ou multa.

§ 1º - O juiz pode deixar de aplicar a pena:

I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;

II - no caso de retorsão imediata, que consista em outra injúria.

§ 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:

Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.

§ 3º Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião ou origem: (Incluído pela Lei nº 9.459, de 1997)

§ 3o Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência: (Redação dada pela Lei nº 10.741, de 2003)

Pena - reclusão de um a três anos e multa. (Incluído pela Lei nº 9.459, de 1997)

(Se o seu caso não se enquadra nos crimes acima, consulte o Código Penal Brasileiro)

Este(s) crime(s) tem sido perpetrado(s) a partir da utilização indevida da estrutura e dos serviços prestados pela (Colocar aqui o nome da empresa prestadora do serviço) e vem causando danos irreparáveis a minha (honra, e/ou imagem e/ou reputação). Com esta notificação, Vossa Senhoria passa a tomar conhecimento formal destes fatos criminosos perpetrados através do (colocar o nome do serviço), sob sua responsabilidade, e qualquer omissão e/ou negligência na tomada de providências imediatas ensejará a adoção das medidas cabíveis para apuração das responsabilidades cíveis e criminais.

DO PEDIDO

Considerados os fatos narrados, sem prejuízo de outras medidas extrajudiciais e judiciais cabíveis, em conjunto com o que dispõe o direito invocado, pretende o Requerente ver reconhecidas e adotadas pela (indicar aqui o nome da empresa prestadora do serviço) as seguintes providências:

1) Retirada imediata do conteúdo ilegal e/ou ofensivo do (serviço onde o material está hospedado, incluindo o(s) link(s) pertinentes), sob pena de ajuizamento da competente ação de responsabilidade.

2) Preservação de todas as provas e evidências da materialidade do(s) crime(s) e todos os indícios de autoria, incluindo os logs e dados cadastrais e de acesso do(s) suspeito(s), necessários para subsidiar a instrução do inquérito policial criminal e a competente ação judicial.

(Narrar aqui as demais providências pretendidas, caso seja necessário ao seu objetivo)

São os termos em que pede imediata providência.

(Local, data e ano).

(Nome e assinatura)

Anexo B

Pedido de quebra de sigilo de dados telemáticos para provedor que hospeda *site* . Pornografia infantil (MINISTÉRIO PÚBLICO FEDERAL, 2006, p. 58).

EXCELENTÍSSIMO SENHOR JUIZ FEDERAL DA ª VARA CRIMINAL DA SEÇÃO JUDICIÁRIA DE SÃO PAULO.

Procedimento Criminal n.º XXXXXXXX

O MINISTÉRIO PÚBLICO FEDERAL, pelo Procurador da República infra-assinado, vem respeitosamente à presença de Vossa Excelência expor e requerer o seguinte:

O presente procedimento de investigação foi instaurado para apurar veiculação de imagens pornográficas envolvendo crianças adolescentes por usuários da Rede Mundial de Computadores, em virtude de noticia criminis enviada por e-mail a esta Procuradoria.

Consta da notícia que o site www.ubbi.com.br hospeda páginas com imagens pornográficas de crianças e adolescentes. De fato, a pesquisa em referido site demonstrou existirem "álbuns" contendo imagens pornográficas de crianças e adolescentes, conforme cópias ora anexadas.

Estando presentes indícios razoáveis da materialidade e da autoria do delito tipificado no artigo 241 da Lei 8.069/90, e sendo a quebra do sigilo dos dados telemáticos o único meio possível pelo qual pode ser feita a prova, requeiro a QUEBRA DO SIGILO DE DADOS TELEMÁTICOS, devendo a empresa UBBI16 apresentar, no prazo de quinze dias, cópias em CD-R das páginas anexas, todos os dados cadastrados do autor do "álbuns" e, ainda, dos logs e IPs gerados no momento da transmissão.

São Paulo, 18 de janeiro de 2005.

Anexo C

Pedido de quebra de sigilo de dados telemáticos para concessionária de telefonia. Pornografia infantil (MINISTÉRIO PÚBLICO FEDERAL, 2006, p. 59).

3a Vara Federal Criminal da Subseção Judiciária de São Paulo
Autos n.º XXXXXXXXX

MM. Juiz:

1. Ciente da decisão prolatada às fls. 59/61.

2. Analisando-se os documentos fornecidos pelo provedor Yahoo!, juntados às fls. 45/58, verificou-se, em primeiro lugar, através dos dados cadastrais fornecidos pelo usuário do e-mail xxxxxxxxxx@yahoo.com.br (fls. 45), que o IP utilizado por ele no momento da criação da conta foi o 200.171.135.82.

Em pesquisa realizada junto ao site *registro.br*, constatou-se que o IP em questão está registrado na empresa TELECOMUNICACOES DE SAO PAULO S.A. – TELESP, sendo, portanto, este o provedor que fornece acesso à internet para o usuário.

Diante do exposto, havendo indícios razoáveis da prática de crime gravíssimo – publicação, por meio da rede mundial de computadores, de fotografias e imagens com pornografia e cenas de sexo explícito envolvendo crianças e adolescentes – requer o Ministério Público Federal a **QUEBRA DE SIGILO DE DADOS TELEMÁTICOS**, devendo a concessionária TELESP (Rua Martiniano de Carvalho, n.º 851, São Paulo/SP) informar, no prazo de 05 (cinco) dias, os dados cadastrais do usuário que se conectou à internet no dia 09 de fevereiro de 2.002, às 19h50m06s (BRST GMT – 0200) e às 16h32m09s (EST GMT – 0500), utilizando-se do IP 200.171.135.82, em ambos os horários;

São Paulo, 16 de março de 2005.

Anexo D

Endereço de delegacias especializadas em crimes cibernéticos

Policia Federal
E-mail: crime.internet@dpf.gov.br

Brasília
Polícia Civil - Divisão de Repressão aos Crimes de Alta Tecnologia (DICAT)
Endereço: SIA TRECHO 2, LOTE 2.010, 1º ANDAR, BRASÍLIA-DF.
CEP: 71200-020
Telefone: (0xx61) 3462-9533
E-mail: dicat@pcdf.df.gov.br

Espírito Santo
Polícia Civil - Núcleo de Repressão a Crimes Eletrônicos (NURECCEL)
Endereço: Av. Nossa Senhora da Penha, 2290, Bairro Santa Luiza, Vitória/ES
CEP: 29045-403
O Núcleo funciona do edifício-sede da Chefia de Polícia Civil, ao lado do DETRAN.
Telefone: (0xx27) 3137-2607
E-mail: nureccel@pc.es.gov.br

Goiás
Polícia Civil - Divisão de Repressão aos Cibercrimes (DRC) da Delegacia Estadual de Investigações Criminais (DEIC)
Av. Atilio Correa Lima, S/N, Cidade Jardim, Goiânia/GO
CEP:74425-030
Fones: (0xx62) 3201-1140 / 3201-1150 / 1144 / 1145 / 1148 / 1151
Denúncia: 197
E-mail: deic-goiania@policiaicivil.go.gov.br

Minas Gerais
Delegacia Especializada de Repressão ao Crime Informático e Fraudes Eletrônicas - DERCIFE
Av. Presidente Antônio Carlos, 901, São Cristóvão, Belo Horizonte/MG
CEP: 31.210-010
Tel: 31 3429.6026
E-mail: dercifelab.di@pc.mg.gov.br

Paraná
Polícia Civil - Núcleo de Combate aos Cibercrimes (Nuciber)
Rua José Loureiro, 376, 1º Andar, sala 1, Centro, Curitiba/PR
CEP: 80010-000

Telefone: (0xx41) 3323 9448
E-mail: cibercrimes@pc.pr.gov.br

Rio de Janeiro
Polícia Civil - Delegacia de Repressão aos Crimes de Informática (DRCI)
Endereço: Rua Professor Clementino Fraga, nº 77, Cidade Nova (prédio da 6ª DP), Rio de Janeiro/RJ
CEP: 20230-250
Telefone: (0xx21) 3399-3200/3201 ou 2242-3566
E-mails: drci@policiacivil.rj.gov.br / drci@pcerj.rj.gov.br

São Paulo
Polícia Civil - 4ª Delegacia de Delitos Cometidos por Meios Eletrônicos – DIG/DEIC
Avenida Zack Narchi,152 - Carandiru, São Paulo/SP
CEP: 02029-000
Telefone: (0xx11) 2221-7030
E-mail: 4dp.dig.deic@policiacivil.sp.gov

Anexo E

Endereços para denuncias (CRIMES PELA INTERNET, 2011).

webpol@policia-civ.sp.gov.br – Policia paulista especializada em crimes digitais.

mail-abuse@cert.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT) – Para encaminhamento de denúncias de mensagens fraudulentas (deve ser enviada uma cópia do e-mail original e também comunicar a instituição que está sendo utilizada no golpe). O site AntiSpam ensina como proceder uma denúncia.

phishing@cais.rnp.br – Centro de Atendimento a Incidentes de Segurança (CAIS) da Rede Nacional de Ensino e Pesquisa (RNP) – Para encaminhamento de denúncias mensagens fraudulentas (deve ser enviada uma cópia do e-mail original e também comunicar a instituição que está sendo utilizada no golpe).

artefatos@cais.rnp.br – Centro de Atendimento a Incidentes de Segurança (CAIS) da Rede Nacional de Ensino e Pesquisa (RNP) – Para encaminhamento de denúncias de aplicativos suspeitos (cavalos-de-tróia e outros programas maléficos usados nos golpes online).

crime.internet@dpf.gov.br – Mensagens que se refiram aos crimes de internet devem ser reportadas ao novo canal centralizador dessas denúncias na Divisão de Comunicação Social da Polícia Federal.

reclameaqui.net – Site para quem costuma fazer comprar ou usar serviços pela internet, bom para tirar dúvidas, fazer reclamações ou pesquisar empresas fraudulentas.

ic3.gov- Internet crime Complaint Center – Site para denunciar crimes digitais internacionais.

denunciar.org.br – Safernet Brasil – é uma organização não governamental que reúne especialistas para combater crimes digitais. O que denunciar? Pornografia Infantil, Racismo, Xenofobia e Intolerância religiosa, Neonazismo, Apologia e Incitação a crimes contra a Vida, Homofobia, Apologia e Incitação a práticas cruéis contra animais, entre outros.

Hot Line – Denúncias para casos de pedofilia.