DELITOS FISCAIS: VALIDADE DA PROVA OBTIDA EM MEIO ELETRÔNICO

Márcia Aguiar Arend
Max Zuffo

Promotores de Justiça - SC

Sumário: Introdução; 1. A prova nos delitos fiscais; 2. O Acesso da fiscalização aos dados eletrônicos; 3. Desmistificando a técnica; 4. Conclusão; 5.Bibliografia.

INTRODUÇÃO

Assistimos, neste limiar do terceiro milênio, ainda maravilhados, à revolução tecnológica que vem modificando e melhorando, em certa medida, nossas vidas. Internet, telefonia móvel celular, WAP, mensagens SMS, transmissão de dados via satélite, computadores com velocidade de processamento e capacidade de armazenamento nunca então imaginados, homebanking, B2B, handheld computers, e-mails, videoconferência e outras novas tecnologias estão diminuindo as fronteiras do nosso mundo, revolucionando as comunicações, implicando mudanças efetivas nos modelos de organização das corporações e do trabalho, alterando, sobremaneira o nosso cotidiano e as nossas vidas.

No entanto, é fato público e notório que o desenvolvimento das mesmas tecnologias, que tanto facilitaram tornando mais agradável e confortável

viver, também serviram como instrumento adequado para uma verdadeira revolução tecnológica no mundo do crime, que hoje conta com sofisticação e recursos técnicos suficientes, tanto para agir simultaneamente em diversos locais da chamada "aldeia global", lavando dinheiro através de operações bancárias realizadas pela Internet em paraísos fiscais, quanto para organizar rebeliões em presídios por intermédio do uso de aparelhos celulares[1], como as ocorridas no sistema presidiário do Estado de São Paulo, empreendidas pela organização criminal PCC – Primeiro Comando da Capital.

As alterações provocadas por esta revolução tecnológica no mundo do crime produzirão reflexos imediatos no Direito Penal e Processual Penal, que estarão obrigados a lidar com novos fatos delitivos cuja criminalização será demandada pela sociedade. Ainda que subsistam os elementos anímicos, os agentes têm a faculdade de utilizar novos instrumentos de comunicação capazes de lesar direitos e produzir danos. Há, novas maneiras de praticar ilicitudes, e o nosso sistema ostenta descrições típicas incompatíveis com as novas tecnologias de comunicação, as quais têm importantes repercussões no campo probatório, para as quais também não dispomos de legislação adequada. Apenas para sugerir a reflexão, exemplificamos os crimes contra a honra praticados por e-mail, a sonegação fiscal praticada por falso em meio eletrônico, os seqüestros planejados e organizados com o auxílio de telefones celulares móveis, etc., além dos delitos já praticados em ambientes virtuais, como no caso da prática de furto do dinheiro depositado em conta corrente por um hacker que obteve, indevidamente, a senha do homebanking da vítima.

Diversos são os desafios a serem enfrentados pelos operadores jurídicos que se defrontam com estas novas espécies de lesividade em um ordenamento jurídico que, como o nosso, não se presta para intimidar, reprimindo apenas os agentes da chamada criminalidade "convencional".

A adoção das novas tecnologias de comunicação como instrumentos para produzir lesão reclama aprofundamento reflexivo no que respeita à validade das provas obtidas em meios eletrônicos de armazenamento de dados, inclusive quando estes são apreendidos judicialmente no curso de investigações de práticas criminosas.

Argumentam os que se insurgem contra a produção desta modalidade de prova, que os meios eletrônicos de armazenamento de dados encontram-

[1] Como se verificou no dia 21 de Fevereiro de 2001, quando o PCC promoveu 29 rebeliões simultâneas em presídios paulista. Informações disponíveis em: <http://www2.correioweb.com.br/cw/2001-02-21/mat_28165.htm>. Acesso em: 26 set. 2001.

se sob o manto de proteção do art. 5º, X e XII da Constituição Federal, os quais garantem, respectivamente, a inviolabilidade da intimidade e da vida privada e a inviolabilidade e o sigilo da correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas, sendo ilegal, neste entendimento, a realização de perícia para avaliar o conteúdo dos computadores e demais meios de armazenamento eletrônico e magnético de dados.

Os que se valem deste argumento, sustentam seu raciocínio no acórdão lavrado pelo Supremo Tribunal Federal na polêmica Ação Penal n.º 307-3 do Distrito Federal, cujos reús eram o ex-presidente da República Fernando Collor de Mello e seu amigo (assassinado) PC Farias, dentre outros co-réus. Foi considerada ilícita a prova produzida a partir do laudo de degravação do conteúdo de um computador apreendido pela Polícia Federal, sem as devidas formalidades legais.

Essa discussão assume especial relevância no Direito Penal Tributário, onde a influência das novas tecnologias começa a ser sentida na prática dos delitos de sonegação fiscal, especialmente porque é significativo o número de contribuintes que, em virtude das facilidades provindas do uso de computadores, opta por manter a sua escrita fiscal em meio eletrônico ou magnético de armazenamento de dados, os quais passam a assumir papel relevante na produção de provas da prática destes delitos.

1. A PROVA NOS DELITOS FISCAIS

Na investigação da prática de qualquer atividade delitiva é lícito que as autoridades policiais e o Ministério Público requeiram, com base no art. 240, CPP[2], que o Poder Judiciário os autorize a promover a busca

[2]CPP - Código de Processo Penal.
Art. 240. A busca será domiciliar ou pessoal.
§ 1º. Proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem, para:
a) prender criminosos;
b) apreender coisas achadas ou obtidas por meios criminosos;
c) apreender instrumentos de falsificação ou de contrafação e objetos falsificados ou contrafeitos;
d) apreender armas e munições, instrumentos utilizados na prática de crime ou destinados a fim delituoso;
e) descobrir objetos necessários à prova de infração ou à defesa do réu;
f) apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato;
g) apreender pessoas vítimas de crimes;
h) colher qualquer elemento de convicção.

e apreensão de todos os elementos necessários à prova da ação delitiva, bem como de qualquer elemento de convicção que possa contribuir para a formação da *opinio delicti*.

Na apuração da prática de delitos fiscais, especialmente aqueles nos quais os agentes ativos valem-se das facilidades oriundas das novas tecnologias para a perpetração da sonegação, é comum que o requerimento de busca e apreensão vise apreender, inclusive, todos os dispositivos de armazenamento eletrônico ou magnético de dados, tais como, CPU, disquetes, fitas magnéticas, CD-ROMs e discos ópticos, onde possam estar demonstradas a prática dos delitos, ou mesmo qualquer registro que sirva como elemento para a comprovação da prática do crime investigado.

A necessidade da realização de perícia nos equipamentos de armazenamento eletrônico e magnético de dados passa a ser, então, procedimento essencial para assegurar a apuração do cometimento de delitos contra a ordem tributária. Ora, se tais crimes foram cometidos por esses meios, então as provas podem estar arquivadas em equipamentos que devem ser apreendidos, fato que torna imperiosa a realização da perícia criminal, para determinar se dentre os dados armazenados nos equipamentos, residem as provas destes crimes.

São impertinentes os argumentos de que os dados contidos em computadores e outros meios de armazenamento eletrônico ou magnético de dados estão garantidos pelo sigilo por conterem informações relativas à intimidade comercial e pessoal de empresas, sob o amparo do art. 5º, XII da Constituição Federal, consoante o entendimento contido no citado acórdão do Supremo Tribunal Federal.

É fundamental ressaltar que o conteúdo do inciso XII do art. 5º da CF/88 estabelece o sigilo das correspondências, das comunicações telegráficas, das comunicações de dados e das comunicações telefônicas, não estabelecendo, entretanto, o sigilo dos dados em si.

Neste passo, importante gizar que o vocábulo comunicação, de acordo com o Dicionário Aurélio Eletrônico Séc. XXI, versão 3.0, constitui o ato ou efeito de emitir, transmitir e receber mensagens por meio de métodos e/ou processos convencionados, quer através da linguagem falada ou escrita, quer de outros sinais, signos ou símbolos, quer de aparelhamento técnico especializado, sonoro e/ou visual. Isso significa dizer que, a prin-

cípio, de acordo com o art. 5°, XII, CF/88 não seria possível a violação do fluxo de comunicação de dados.

No entanto, não obstante o sigilo das comunicações ser constitucionalmente garantido, é possível que os dados comunicados sejam, posteriormente, objeto de prova, sem que tal circunstância implique afetamento ao direito à intimidade, pois caso contrário qualquer registro de dados, seja em meio magnético ou eletrônico, ou mesmo qualquer rabisco em um pedaço de papel, não poderia ser admitido como prova em qualquer processo, fosse ele de natureza civil ou mesmo criminal, pois estaria violando o direito à intimidade e o sigilo da comunicação de dados.

Essa interpretação esdrúxula dos dispositivos constitucionais que tutelam a intimidade e o sigilo da comunicação de dados não é adequada e tampouco decorre do nosso ordenamento jurídico, tanto que o Código de Processo Penal (arts. 231 e seguintes), quanto o Código de Processo Civil (arts. 364 e seguintes), possuem regramentos tidos como válidos perante nossa Constituição para a produção de provas documentais, dentre as quais, necessariamente, encontram-se as provas documentais registradas em meio magnético.Nos códigos de Processo Penal e Civil, o documento é conceituado como sendo " a coisa que representa um fato, destinada a fixá-lo de modo permanente e idôneo, reproduzindo-o em juízo" [3] ou ainda "na definição de Carnelutti, documento é 'uma coisa capaz de representar um fato'... ...em sentido lato, documento compreende não apenas os escritos, mas toda e qualquer coisa que transmita diretamente um registro físico a respeito de algum fato, como os desenhos, as fotografias, as gravações sonoras, filmes cinematográficos etc."[4]

Ao versarem sobre as provas documentais estes diplomas dão valor probatório aos instrumentos ou papéis públicos ou particulares (art. 232, CPP), tanto que o art. 376 do CPC estabelece que as cartas, bem como os registros domésticos, provam contra quem os escreveu quando enunciam o recebimento de um crédito; contêm anotação, que visa suprir a falta de título em favor de quem é apontado como credor ou expressam conhecimento de fatos para os quais não se exija determinada prova.

Com base nestes preceitos, as mais diversas provas foram produzidas e utilizadas em processos penais sem que se levantasse a eiva de ilicitude

[3] CAPEZ, Fernando. *Curso de Processo Penal.* São Paulo: Saraiva, 2.000. 5 ed., p. 285.

[4] THEODORO JUNIOR, Humberto. *Curso de Direito Processual Civil. Vol. I.* Rio de Janeiro: Forense, 2.001, p. 393.

das mesmas por violação ao sigilo das comunicações de dados. Apenas para enriquecer a reflexão poder-se-ia questionar: qual o julgador que invalidaria uma sentença condenatória pela prática de tráfico ilícito de entorpecentes sob o argumento de que a prova do comércio destas substâncias, consistente em uma agenda contendo o nome dos fornecedores e adquirentes da droga, seria uma prova ilícita por violar o direito à intimidade e o sigilo da comunicação de dados do traficante? A resposta é óbvia: ninguém invalidaria esta sentença, por se tratar de uma prova absolutamente válida. A agenda apreendida constitui acervo de informações (dados) registradas até o momento da apreensão, e integra o conjunto de objetos utilizados pelo traficante para o empreendimento criminoso.

Ocorre que os dispositivos legais que regram a produção da prova documental foram criados em momentos nos quais o papel era, por excelência, o meio utilizado para registro dos fatos e conseqüente constituição dos documentos. No tempo presente, o papel já pode ser dispensado, seja para o registro dos dados, seja para a comunicação entre as pessoas, seja para fixar a prova das relações comerciais, institucionais e até afetivas.

Estamos num tempo – já nem tão novo assim –, onde é crescente o número de situações em que fatos da vida são registrados em meio eletrônico ou magnético. Isso ocorre nas mais corriqueiras situações do cotidiano das pessoas, como por exemplo na agenda telefônica de um aparelho celular, no cadastro de endereços de um programa de e-mails, nos arquivos pessoais armazenados em um computador, em uma agenda eletrônica que registra os compromissos pessoais diários, nos arquivos de uma instituição financeira que armazenam os dados relativos ao seu patrimônio monetário. Enfim, as possibilidades são infinitas, instaurando imediatas conseqüências no mundo jurídico, especialmente no universo processual.

Os acervos eletrônicos de dados estão para o nosso tempo como sempre estiveram os acervos manuscritos de dados em livros, cadernos, cartas, diários, ou bilhetinhos. Nestes, nunca se admitiu a inviolabilidade seja da intimidade ou da privacidade como garantia do acobertamento ou da impunidade de crimes. Os documentos quando repositórios de provas sobre a prática de crimes, desde que legalmente apreendidos e devidamente submetidos à perícia, constituíram, nas sociedades "pré-internetianas", núcleos seguros para respaldar o julgador.

É evidente que a produção da prova documental assentada sobre o papel, difere da que se encontra em meios eletrônicos e magnéticos. Esta

última reclama uma decodificação da linguagem binária, a linguagem do computador, para que se torne compreensível ao intelecto do julgador, não acostumado ao domínio dos códigos binários próprios da computação. É impossível perceber num disco rígido, sem que seja ligada a máquina computador, o que nela está contido e tampouco a olho nu perceber a presença física dos códigos binários (0101100001.....e assim sucessivamente).

Assim, enquanto nos documentos tradicionais que se utilizam do papel como registro fixo de um fato ou ato, é possível compreender, pela simples leitura gráfica, representante da linguagem verbal, a natureza do documento, a intenção dos seres emitentes da vontade e o alcance do ato consignado no papel, nos documentos eletrônicos ou em meio magnéticos, é necessária a conversão da linguagem binária para a nossa linguagem corrente.

Da mesma forma como ocorre na análise de uma prova documental consistente em uma fotografia, um filme ou uma gravação sonora, onde não podemos colher o conteúdo da prova sem o auxílio de instrumentos que revertam os dados colhidos no negativo da fotografia, no filme ou na fita com a gravação para padrões de imagem e som reconhecíveis por nossos sentidos, assim como não podemos compreender o conteúdo dos dados colhidos em um HD, um disquete ou um CD apenas mediante sua contemplação.

Isso significa que as provas colhidas em computadores, CDs, disquetes, ou quaisquer outros meios magnéticos ou eletrônicos de armazenamento de dados são provas documentais, submetidas ao regime constitucionalmente válido de produção desta espécie de prova, necessitando apenas de um processo mais complexo para a conversão destes dados armazenados para padrões compreensíveis e aptos a subsidiar o julgador da prova.

Portanto, assim como não há violação das cláusulas constitucionais que tutelam a intimidade e o sigilo das comunicações quando da apreensão de documentos nas empresas, não haverá violação na colheita de dados contidos nos objetos apreendidos, por se tratarem de provas de natureza documental.

Em se tratando de documentação fiscal a questão toma outro norte, especialmente em razão da legislação que foi produzida para a ade-

quação da vida comercial atual às novidades da veloz e eficiente informatização de dados e da economia.

Atento aos novos agires do mundo negocial e às novas operações comerciais que foram sendo realizadas, a Administração Tributária entendeu que não poderia continuar ignorando a informática. Muito ao contrário. Tem nela uma grande aliada, apta a garantir maior agilidade na detecção das operações sobre as quais há incidência de impostos, assim como auxiliar nas ações próprias do poder de polícia tributário, exercido pelos corpos fiscais das entidades tributantes.

O simples fato de uma pessoa jurídica adotar a escrita fiscal por meio magnético não lhe reserva direitos de inviolabilidade dos dados que têm armazenado nos seus computadores. Os acervos de dados em computador ou outros meios magnéticos das empresas que realizam fatos geradores do Imposto sobre Circulação de Mercadorias, continuam sujeitos à fiscalização fazendária, e sobre eles é que os agentes dos fiscos promovem as verificações fiscais para legitimação dos lançamentos fiscais.

A pretensão de quem busca acobertar-se nas garantias da intimidade e da privacidade documental e de dados é de todo injustificável posto que os computadores e meios magnéticos que venham a ser apreendidos no curso de qualquer investigação da prática de crimes contra a ordem tributária, ostentam potencial e inequívoca condição de provar não só as defraudações, mas a dimensão temporal da atividade sonegadora.

Estaríamos admitindo o maior dos absurdos se a utilização de meios eletrônicos servisse, como pretendem alguns, para acobertar qualquer crime, ou frustrar a prova da sua prática ou a identificação dos seus autores. Seria erigir a informática ao grau de ciência geradora da impunidade, o computador como o instrumento a serviço dos criminosos e o Judiciário, o Ministério Público e a Polícia como organismos do silêncio e da insanidade, num mundo onde o crime não teria nenhuma autoridade a enfrentar e reagir.

3. DESMISTIFICANDO A TÉCNICA

As provas documentais produzidas com base em dados armazenados em meios magnéticos e eletrônicos é algo recente nos processos judiciais, e ainda cercada por certas místicas que tendem a macular a sua

eficácia.A estratégia mais comum de defesa de réus em processos criminais, ao se verem confrontados com provas documentais desta natureza, é alegar que os dados contidos no computador foram maliciosamente enxertados ou alterados pela acusação com o intuito de incriminá-los, buscando com isso criar a dúvida sobre a legitimidade da prova, esperando, assim, obter a absolvição por insuficiência de provas. No entanto, se estas provas são cuidadosamente manuseadas por especialistas, é possível afastar, com êxito, o discurso da defesa.

Atualmente, os peritos criminais ao lidarem com esse tipo de prova utilizam-se de um procedimento chamado de duplicação pericial[5], onde o conteúdo dos equipamentos eletrônicos ou magnéticos que contenham as possíveis provas, como HDs, CDs ou disquetes, são integralmente duplicados em um equipamento idêntico, que é então submetido à efetiva análise, sendo o original preservado, para contraprova, caso haja necessidade.

Para dar mais credibilidade ao processo de duplicação pericial dos meios de armazenamento de dados, tem-se adotado os seguintes procedimentos: os equipamentos são lacrados quando da sua apreensão e os lacres são removidos apenas na presença dos proprietários destes bens, momento no qual são entregues à custódia dos peritos judiciais que iniciam o procedimento de duplicação.

Os peritos podem utilizar os processos de somas de verificação criptográfica no processo de duplicação pericial para atestar, posteriormente, a integralidade da prova produzida.Kevin Mandia e Chris Prosise explicam como funciona este procedimento:

> "Se um arquivo e a cópia confiável forem perfeitamente equivalentes, a integralidade do arquivo fica validada. O problema está em fazer a comparação – examinam-se os arquivos linha a linha ou comparam-se atributos, como o tamanho do arquivo? E se o arquivo em questão for um binário compilado? Como fica a integridade dele?
>
> A solução é usar somas de verificação criptográficas. Uma soma de verificação criptográfica, também conhecida como resumo de mensagens ou como impressão digital, é basicamente uma

[5]Maiores informações sobre estes e outros procedimentos de investigação de crimes desta natureza podem ser obtidas na obra: MANDIA, Kevin. *Hackers: resposta e contra ataque: investigando crimes por computador.* Rio de Janeiro: Campus, 2001.

> assinatura digital. É criada aplicando-se um algorítimo ao arquivo. Cada arquivo tem uma soma de verificação exclusiva. Portanto, trata-se de um atributo perfeito para verificar a integridade dos arquivos.
>
> [...] Hoje em dia, a soma de verificação mais comum e mais aceita é o algoritimo MD5, criado por Ron Rivest, do MIT, e publicada em abril de 1.992 como o RFC 1321. O algoritimo MD5 cria uma soma de verificação de 128 bits de qualquer arquivo grande.
>
> [...] Para criar uma soma de verificação MD5 de um arquivo binário, deve-se usar o sinalizador –b (desnecessário nos sistemas UNIX):
>
> C:\ > md5sum –b test.doc
>
> 95640dd2eabc0e51e2c750ae8c0cd4b5 *test.doc
>
> O asterisco (*) antes do nome indica que a entrada é um arquivo binário. O nosso arquivo test.doc contém o texto "Isto é um documento de teste". Se editarmos o arquivo, mudando o texto para "Isto é um documento de teste2", teremos a seguinte soma de verificação:
>
> C:\ > md5sum –b test2.doc
>
> Cc67710c67ef69ed02c461c9a9fbe47e *test2.doc
>
> Observe-se que a soma de verificação mudou, assim como o conteúdo do arquivo. (A mudança do nome do arquivo não afeta a soma de verificação.)"[6]

Utilizando-se de tal procedimento é possível, no momento em que é realizada a duplicação pericial, extrair uma soma de verificação criptográfica do material a ser duplicado, e, posteriormente, caso venha a ser discutida a integralidade do laudo produzido com base no material duplicado, demonstrar que a soma de verificação criptográfica obtida no material apreendido e a obtida no material duplicado são idênticas, demonstrando assim que não houve qualquer alteração no conteúdo das provas.

Com isso é garantida a integralidade da prova, evitando que a mesma seja maculada desde o momento do início da perícia até a discussão da mesma no processo. A presença dos titulares dos bens, na oportunida-

---

[6] MANDIA, Kevin. *Hackers: resposta e contra ataque: investigando crimes por computador.* Rio de Janeiro: Campus, 2001, p. 39-40.

de de deslacramento, assegura a não violação do equipamento apreendido e que não houve qualquer manuseio indevido desses equipamentos até o momento da entrega dos mesmos aos peritos, enquanto a utilização de procedimentos como a soma de verificação criptográfica, atestam que não houve qualquer alteração posterior no material periciado.

4. CONCLUSÃO

Conclui-se, portanto que:

– as novas tecnologias de comunicação podem constituir instrumentos para produção de danos, sendo necessária a reprogramação das normas processuais para disciplinar a produção das provas obtidas em meio eletrônico;

– a intensa utilização do computador na escrita fiscal das empresas e pelas pessoas para armazenamento de dados com os quais possa ser obtida a prova de crime contra a ordem tributária, reclama cuidado específico na execução dos mandados de busca e apreensão de computadores, além das perícias de duplicação pericial para preservação do corpo de delito dos documentos em meio eletrônico aprendidos;

– há diferença entre comunicação de dados e armazenagem de dados em meio eletrônico, sendo que a obtenção das informações armazenadas em computador não implica violação do direito constitucional da intimidade, consagrado no art. 5°, inciso XII da Constituição Federal.

5. BIBLIOGRAFIA

AN, Robert C. *Intelligence Led Policing and the Key Role of Criminal Intelligence Analysis: Preparing for the 21st Century*. Disponível em: < HREF="http://www.interpol.com/Public/cia/fahlman.asp" MACROBUTTON HtmlResAnchor http://www.interpol.com/Public/cia/fahlman.asp>

CANOTILHO, J. J. Gomes. *Direito Constitucional*. Coimbra: Livraria Almedina, [s.d]. 4. ed. p. 1234-1240

CAPEZ, Fernando. *Curso de Processo Penal*. São Paulo: Saraiva, 2.000. 5 ed., p. 285.

CPP - Código de Processo Penal.

MANDIA, Kevin. *Hackers: resposta e contra ataque: investigando crimes por computador.* Rio de Janeiro: Campus, 2001, p. 39-40.

MORAES, Alexandre de. *Direito Constitucional.* São Paulo: Atlas, 2000. 8. ed. p. 78.

Statement for the Record of Steven C. McCraw, Deputy Assistant Director Investigative Services Division Federal Bureau of Investigation on Organized Crime, Drug Trafficking, and Terrorist Acts Before the House Judiciary Committee, Subcommittee on Crime Washington, D.C. Disponível em : <hHREF="http://www.fbi.gov/congress/congress00/mccraw.htm" MACROBUTTON HtmlResAnchor http://www.fbi.gov/congress/congress00/mccraw.htm>

THEODORO JUNIOR, Humberto. *Curso de Direito Processual Civil. Vol. I.* Rio de Janeiro: Forense, 2.001, p. 393.