DO SIGILO DOS DADOS CADASTRAIS DE CLIENTES DO PROVEDOR DE ACESSO À INTERNET: ALGUMAS CONSIDERAÇÕES SOBRE A PROVA DE UM CRIME EM UM CONTEXTO DIGITAL

Mário Furlaneto Neto[1]

José Eduardo Lourenço dos Santos[2]

Resumo: Quando se abordam delitos cometidos por meio da *Internet*, surge, logo de início, a preocupação sobre como se irá realizar a investigação criminal e como se produzirá a prova processual. Partindo-se da análise de hipóteses de delitos praticados por meio da *Internet*, mediante uma revisão crítica bibliográfica, busca-se nas linhas que se seguem, traçar uma idéia clara e simples, do que se pode fazer no campo da prova, com respeito à legislação penal e processual penal em vigor, bem como os Direitos Fundamentais previstos constitucionalmente. Conclui-se, neste contexto, pelo papel preponderante da vítima na preservação dos indícios e vestígios eletrônicos, bem como pela necessidade de interação entre os profissionais do Direito, da Ciência da Computação e de outras Ciências afins, para o sucesso da persecução criminal.

Palavras-chave: Prova. Delitos informáticos. Internet.

Abstract: When crimes committed by means of *Internet* are approached, what causes one to worry right from the beginning is how investigation will be conducted into and how procedural evidence will be produced. From hypotheses analysis of *Internet-based* crimes, and through critical bibliographical review, the main purpose of this paper is to give a simple and clear idea of what can be done in view of producing evidence, with regard to penal and procedural legislation in force as well as to Fundamental Rights due to Constitution. In such context, conclusion is for victim's preponderant role concerning electronic signs and traces as well as in the need for interaction between professionals belonging to different fields such as Law, Computing Sciences and other sciences alike to achieve penal persecution.

Keywords: Evidence. Computer crimes. Internet

1 Doutor em Ciência da Informação (UNESP-Marília/SP). Delegado de Polícia. Professor do UNIVEM-Marília/SP. E-mail: *mariofur@flash.tv.br*.

2 Mestre em Direito (UNIVEM-Marília/ SP). Delegado de Polícia. Professor do UNIVEM-Marília/SP. E-mail: *jels@univem.edu.br*.

Resumen: Cuando se abordan delitos cometidos por medio de Internet, surge, de inmediato, la preocupación sobre como se realizará la investigación criminal y como se producirá la prueba procesal. Partiendo del análisis de hipótesis de delitos practicados por medio de Internet, mediante una revisión crítica bibliográfica, se busca en las líneas a continuación, trazar una idea clara y simple de lo que se puede hacer en el campo de la prueba al respecto de la legislación penal y procesal penal en vigor, así como también los Derechos Fundamentales previstos constitucionalmente. Se concluye, en este contexto, por el papel preponderante de la víctima en la preservación de los indicios y vestigios electrónicos, así como por la necesidad de interacción entre los profesionales del Derecho, de la Ciencia de la Computación y de otras Ciencias semejantes, para el éxito de la persecución criminal.

Palabras-clave: Prueba. Delitos informáticos. Internet.

INTRODUÇÃO

Um cracker, morador em Brasília, mediante o emprego de um keylog[34], subtrai a senha e dados da conta bancária de um internauta morador de Marília. Posteriormente, acessa-a via home banking e sem provocar suspeita, transfere eletronicamente um valor considerável em dinheiro para uma certa conta corrente, alugada de um terceiro, junto a uma instituição bancária situada em Goiânia. Na seqüência, exaurindo o crime, saca parte do dinheiro depositado na conta de aluguel, de forma a deixar ali apenas o montante correspondente à locação da conta bancária.

O evento, ficticiamente criado para demonstrar o panorama do crime em um contexto digital, vem crescendo esponencialmente no cenário nacional e internacional (COELHO, 2004), a ponto de estimar-se um prejuízo, somente no primeiro semestre deste ano, em cerca de cento e setenta milhões de reais (SANTOS; FURLANETO NETO, 2004), de forma a ultrapassar o dano estipulado pelos crimes de roubo em casas bancárias.

Em um outro exemplo, um e-mail circula pela rede, enviado aos conhecidos de A, bem como a ele diretamente, chamando-o de incapaz, dentre outros adjetivos, de forma a macular a sua honra subjetiva.

Assim, neste novo cenário, em que o autor do crime não mostra o seu rosto, oculta sua identidade e deixa apenas vestígios eletrônicos para serem rastreados, a fim de se ligar a vítima ao criminoso, é que se deve desenvolver a investigação criminal.

Nesse contexto, a prova material a ser produzida para a apuração da autoria do crime merece especial destaque, mormente em decorrência do ônus da prova.

Pretende-se neste artigo, abordar algumas questões pertinentes à preservação da prova em um contexto digital, a fim de que os órgãos encarregados da investigação criminal possam chegar a tecer diligências visando a elucidar a autoria do crime digital. Não abordaremos, neste estudo, a questão da extraterritorialidade, que poderá se verificar quando ocorrer a transnacionalidade do delito praticado por meio da informática, isto é, naqueles crimes cujo agente possui uma conta de e-mail em um provedor hospedado no exterior, fora do domínio .br, de onde inicia a conduta que vem a atingir um bem jurídico tutelado pelo ordenamento jurídico pátrio, por se tratar de assunto complexo e que merece abordagem específica.

Porém, antes de atingirmos o objetivo específico do artigo, faz-se necessário discutirmos a natureza jurídica do provedor de acesso à Internet, bem como o sigilo dos dados cadastrais de clientes do provedor.

1 NATUREZA JURÍDICA DO PROVEDOR DE ACESSO À *INTERNET*

Se por um lado o provedor significa aquele que alimenta a rede com informações, por outro viabiliza a conexão de alguém à rede, sua entrada no ciberespaço. Existe, portanto, o provedor de informações e o provedor de acesso, cujas atividades podem ser ou não remuneradas.

Tanto no Brasil como no mundo, os provedores são intermediadores que oferecem o acesso à Internet mediante linha telefônica ou outro meio adequa-

3 *Keylog* ou cavalo de tróia é um vírus que permite a captura de dados informáticos. Alguns cavalos de tróia permitem até a interceptação ambiente clandestina.

do para a comunicação entre duas pessoas, tais como ondas de rádio ou cable. Utilizando uma figura de linguagem, o provedor seria apenas uma chave que destranca a porta da rede mundial, que por sua vez libera um espaço virtual.

Assim, os provedores não realizam o transporte de sinais de telecomunicações, mas tão somente utilizam o sistema de transporte de sinais já existente. Ao estabelecer a conexão do usuário com a Internet, seja via Embratel ou por qualquer outro meio disponível, os provedores de acesso utilizam-se da rede pública de telecomunicações, unicamente para permitir a conexão do usuário com a rede mundial através da linha telefônica ou por outro meio adequado.

Em outras palavras, seguindo o entendimento de Lima Júnior (2003), primeiramente temos a ação do usuário enviando dados ao seu provedor mediante um serviço de informações, explorado pela União. Posteriormente temos armazenamento, apresentação, movimentação ou recuperação desses dados pelo provedor de acesso, executando uma atividade meramente privada. Por derradeiro, temos a relação deste provedor de acesso com outros provedores através de um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde.

Percebe-se, assim, que todos os dados de conexões ou fluxo de informações, ou seja, o caminho percorrido na grande rede por quem a ela tem acesso, pode ser identificado pelo chamado provedor, que, para tanto, se faz valer do IP (Internet Protocol), protocolo identificador de cada máquina conectada.

Neste contexto, a atividade dos provedores de acesso à Internet é considerada como serviço de valor adicionado e não como serviço de telecomunicações.

Serviço de valor adicionado é aquela atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte, e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações.

Pela interpretação dos artigos 60 e 61 da Lei n. º 9.472, de 16 de julho de 1997, publicada no Diário Oficial da União de 17 de julho de 1997, o serviço de valor adicionado não constitui serviço de telecomunicações, razão pela qual, no entendimento de Lima Júnior (2003), o provedor se classifica como pessoa jurídica de direito privado, com os direitos e deveres inerentes a essa condição.

O tema abordado nesta seção é de importância ímpar para fundamentar o assunto a ser tratado na próxima, onde discutiremos a questão do sigilo dos dados cadastrais de clientes do provedor de acesso à Internet, por possuir relevância na investigação do crime praticado por meio da informática e, no caso, para o delito de pornografia infantil.

2 DO SIGILO DOS DADOS CADASTRAIS DE CLIENTES DO PROVEDOR DE ACESSO À INTERNET

Superada a fase de identificação do IP, a importância da análise dos dados cadastrais de clientes do provedor de acesso à Internet se deve ao fato de ser imprescindível para o esclarecimento da autoria do delito, pois somente o provedor poderá informar, na data e horário preciso, os dados do internauta cujo equipamento foi utilizado para a perpetração da conduta ilícita.

A questão ganha maior controvér-

sia quando se passa a analisar a redação do inciso XII do artigo 5º da CF[45].

Isso porque o sigilo absoluto foi imposto como regra, sendo exceção a sua quebra, que somente poderá ser autorizada nos casos expressamente previstos na Lei nº 9296, de 24 de julho de 1996, desde que estejam relacionados à prática de delitos.

Imediatamente é levantada a seguinte hipótese: o sigilo relativo a que o legislador impôs ao utilizar a expressão "salvo, no último caso", aposta na parte final do inciso ora comentado, quer se referir apenas ao sigilo telefônico ou se estende também ao sigilo de correspondência e de dados?

A incorreta grafia utilizada pelo legislador fez surgir três correntes: os que defendem que somente pode ser quebrado o sigilo de comunicações telefônicas, com observância restrita dos critérios legais; aqueles que entendem haver dois grupos, o da correspondência, cujo sigilo é absoluto, e o das comunicações telegráficas, de dados e comunicações telefônicas, em que o sigilo seria relativo; e a corrente em que o entendimento prevalecente é o de que o sigilo absoluto abrangeria o grupo das comunicações telegráficas e correspondência, havendo sigilo relativo quanto ao grupo das comunicações telefônicas e de dados.

Pela relevância e implicações diretas no procedimento investigatório dos crimes praticados por meio da informática, passaremos a discorrer sobre os fundamentos jurídicos de todas as correntes, porém, antes de entrarmos nessa seara, necessário se torna definir o termo "dados" utilizado pelo legislador.

A esse respeito, denominando "dados pessoais", Tucci (1993, p. 428) entende se tratar de informações particulares e íntimas do indivíduo, confidenciais, podendo ser quaisquer dados, inclusive os informáticos, enquanto, para Cretela Júnior (1988, p. 269), se referem a informações sobre as pessoas.

Fazendo considerações sobre a privacidade no comércio eletrônico, Kaku (2000, p. 89-90) entende ser ponto capital a inviolabilidade do sigilo de dados para o comércio eletrônico. Sob forma abrangente, define dado como sendo tudo o que trafega na Internet, não importando que seja "uma simples pesquisa ou o cadastro que se aceita fazer através da rede". Considera, inclusive, "imagens que possam ser armazenadas sob qualquer meio ou forma". Conclui afirmando que "dado é uma informação armazenada, não importando por quanto tempo e que diz respeito aos atos e fatos nossos do dia-a-dia".

Abordando aspectos constitucionais da lei que regulamentou o processo de escuta telefônica e os fluxos de comunicações estabelecidos em sistemas de informática e telemática, Hoeshl (2000, p. 105-106) discorda dos autores por entender que o dispositivo constitucional trata de formas de comunicações, quer sejam por telefone, carta, telegráfica ou transmissão de dados, elevando essa última a meio de comunicação.

O autor sustenta seu entendimento ao resgatar definições esculpidas no Decreto 97.057, de 10 de novembro de 1988, em que os serviços de telecomu-

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

XII – é inviolável o sigilo de correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

nicações são classificados quanto à forma em telegrafia, telefonia, televisão, transmissão de dados, teledifusão e outras formas[5][6]. (Grifo nosso).

Aprofunda-se ainda mais ao estabelecer a diferença entre transmissão de dados e comunicação de dados, aquela constituída pelo envio, e esta, mais abrangente, por envolver, também, o recebimento, de forma a definir todo o processo.

Culmina trazendo à colação a definição legal de dado, caracterizada pela "informação sistematizada, codificada eletronicamente, especialmente destinada a processamento por computador e demais máquinas de tratamento racional e automático da informação[6]", para concluir que a expressão "dados" contida no texto constitucional significa comunicação de dados, "forma de comunicação, paralela às demais ali apresentadas".

Nesse aspecto, o direito comparado traz uma grande contribuição para a questão, pois a Diretiva 46/1995 do Parlamento Europeu e do Conselho da União Européia, norte para uma legislação assemelhada em todos os países membros, disciplinou dados não como meio de comunicação, mas sim como dados pessoais. Assim, para a Diretiva, consideram-se dados pessoais toda informação sobre uma pessoa física identificada ou identificável; aborda o tratamento dos dados pessoais mediante qualquer processo que vise a guarda, registro, organização, conservação, elaboração ou modificação, extração, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma que lhes facilite o acesso, cotejo ou interconexão, assim como bloqueio, supressão ou destruição de referidos dados. (Grifo nosso).

Com base nessa Diretiva, a Espanha, um dos membros da Comunidade Européia – CE, editou a Lei Orgânica nº 15, de 13 de dezembro de 1999, disciplinando a proteção de dados de caráter pessoal, tendo a doutrina, com base na análise legislativa, classificado os dados pessoais em públicos e privados. Os dados pessoais públicos são os conhecidos por um número indeterminado de pessoas, sem que o titular possa identificar a origem e forma de propagação, como por exemplo, a lista de pessoas que pertençam a grupos profissionais contendo apenas dados de nome, título, profissão, atividade, grau de instrução, direção e indicação de que pertença ao grupo, etc. Os privados, aqueles em que a pessoa se abriga em fornecê-los a terceiros em situação tratada e regulamentada por lei.

A respeito dos dados pessoais privados, a doutrina os subdividiu em íntimos e secretos. Consideram-se íntimos aqueles em que a pessoa pode proteger sua difusão frente a qualquer um, mas se obriga a revelá-los em cumprimento a suas obrigações cívicas, como, por exemplo, ao prestar informações tributárias ou em caso de insolvência

5 Art. 4º. Os serviços de Telecomunicações, para os efeitos deste Regulamento Geral, dos Regulamentos Específicos e Normas Reguladoras Complementares, compreendendo a transmissão, emissão ou recepção de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza por fio, rádio, eletricidade, meios ópticos ou qualquer outro processo eletromagnético, classificam-se do seguinte modo:

I – quanto à forma de telecomunicação empregada:

a) telegrafia;

b) telefonia;

televisão;

transmissão de dados;

teledifusão;

outras formas.

6 Cf. art. 6º, item 23 do Decreto 97.057/1988.

econômica. Os dados pessoais secretos são subdivididos em sensíveis e sensibilíssimos. Os sensíveis são aqueles em que a pessoa não está obrigada a fornecê-los a ninguém, salvo em casos excepcionais tratados em lei, como, por exemplo, vida sexual e saúde, enquanto os dados pessoais secretos sensibilíssimos estariam sujeitos a uma tutela mais rígida, não havendo obrigação de sua revelação por nenhum motivo, salvo por disposição de seu titular, como, por exemplo, dados sobre ideologia, filiação sindical, religião ou crenças.

Em que pese a legislação espanhola prever um controle sobre todos os dados pessoais, tanto públicos como privados, não pretendeu obstaculizar o fluxo de informações, mas sim evitar danos a outros interesses legítimos, servindo como instrumento de regulamentação e racionalização de sua circulação, tanto assim que o direito à intimidade somente tutelou os dados privados, em especial os secretos.

O Conselho da União Européia e o Parlamento Europeu ampliou o alcance da Diretiva 46/1995, ao editar a Diretiva 58, de 12 de julho de 2002, que estabeleceu regras claras sobre o tratamento de dados pessoais e a proteção da intimidade no setor das comunicações eletrônicas.

No que se refere ao tratamento de dados pessoais, a nova Diretiva estabeleceu que os Estados membros garantirão, por de legislação própria, a confidencialidade das comunicações e de dados de tráfego associadas a elas, realizadas pelas redes públicas de comunicações e os serviços de comunicações eletrônicas disponíveis ao público, cujo contexto se insere a Internet, proibindo, em particular, a escuta, a gravação, o armazenamento e outros tipos de intervenção ou vigilâncias das comunicações ou dados de tráfego associado a elas por pessoas distintas das dos usuários interessados.

Ressalvou as hipóteses de limitações legais que poderão ser adotadas por lei pelos países membros quando forem medidas necessariamente proporcionais e apropriadas em uma sociedade democrática para proteger a segurança nacional, a defesa, a segurança pública, a prevenção, a investigação, o desvendamento da autoria e a persecução de delitos, incluindo, nessas hipóteses, a possibilidade de armazenamento dos dados por prazo limitado para que os encarregados das investigações cumpram suas metas com o máximo de eficiência possível.

Disciplinando sobre os serviços da sociedade de informação, em cujo contexto se insere a Internet, e o comércio eletrônico, a Lei Orgânica espanhola n. 34, de 11 de julho de 2002, previu, por parte dos provedores de acesso a Web, a retenção de dados de conexão e tráfego gerados pela comunicação, pelo prazo máximo de doze meses, visando a conservá-los como marco para uma investigação criminal, bem como para a salvaguarda da segurança pública ou defesa nacional, obrigando ao fornecimento das informações mediante requisição judicial.

Como vimos, a legislação espanhola, seguindo diretrizes do Parlamento Europeu e do Conselho da União Européia, tratou distintamente a questão dos dados pessoais e do tratamento desses dados, impondo como regra o sigilo dos dados pessoais particulares e o seu tratamento, mas impondo mecanismos judiciais para a revelação nos casos em que legalmente o interesse público seja preponderante.

Analisados alguns conceitos doutrinários sobre as definições da expressão “dados”, empregada pela Constituição, comparando-se com o direito

alienígena, passaremos a analisar as correntes que abordam a questão da tutela absoluta ou relativa do sigilo das comunicações prevista no texto constitucional.

Após agrupar as garantias individuais em função de seu objeto, discorrendo sobre direito à segurança, Silva (1990) deixa evidente ser apenas admissível a quebra do sigilo das comunicações telefônicas, conferindo um caráter de sigilo absoluto às demais hipóteses. Para o autor, a norma tutela a liberdade de manifestação e pensamento, de um lado, e de outro, o segredo, como expressão do direito à intimidade.

Na mesma linha de raciocínio, Tucci (1993, p. 432) entende ser absoluta a vedação de quebra do sigilo de correspondência, das comunicações telegráficas e de dados pessoais, somente podendo ser admitida a quebra do sigilo de comunicações telefônicas, na forma da lei.

Esposando o mesmo entendimento, Hoeschl (2000) acrescenta haver exceções à regra da tutela absoluta do sigilo de comunicações telegráficas, comunicações de dados e das correspondências, nas hipóteses de estados de sítio e de defesa, previstas nos artigos 136[7][8] e 139[8][9] da CF. Em sua opinião somente no estado de sítio é que será permitida interceptação da comunicação de dados, possibilidade que não se admite no estado de defesa.

Conclui o autor ser inconstitucional o parágrafo único da Lei 9.296/1996[9][10] que expandiu a interceptação telefônica, como meio de prova, para os fluxos de comunicações estabelecidos em sistemas de informática e telemática.

Igual entendimento, no que tange, inclusive, à inconstitucionalidade do parágrafo único da Lei 9.296/1996, defende Greco Filho (1996, p. 11-12), para quem o texto da CF admite duas interpretações possíveis: "a ressalva, considerando-se a expressão 'no último caso', aplica-se às comunicações telegráficas, de dados e às comunicações telefônicas, ou aplica-se somente às comunicações telefônicas".

Em seus argumentos, o autor aduz que:

> [...] se a Constituição quisesse dar a entender que as situações são apenas duas, e quisesse que a interceptação fosse possível nas comunicações telegráficas, de dados e das comunicações telefônicas, a ressalva estaria redigida não como 'no último caso', mas como no 'segundo caso'. Ademais, segundo os dicionários,

7 [8] Art. 136. O Presidente da República pode, ouvidos o Conselho da República e o Conselho de Defesa Nacional, decretar estado de defesa para preservar ou prontamente restabelecer, em locais restritos e determinados, a ordem pública ou a paz social ameaçadas por grave e iminente instabilidade institucional ou atingidas por calamidades de grandes proporções na natureza.

8 [9] Art. 139. Na vigência do estado de sítio decretado com fundamento no artigo 137, I, só poderão ser tomadas contra as pessoas as seguintes medidas:

[...]

III – restrições relativas à inviolabilidade da correspondência, ao sigilo das comunicações, à prestação de informações e à liberdade de imprensa, radiodifusão e televisão, na forma da lei;

9 [10] Art. 1º. A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.

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

último caso significa derradeiro, o que encerra, e não, usualmente, o segundo.

Discorrendo sobre questões pertinentes à interceptação telefônica, Rangel (2000) defende posição diversa das até aqui apresentadas. Para o autor, "o dispositivo constitucional está dividido em dois grupos", o primeiro, abrangendo o sigilo da correspondência e das comunicações telegráficas, e o segundo, o das comunicações telefônicas e de dados, de maneira que "a expressão 'último caso' açambarcaria dados e comunicações telefônicas".

Para justificar a tese de que o legislador constituinte quis e permitiu a quebra do sigilo de dados, sejam dados das comunicações telefônicas ou quaisquer outros dados de comunicação, foi enfático ao dizer que ao

> defendermos tese diferente estaríamos imaginando que o Constituinte somente se preocupou com a comunicação via telefone deixando de fora a comunicação de dados sem o uso de telefone. Ou seja, o criminoso da era da informática, ou o criminoso via satélite, ou da fibra óptica, ou ainda o que utilizasse infravermelho estaria protegido diante da norma constitucional. Nada mais errado (Rangel, 2000).

Em artigo em que tece comentários sobre a Comissão Parlamentar de Inquérito – (CPI) e a quebra do sigilo telefônico, Gomes (2002) empresta os ensinamentos de Grinover (1990, p. 60) para conferir relatividade aos direitos fundamentais, assim se expressando:

> O ponto de partida para o verdadeiro entendimento do assunto reside em reconhecer a 'relatividade' dos direitos fundamentais (muitos chamados de 'liberdades públicas no antigo direito francês). 'É cediço', enfatiza Ada P. Grinover, 'na doutrina constitucional moderna, que as liberdades públicas não podem ser entendidas em sentido absoluto, em face da natural restrição resultante do princípio da convivência das liberdades, pelo que não se permite que qualquer delas seja exercida de modo danoso à ordem pública e às liberdades alheias'. Deve-se reconhecer, enfatizam alguns comentaristas da Constituição de 1988, que o princípio do sigilo absoluto, algumas vezes, não se coaduna com a realidade e a necessidade sociais. Os dados pessoais, em conclusão, seja no momento de uma comunicação (telefônica ou por outra forma), sejam os armazenados (estanques), não gozam de sigilo absoluto.

Admite o autor ser possível a quebra judicial de dados pretéritos e estanques, tais como data, hora e tempo de duração das ligações, bem como núme-

ros dos telefones que foram utilizados para os diálogos, desde que para instruir investigação policial ou persecução judicial, justificando a limitação da tutela do sigilo, "tanto pela prevalência em alguns casos concretos do interesse público quanto pela 'convivência' das liberdades entre os particulares".

Porém, salienta que

> [...] nenhum direito fundamental pode sofrer restrição sem a intervenção do legislador (isto é, sem a interpositio legislatoris). De qualquer modo, não são poucas as leis no Brasil que autorizam a ingerência nos dados alheios. Assim, Código Tributário Nacional, art. 198, Código de Processo Civil, art. 399, Lei Federal nº 3.470/58, art. 54, Lei Complementar nº 75/93 (Lei Orgânica do Ministério Público da União), Lei nº 8.625/93 (Lei Orgânica Nacional do Ministério Público), etc. Havendo requerimento do Ministério Público, por exemplo, por força das suas leis orgânicas, já está atendido o princípio da legalidade.

Em seu entendimento, deve ainda a Autoridade Judiciária analisar com imperatividade no momento da decisão, o princípio da proporcionalidade, pois "não é qualquer caso de investigação criminal ou instrução penal que justifica tal medida, tão invasora da intimidade alheia".

Em uma visão mais ampla, sob o ponto de vista da finalidade ética e social da garantia constitucional, Grinover (1990, p. 68) sustenta a inviolabilidade do sigilo de correspondência e das comunicações telegráficas e telefônicas, de maneira que "pode a lei (como o faz) abrir exceções ao princípio, sem que com isso se configure qualquer inconstitucionalidade".

Nesse sentido a autora arremata dizendo que "tal entendimento não pode significar a aniquilação do preceito constitucional, devendo a lei conter as exceções dentro de limites razoáveis, que não ponham por terra a garantia".

Em análise à admissibilidade da prova ilícita por derivação[10][11] no processo penal, mormente nas hipóteses de interceptações telefônicas e escutas clandestinas, Capez (1998, p. 32-33) entende não se justificar a postura inflexível de se desprezar, sempre, tais provas, sob o argumento de que em caso de conflitos entre princípios fundamentais da Constituição, deve prevalecer sempre o de maior valor, evitando-se, assim, um mal maior, citando como exemplos uma eventual condenação injusta ou a impunidade de perigosos marginais.

Justifica a sua tese sob o argumento de que

> [...] o direito à liberdade (no caso da defesa) e o direito à segurança, à proteção à vida, do patrimônio etc. (no caso da acusação) muitas vezes não podem ser restringidos pela prevalência do direito à intimidade (no caso das interceptações telefônicas e das gravações clandestinas) e pelo princípio da proibição das demais provas ilícitas.

10 [11] Segundo Capez (1998, p. 31), as chamadas provas ilícitas por derivação "são aquelas em si mesmas lícitas, mas produzidas a partir de outra ilegalmente obtida".

Segue seu raciocínio dizendo que "no caso de princípios constitucionais contrastantes, o sistema faz atuar um mecanismo de harmonização que submete o princípio de menor relevância ao de maior valor social", admitindo, assim, a aplicação do princípio da proporcionalidade, cuja origem se desenvolveu na Alemanha (Verhaltnismassigkeitsprinzip), no período pós-guerra.

A doutrina e a jurisprudência dominante são no sentido de que a prova favorável ao réu pode ser utilizada em seu favor, ainda que colhida com infringência a direitos fundamentais seus ou de terceiros (prova ilícita pro reo), porém, antes da entrada em vigor da lei 9.296/1996, em análise com o contexto das demais provas obtidas por meio lícito, julgado da 6ª Turma do STJ, nos autos do HC 3.982/RJ, em 5-12-1995, publicado no DJU, em 26 fev. 1996, p. 4084, o relator, Min. Adhemar Maciel, contrariando posição do STF, a reconheceu como também admissível a favor da acusação (*pro societate*), cujo acórdão diz:

> Constitucional e processo penal. Hábeas Corpus. Escuta telefônica com ordem judicial. Ré condenada por formação de quadrilha armada, que se acha cumprindo pena em penitenciária, não tem como invocar direitos fundamentais próprios do homem livre para trancar ação penal (corrupção ativa) ou destruir gravação feita pela polícia. O inciso LVI do art. 5º da Constituição, que fala que 'são inadmissíveis [...] as provas obtidas por meio ilícito', não tem conotação absoluta. Há sempre um substrato ético a orientar o exegeta na busca de valores maiores na construção da sociedade. A própria Constituição Federal Brasileira, que é dirigente e pragmática, oferece ao juiz, através da 'atualização constitucional' (Verfassungsaktualisierung), base para o entendimento de que a cláusula constitucional invocada é relativa. A jurisprudência norte-americana, mencionada em precedente do Supremo Tribunal Federal, não é tranqüila. Sempre é invocável o princípio da 'Razoabilidade' (Reasonableness). O princípio da exclusão das provas ilicitamente obtidas (Exclusionary Rule) também lá pede temperamentos. Ordem denegada[11][12].

Mais recentemente, sob a vigência da Lei 9.296/1996, julgado pioneiro do Tribunal Regional do Trabalho da 10ª região, nos autos do processo 504/2002 RO, reconheceu a justa causa para a demissão de funcionário que

11 [12] Cf. CAPEZ, 1998, p. 34-35.

fez uso indevido de e-mail da empresa, reconhecendo a aplicação do princípio da proporcionalidade, em que pese a proteção à individualidade, à liberdade ou à privacidade, ser essencial no respeito ao Estado de Direito, sob o argumento de que essa proteção não pode ser absoluta, de forma a resultar no desrespeito a outras garantias de igual relevância, sob pena de serem violados outros direitos, senão maiores, de igual importância, ou que, igualmente precisam ser preservados. A ementa do acórdão diz:

> 26.06.2002 – Envio de e-mail – Justa Causa (HSBC). RO 0504/2002 Relatora: Juíza Márcia Mazoni Cúrcio Ribeiro. Revisor: Juiz Douglas Alencar Rodrigues Recorrente: HSBC Seguros Brasil S/A. Recorrente: Omitido. Recorrido: Os mesmos. Origem: 13ª Vara do Trabalho de Brasília DF (Juiz José Leone Cordeiro Leite). EMENTA: JUSTA CAUSA. E-MAIL. PROVA PRODUZIDA POR MEIO ILÍCITO. NÃO-OCORRÊNCIA. Quando o empregado comete um ato de improbidade ou mesmo um delito utilizando-se do e-mail da empresa, esta em regra, responde solidariamente pelo ato praticado por aquele. Sob este prisma, podemos então constatar o quão grave e delicada é esta questão, que demanda a apreciação jurídica dos profissionais do Direito. Enquadrando tal situação à Consolidação das Leis do Trabalho, verifica-se que tal conduta é absolutamente imprópria, podendo configurar justa causa para a rescisão contratual, dependendo do caso e da gravidade do ato praticado. Considerando que os equipamentos de informática são disponibilizados pelas empresas aos seus funcionários com a finalidade única de atender às suas atividades laborativas, o controle do e-mail apresenta-se como a forma mais eficaz, não somente de proteção ao sigilo profissional, como de evitar o mau uso do sistema Internet que atenta contra a moral e os bons costumes, podendo causar à empresa prejuízos de larga monta.

O debate doutrinário a respeito da questão faz surgir um outro ponto crítico, pois, salvo na hipótese da corrente que admite a quebra do sigilo das comunicações de dados, ainda que pela adoção do princípio da proporcionalidade, qualquer outra interpretação doutrinária fará com que os crimes praticados por meio da informática dificilmente sejam investigados no Brasil, tornando o país um verdadeiro paraíso do crime informático, por não se admitir o rastreamento de e-mails ou a quebra do sigilo de comunicação de dados. Ademais, entendendo-se pela tutela absoluta de tais garantias, por se tratarem de clausula pétrea, o ordenamento jurídico somente poderia ser modificado pela formação de um novo

Estado, mediante a instalação de uma nova assembléia constituinte.

Importa dizer que a privacidade do usuário encontra-se regulamentada no inciso X do artigo 5º da CF, ao prever serem "invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação", bem como na Lei n.º 8.078/90 - Código de Defesa do Consumidor, de maneira que o legislador pátrio tomou a cautela de responsabilizar o provedor e a autoridade requisitante quando houver divulgação indevida dos dados pessoais do usuário ou das comunicações de dados, haja vista a imposição de sigilo absoluto ao procedimento que decretar sua quebra.

3 BREVES CONSIDERAÇÕES SOBRE A PROVA

No processo penal, a prova destina-se à formação da livre convicção do juiz acerca da existência ou não de um fato, suas circunstâncias, além da falsidade ou veracidade de uma afirmação, sobre os quais pesam incerteza, dúvida, e que, por suas relevâncias, precisam ser cabalmente demonstradas perante o julgador para que a causa tenha o seu deslinde.

Segundo Tourinho Filho (2003, p. 215-216) "provar significa fazer conhecer a outros uma verdade conhecida por nós. Nós a conhecemos: os outros não". Dentro desse contexto, o autor enfatiza que para efetivar a prova, deve a parte "apresentar os necessários meios para que dela tomem conhecimento".

Salvo os fatos axiomáticos ou intuitivos[12][13], os notórios[13][14], as presunções legais[14][15] e os fatos inúteis[15][16], todos os restantes devem ser provados por quem tem interesse em alegar (ônus da prova), inclusive o fato admitido ou aceito[16][17]. Deve a prova ser admissível pela lei e costumes judiciários, ser pertinente ou fundada em relação ao processo, visar a esclarecer uma questão controvertida e ser possível a sua realização.

Por vigorar no processo penal o princípio da verdade real, "não há de se cogitar qualquer espécie de limitação à prova, sob pena de se frustrar o interesse estatal na justa aplicação da lei" (CAPEZ, 2003, p. 263). Ocorre que esse princípio da liberdade probatória não é absoluto, sofrendo restrições em algumas hipóteses legais, em que somente se admite a prova mediante certas formalidades, como, por exemplo, no estado de pessoa (casamento, morte, parentesco) em que a prova somente pode ser feita com a respectiva certidão.

Assim, de forma não taxativa e com valor relativo, o código de processo penal admitiu como meio de prova

12 [13] Aqueles que são evidentes, como por exemplo, nos casos em que as lesões externas forem de tal monta que tornam evidente a morte da vítima, sendo dispensado o exame de corpo de delito intermo.

13 [14] Aqueles cujo conhecimento faz parte da cultura de uma sociedade. Desnecessária a prova de que o fogo queima e que a água molha.

14 [15] Decorrentes da própria lei, podendo ser absolutas (*jure et de jure*) e que, portanto, não admitem prova em contrário, como, por exemplo, a nacionalidade do filho de brasileiros, nascido no Brasil, ou relativas (*juris tantum*), em que se admitem prova em contrário, como a presunção de paternidade na hipótese do filho nascido na constância de um casamento.

15 [16] Fatos que não influenciam na solução da causa.

16 [17] Também chamado fato incontroverso, pois foi admitido pela parte. Diferentemente do processo civil, em que vigora a verdade ficta, o processo penal não adotou a presunção de veracidade quanto o fato admitido pela parte.

a produção de perícia, o interrogatório do acusado, a confissão, perguntas formuladas ao ofendido, oitiva de testemunhas, reconhecimento de pessoas ou coisas, acareações, a prova documental, bem como os indícios, prevendo como acautelatória a medida de busca e apreensão de coisas ou pessoas.

É dentro deste contexto que a investigação criminal deverá ocorrer, sem, jamais, desrespeitar os direitos e garantias individuais expressos na Carta Magna, tidos como fundamentais.

Levando-se em consideração o ônus da prova, deverá a acusação fazer prova da autoria e materialidade do delito, caso queira que a sua pretensão seja reconhecida pelo juiz, no ato da entrega da prestação jurisdicional.

Em razão disso, mister se faz tecermos alguns comentários sobre a preservação da prova em um contexto digital, pois, deve o agente do direito valer-se dos dispositivos legais que tem ao seu alcance.

4 PRESERVAÇÃO DA PROVA EM UM CONTEXTO DIGITAL

Resgatando o primeiro exemplo utilizado no preâmbulo do artigo, para fins didáticos, levaremos em consideração que o keylog foi introduzido no hd – hard disc do internauta por meio de um e-mail indesejado, o que possibilitou o cracker obter informações preciosas como o número da conta bancária, agência e senha do home banking.

Um primeiro questionamento se impõe: assim que o internauta constatar que o seu computador foi invadido, deve imediatamente desligar o computador?

Em que pese ser esta a conduta instintiva a ser tomada pelo internauta, normalmente dotado de conhecimentos mínimos em informática, para Montanaro Barrales[17][18], o ideal é desligar a Internet, sem desligar o CPU, bem como interpelar o provedor para preservar os arquivos logs[18][19], de forma a não perder dados importantes para o rastreamento. Assim, nesse contexto, a vítima tem papel fundamental para a preservação da prova material.

A interpelação ao servidor se faz necessária em decorrência de o Brasil não possuir legislação que o obrigue a manter o tráfego ou arquivos logs de seus clientes, diferentemente da legislação espanhola, por exemplo.

Concomitantemente, deve ser comunicada a polícia civil para que esta, juntamente com o perito oficial ou louvado possa tomar as providências pertinentes.

Ressalte-se que nem sempre há, em um primeiro momento, a necessidade de autorização judicial para se chegar ao IP do suspeito, diante desse dado ser de domínio público e ser acessado por qualquer um que tenha conhecimento técnico para tal. Após a identificação do IP, deverá o provedor fornecer os dados cadastrais do cliente, sem que, para tanto, seja necessária autorização judicial, porém, para a confirmação dos dados obtidos no ato da investigação criminal preliminar, com os arquivos logs mantidos pelo provedor, necessário se faz ordem judicial, em decorrência do disposto no inciso XII do artigo 5º da CF.

No que tange ao descobrimento

17 [18] O autor, Domingo Martin Montanaro Barrales, é perito em segurança eletrônica e proferiu recente palestra no Fórum sobre Direito Eletrônico, organizado pelo IPEC – Instituto Paulista de Educação Continuada, realizado em novembro, na cidade de São Paulo, onde abordou a recuperação de indícios e vestígios eletrônicos em um contexto de crime digital.

18 [19] Segundo Solha (1999), *logs* são "registros de atividade do sistema".

da origem do e-mail, Montanaro Barrales classifica a investigação em linear e não linear.

A investigação linear se dá por meio de informações obtidas junto ao provedor, no que tange ao cadastro do cliente que utilizou determinado IP.

Processo mais complexo, porém, muito mais eficiente, se dá por meio da investigação não linear. Por meio de uma engenharia regressiva, busca-se a localização de onde o IP originário está instalado, sem que haja invasão da privacidade ou violação a direito e garantia fundamental. A engenharia regressiva ou engenharia social é realizada por meio de mecanismos disponíveis na própria rede mundial de computadores.

CONCLUSÃO

Assim, pode-se concluir que o papel da vítima na preservação dos vestígios eletrônicos deixados pela perpetração de delitos informáticos é de suma importância, pois, dependendo da atitude que tiver com relação a sua máquina, assim que descobrir a ação ilícita, orientará o caminho da investigação, podendo, inclusive, muitas vezes dificultar a coleta de provas.

Ressalta-se, aqui, o papel importante da Ciência da Computação no processo de segurança eletrônica, na medida em que são desenvolvidas técnicas e softwares para evitar invasão em sistemas de computadores, bem como, caso isso venha a ocorrer, possibilitar, de forma rápida e eficaz, que os indícios e vestígios possam ser recuperados, ainda quando inadvertidamente "deletados" pela vítima ou quando propositadamente apagados pelo investigado, possibilitando o rastreamento para se chegar ao autor do crime.

Do que se analisou no presente artigo, constata-se que a investigação criminal nos crimes digitais requer profissionais especializados e em constante interface com os avanços tecnológicos, sem, jamais, esquecer-se de que nesse mitié deverá haver, sempre, a interação entre profissionais do Direito, da Ciência da Computação e outras ciências afins.

REFERÊNCIAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Disponível em: <http://www.senado.gov.br>. Acesso em 8 abr. 2003.

_____. **Decreto n.º 97057 de 10 nov. de 1988**. Altera os títulos i, ii e iii do regulamento geral para execução da lei 4.117, de 27 de agosto de 1962. Disponível em: <http://senado.gov.br>. Acesso em 8 abr. 2003.

_____. **Lei nº 8078 de 11 de set. de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://senado.gov.br>. Acesso em 8 abr. 2003.

_____. **Lei nº 9296 de 24 de jul. de 1996**. Regulamenta o inciso XII, parte final, do artigo 5º da Constituição Federal. Disponível em: <http://senado.gov.br>. Acesso em 8 abr. 2003.

_____. **Lei n.º 9472 de 16 de jul. de 1997**. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da emenda constitucional 8, de 1995. Disponível em: <http://senado.gov.br>. Acesso

em 8 abr. 2003.

CAPEZ, Fernando. **Curso de processo penal**. 2. ed. São Paulo: Saraiva, 1998. 621p. ISBN 85-02-02406-X.

_____, Fernando. **Curso de processo penal**. 9 ed. São Paulo: Saraiva, 2003. 678p. ISBN 85-02-04287-4.

COELHO, Rodrigo Durão. **Fraude online cresce e vira epidemia mundial**. Disponível em: http://informatica.terra.com.br/interna/O,,OI434865-EI553,00.html. Acesso em: 06 dez 2004.

COMUNIDAD EUROPEA. **Directiva 95/46/CE del Parlamento Eureopeo y el Consejo de la Unión Europea**. Disponível em: <http://www.delitosinformaticos.com/protecciondatos/directiva95-46.shtml>. Acesso em: 10 dez. 2002.

_____. Directiva 2002/58/Ce Del Parlamento Europeo Y del Consejo de 12 de Julio de 2002. **Diario Oficial de las Comunidades Europeas**, Bruselas, L 201, de 31 jul. 2002, p. 37-47.

CRETELA JÚNIOR, José. **Comentários à Constituição brasileira de 1988**. Rio de Janeiro: Forense Universitária, 1988, v.1, 581 p. ISBN 85-218-0013-4.

ESPAÑA. **Ley Orgánica n.º 15 de 13 de dic. de 1999**, de Protección de Datos de CarácterPersonal. B.O.E. Nº 298. Martes 14 de diciembre de 1999. Disponível em: <www.delitosinformaticos.com>. Acessado em: 8 abri. 2003.

_____. **Ley Orgánica n.º 34 de 11 de Jul. de 2002**, de servicios de la sociedad de la información y de comercio electrónico. BOE num. 166, de 12 jul. de 2002. p. 25388-25403. Disponível em: <www.delitosinformaticos.com>. Acessado em: 8 abri. 2003. LIMA JÚNIOR, Carlos Daniel Vaz de. O sigilo do cadastro de clientes dos provedores de acesso à Internet. Disponível em: <http://www.carlosdaniel.net/>. Acesso em: 2 abr. 2003.

GOMES, Luiz Flávio. **A CPI e a quebra do sigilo telefônico**. Disponível em: <http://campus.fortunecity.com/clemson/493/jus/m05-010.htm>. Acesso em: 31 out. 2002.

GRECO FILHO, Vicente. **Interceptação telefônica**: considerações sobre a lei nº 9.269, de 24 de julho de 1996. São Paulo: Saraiva, 1996. 60 p. ISBN 85-02-02185-0.

GRINOVER, Ada Pelegrini. **Novas tendências no Direito Processual**. Rio de Janeiro: Forense Universitária, 1990. 435 p. ISBN 85-218-0029-0.

_____. _____. Apud GOMES, Luiz Flávio. **A CPI e a quebra do sigilo telefônico**. Disponível em: <http://campus.fortunecity.com/clemson/493/jus/m05-010.htm>. Acessado em: 31 out. 2002.

HOESCHL, Hugo César. Alguns aspectos constitucionais da Lei 9296/96. In: ROVER, Aires José (Org.). **Direito, sociedade e informática**: limites e perspectivas da vida digital. Florianópolis: Boiteux, 2000.

p. 105-113.

KAKU, Willian Smith. Internet e comércio eletrônico: pequena abordagem sobre a regulação da privacidade. In: ROVER, Aires José (Org.). **Direito, sociedade e informática**: limites e perspectivas da vida digital. Florianópolis: Boiteaux, 2000. p. 81-93.

RANGEL, Paulo. Breves considerações sobre a Lei 9296/96 (interceptação telefônica). **Jus Navigandi**, Teresina, v. 4, n. 41, maio 2000. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=195>. Acesso em: 27 nov. 2002.

SANTOS, José Eduardo Lourenço dos; FURLANETO NETO, Mário. Golpe Digital. **Diário,** Marília, p. 2-A, 2004.

SILVA, José Afonso. **Curso de Direito Constitucional positivo**. 6. ed. São Paulo: RT, 1990. 756 p. ISBN 85-203-0795-7.

SOLHA, Liliana Esther Velásquez Alegre. Os logs como ferramenta de detecção de intrusão. **RNP**, Rio de Janeiro, v. 3, n. 3, maio 1999. Disponível em <http://www.rnp.br/newsgen/9905/logs.html>. Acesso em: 13 dez. 2004. ISBN 1518-5974.

TOURINHO FILHO, Fernando da Costa. **Processo Penal.** 25 ed. São Paulo: Saraiva, 2003. v. 3, 640p. ISBN 85-02-04412-5.

TUCCI, Rogério Lauria. **Direitos e garantias individuais no processo penal brasileiro**. São Paulo: Saraiva, 1993. 501p.