Provas e contra-provas periciais nos casos de crime eletrônico: a capacidade da lei processual penal face ao princípio da ampla defesa.

Ariel G. Foina, *Doutorando, Universidad de Salamanca*

***Resumo*—O presente artigo, ao abordar a natureza da prova pericial e sua prática tanto na fase do inquérito quanto no decorrer da instrução criminal, suscita eventuais fragilidades de natureza processual, no caso de crimes eletrônicos puros. Aborda-se a constitucionalidade do uso da Lei 9296 na investigação e instrução de crimes eletrônicos bem como do rito da perícia no Código de Processo Penal quanto ao respeito ao princípio da ampla defesa. Após, conclui pela possibilidade de aplicação subsidiária do Código de Processo Civil ou da criação de juízos especializados em crimes eletrônicos e tecnológicos apontando eventuais problemas de ambas as soluções.**

***Palavras-Chave*—Direito Eletrônico, Crime Eletrônico, Processo Penal, Perícia, Provas Eletrônicas, Contra Prova Pericial**

I. Introdução

O presente artigo vem tratar do que Daoun[1] conceitua como crime de informática puro e que aqui tratamos como crime eletrônico puro, no caso, aqueles em que os bens jurídicos eletrônicos são meio e fim da conduta delitiva.

As ideias aqui propostas são decorrentes da experiência profissional do autor no campo da Advocacia em crimes eletrônicos, bem como, de dados obtidos em pesquisa de campo realizada no decorrer da elaboração de tese doutoral que trata da sub-cultura hacker e outras sub-culturas desviantes localizadas no ciberespaço brasileiro.

II. Da Perícia no Crime Eletrônico na Fase Inquisitorial

O inquérito policial é a fase do procedimento penal no direito brasileiro que precede o processo judicial. No inquérito, ao contrário do processo, o que se pressupõe como princípio orientador dos atos é o princípio do "*in dubio pro societate*", ou seja, na duvida se preza a defesa da coletividade em detrimento do réu.

Assim, nesta fase, nada mais natural do que termos o corpo administrativo do estado responsável pela condução do inquérito, seja a policia civil, federal, orientando seu trabalho para a busca de indícios e argumentos probatórios que busquem a condenação do réu. Esta orientação, de buscar a condenação do réu, é, por princípio jurídico, inversa à do processo penal, onde se busca a absolvição e em que a condenação pressupõe cumprimento de todos os elementos imprescindíveis para tal, via de regra, tipicidade, culpabilidade, nexo causal entre a conduta típica e a conduta do réu e culpabilidade.

Assim, falando-se especificamente da perícia, a linha investigativa da mesma dependerá da quesitação feita pela autoridade condutora do inquérito policial. A forma como se elaboram os quesitos determina a linha investigativa que o perito terá de adotar no decorrer do trabalho pericial.

Não é função do perito conduzir as investigações policiais. Na estrutura administrativa policial brasileira, não temos essa figura técnico-investigadora do "investigador de cena de crime" ou do "detetive cientifico"[2]. No Brasil, o que ocorre é que, as figuras responsáveis pela condução do inquérito (e também do processo, tema que será abordado mais adiante) não são portadoras de conhecimento técnico especializado. Desta forma, na prática, temos agentes policiais, e no caso de inquéritos de maior porte, os próprios delegados de polícia, responsáveis por elaborar quesitos e tomar decisões sobre a condução das referidas investigações, agentes e delegados estes os quais, diferentemente dos peritos, possuem uma formação deliberadamente focada nos aspectos jurídicos do inquérito e não nos aspectos da materialidade técnica do delito eletrônico.

É importante destacar o fato de que, dos crimes previstos no ordenamento jurídico brasileiro, dentre os que dependem de perícia para a efetiva constatação da materialidade, os crimes eletrônicos puros são, sem sombra de dúvida, os crimes onde a efetiva materialização do delito é de mais difícil constatação. Isso se dá devido a uma cultura instaurada dentre diferentes subculturas desviantes da Internet de sempre se tentar apagar os elementos probatórios que possam apontar a autoria (no caso de dano) ou a materialidade (no caso de acesso não autorizado ou de interceptação de comunicação informática) do delito perpetrado.

III. Do Procedimento Pericial no Processo Penal

Assim, vindo do procedimento inquisitorial, realizada sem acompanhamento da defesa do réu, a perícia é recebida no processo penal como mais um dos elementos que podem compor o livre convencimento do magistrado. Na legislação

Manuscrito recebido em 24 de setembro de 2006.

A. G. Foina é Doutorando pela Universidade de Salamanca no programa de Processos de Mudança na Sociedade Contemporânea, Sociólogo pesquisador da Cultura Hacker e Advogado com atuação na área do Direito Eletrônico. (arielfoina@gmail.com ou gomide@usal.es).

pátria só se admitem as provas produzidas no decorrer do processo judicial, de forma que, atos já praticados no inquérito, nos processos administrativos-disciplinares ou nas comissões de sindicância, dependem de ratificação ou de nova produção para que passem a compor o processo penal. Isso ocorre, especialmente com o interrogatório do réu e com o depoimento das testemunhas já ouvidas no inquérito.

Com os laudos periciais, é raro, na pratica jurisdicional, a determinação de que seja refeita a perícia anteriormente já produzida, o que se tem é a intimação dos peritos responsáveis pelo laudo para que os mesmos, na condição de testemunhas, reiterem o já contido no laudo produzido no âmbito do inquérito policial. Nestes casos, o que é possível de se fazer, tanto da parte da defesa do acusado, quanto do *parquet* ministerial, é a apresentação de quesitos novos aos peritos para que os mesmos se manifestem.

Ocorre porém que, uma vez que tanto as delegacias de polícia, sejam elas federais, civis ou administrativas, quanto os juízos penais e criminais, tem sua competência determinada, via de regra, pelo local da ocorrência do delito e a natureza jurídica da vítima. Dessa forma, é natural que, no decorrer do processo penal, a resposta a novos quesitos, e, inclusive, a realização de nova perícia, se for o caso, seja feita exatamente pelo mesmo órgão responsável pela elaboração da perícia no bojo do inquérito policial. Mais do que isso, dependendo da jurisdição, pela carência de peritos especializados em crimes eletrônicos, existe grande possibilidade de que a perícia venha a ser realizada pelo mesmo perito, funcionário do órgão técnico de determinada jurisdição.

IV.Da Perícia no Crime Eletrônico no Processo e dos Juízos Especializados

Assim, é nesse contexto que se deve inserir o debate referente a possibilidade e natureza da perícia dos crimes eletrônicos puros face ao nosso atual ordenamento jurídico.

Nosso foco de preocupação, no presente trabalho, são os crimes eletrônicos puros, assim, é de fundamental relevância o dado empírico já apresentado anteriormente de que a materialidade de tais delitos é de difícil constatação, em especial por determinados traços culturais intrínsecos aos grupos sociais de onde originam boa parte dos autores de tais delitos. Neste contexto, onde o autor do delito é portador de conhecimento técnico tal que é capaz de apagar rastros de acessos não autorizados e registros de entrada e saída de sistemas de forma a dificultar e até a inviabilizar a determinação da materialidade ou o estabelecimento de nexo causal, um dos recursos jurídicos mais importantes para o combate e investigação de tais delitos encontra-se nos mecanismos estabelecidos na Lei 9296 de 1996, que estabelece os procedimentos para a quebra de sigilo telefônico, telemático e informático.

Tal lei porém é um paradoxo jurídico que, por si só, enfraquece a investigação e a instrução processual para estes tipos de crimes. Sua ementa assim diz: "*Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal*", o referido inciso por sua vez afirma:

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

Assim, fica claro que a Carta Magna apenas permite, e a Lei 9296 apenas se propõe, à quebra de sigilo telefônico, descartando-se assim a correspondência, as comunicações telegráficas e de dados.

Porém, por paradoxal que é, a Lei 9296, no parágrafo único de seu artigo 1o traz:

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

Dessa forma, a Lei aqui tratada, quando utilizada para fins de investigação e instrução criminal, nos casos de crimes eletrônicos puros, abre ampla margem a questionamentos referentes a constitucionalidade, e por conseqüência, à validade das provas produzidas sob a égide do referido dispositivo legal, fragilizando assim a investigação e, por conseguinte, a obtenção da verdade real, princípio jurídico fundamental aos processos de natureza penal.

V.Da Contra Prova Pericial e da Ampla Defesa

Outro problema que merece destaque no que tange as perícias de crimes eletrônicos puros, visto o papel fundamental que tem para identificação de nexo de causalidade e de materialidade, nos referidos delitos, é a possibilidade de se ter respeitado o princípio constitucional e humano, do direito à ampla defesa, por parte do acusado.

No ordenamento jurídico brasileiro, quanto ao Código de Processo Penal, o perito, e por conseguinte, a perícia, respondem diretamente ao juízo, bem como, por decorrente dedução, a ambas as partes, tanto defesa quanto acusação, é o que decorre da análise do artigo 159 da referida carta legal, quando afirma:

"*Art. 159. Os exames de corpo de delito e as outras perícias serão feitos por dois peritos oficiais*".

Porém, a jurisprudência entende que, face ao princípio do livre convencimento do juiz, não basta apenas a constatação, por parte do perito do juízo, de uma eventual autoria ou materialidade em determinado delito, há ainda a necessidade de o perito apresentar os elemento que fundamentam seu parecer, os quais, no caso de crimes eletrônicos puros, são, em sua grande maioria, decorrentes de uma análise sistêmica de difícil explicação para pessoas não técnicas, ou, decorrente de dados de programas cuja juntada, em forma documental, fica prejudicada. Para exemplificar tal situação, temos, a

hipótese de uso de detectores de intruso (IDS) e de seus relatórios para fundamentar um nexo de autoria, ou, o uso de analisadores de pacotes para identificar a violação ou o dano a determinado sistema de redes. Em ambos os casos, os registros decorrentes do uso de tais ferramentas, mesmo que claros a um perito de formação técnica, são praticamente ilegíveis a pessoas sem a devida formação, em especial, a média dos delegados e juízes que atualmente atuam no sistema penal brasileiro.

Desta forma, sendo o perito, no caso específico do processo penal brasileiro, figura vinculada direto e exclusivamente ao juiz, não é possível, face nosso atual ordenamento jurídico, a execução de perícia por parte da defesa, ou, se quer, a indicação de assistente técnico da defesa para acompanhar os trabalhos realizados pelo perito oficial, o que torna difícil, o devido exercício do princípio da ampla defesa, uma vez que o próprio advogado de defesa, via de regra, não tem conhecimento técnico o suficiente para, se quer, questionar os fundamentos da decisão do perito na resposta dos quesitos apresentados.

Nota-se que, ao tratar a perícia, o Código de Processo Civil a situa no Capítulo II do Título VII do seu primeiro livros, capitulo esse intitulado como "*Do exame de corpo de delito e das perícias em geral*". É de suma importância frisar que as preocupações aqui apresentadas são decorrentes da complexidade dos elementos formadores do convencimento do perito quanto as fatos juridicamente relevantes nos casos de crimes eletrônicos puros, pois, em tais, não se pode transferir ao perito, responsabilidade que é, por direito e dever, de competência personalíssima do Juiz de decidir a lide.

VI. Possíveis Soluções à Questão

Não obstante a tal, não há, apesar de desejada, a necessidade de um diploma legal específico para tratar do processo no caso de crimes eletrônicos puros e outros delitos tecnológicos, sendo passíveis, sob a égide do nosso atual ordenamento jurídico, duas soluções que passaremos a apresentar.

Primeiramente, reconhecida pelo juízo a complexidade da matéria e a lacuna da lei penal, poder-se-ia aplicar, subsidiariamente, o Código de Processo Civil, assim como se faz em complementação ao processo trabalhista nos casos de perícia.

A aplicação subsidiária do CPC abriria a possibilidade de indicação de assistente técnico, por parte da defesa, para acompanhar os trabalhos periciais, ou, em se tratando de re-perícia ou perícia de contra prova, por exemplo, da pactuação entre Defesa e Ministério Público de eventual instituto ou pessoa técnica de notório saber na área, distinta daquela responsável pela elaboração do primeiro laudo, para formulação de um novo, desde que aprovado pelo Juiz.

Esta solução, se por um lado torna inquestionável o respeito ao princípio da ampla defesa, por outro lado, se vista de uma perspectiva mais pragmática, gera dificuldades que podem vir a influenciar o resultado da referida perícia, dependendo do nível técnico e da natureza da investigação se levamos em conta a doutrina pericial da "cadeia de custódia"[3] que preza pelo controle da prova científica colhida em loco. No caso de outro que não um instituto de criminalística com fé pública ou mesmo, no caso de acompanhamento dos trabalhos por assistente pericial, haveria a necessidade de se trabalhar sobre cópias do material colhido, o que, em se tratando, por exemplo, de tentativa de recuperação de dados em superfície logicamente desmagnetizada tornaria o trabalho impossível ou permitiria, a depender do caso fático, uma contaminação irreversível da amostra.

A segunda solução proposta, é, por um lado, menos complexa, do ponto de vista técnico-legal, porém, de uma dificuldade política extremamente superior. Trata-se da criação de juízos especializados com Juízes de primeira e segunda instâncias com formação técnica suficiente para que os mesmos tenham capacidade de não apenas compreender os laudos periciais, quanto, de apreciar por si mesmos os arquivos e registros que venham fundamentar as respostas do perito.

Tal solução não só reduziria o prejuízo ao princípio da ampla defesa, como, retiraria da prova pericial a carga de ser elemento probatório crucial nos processos aqui em questão, uma vez que permitiria, em casos extremos, a própria inspeção judicial.

A resistência política se dá, porém, devido a necessidade de se compor todo um corpo jurídico, seja de Magistrados, seja de membros do Ministério Público, e até mesmo de Advogados, com tal tipo de formação multidisciplinar. Tal resistência, porém, não carece de outros argumentos que não o meramente político e encontra forte fundamento em dispositivos da doutrina do Direito, quando da interpretação do princípio jurídico do Juiz Natural, bem como do princípio doutrinário da avaliação das condutas sob a ótica do comportamento do "homem médio"

VII. Conclusões

Assim, até o presente momento, fica sem solução a questão aqui apresentada, o que, por hora, não é geradora de maiores preocupações uma vez que, a atual legislação penal brasileira prevê a aplicação efetiva de muitos poucos tipos penais às condutas tidas como crimes eletrônicos puros, em especial o tipo penal do Dano, e o da Interceptação de Comunicação, artigos 163 do Decreto 2848 e 10 da Lei 9296 respectivamente.

Porém, visto que encontra-se em tramitação diferentes projetos de lei com vistas a adicionar os mais diferentes tipos penais decorrentes de delitos eletrônicos puros ao nosso Código Penal, a notória ausência de uma legislação processual que acompanhe os mesmos é preocupante e põe em questão a eficácia de tais normas vindouras.

Referências

[1] DAOUM, Alexandre Jean. “Crimes Informáticos” in BLUM, Renato Opice (org), *Direito Eletrônico: A Internet e os Tribunais*, Bauru: Edipro, 2001.

[2] no uso original do termo Crime Scene Investigator e Forensic Detective

[3] no uso original do termo Chain of Custody

Ariel G. Foina é Doutorando pela Universidade de Salamanca no programa de Processos de Mudança na Sociedade Contemporânea, Sociólogo pesquisador da Cultura Hacker e Advogado com atuação na área do Direito Eletrônico. É bacharel e licenciado em Ciências Sociais pela Universidade de Brasília e detém atualmente Diploma de Estudios Avansados em Sociologia pela Universidad de Salamanca aonde desenvolve tese doutoral cujo objeto são as sub-culturas desviantes do ciberespaço, especialmente no Brasil.

No ano de 2005, foi membro de Research Cluster sobre Tecnologia e Ação Social junta à Sheffield Hallam University na Inglaterra além de participar do PhD Forum do Human-Computer Interface Issues in e-Democracy do grupo Toward Electronic Democracy da Manchester Business School.

Dr. Foina é advogado inscrito na Seccional do Distrito Federal da Ordem dos Advogados do Brasil e tem diversas publicações na área de Direito Eletrônico, Cultura Hacker, Sociologia do Desvio e do Crime, além de trabalhar com pesquisas e projetos sociais na área de extensão universitária e educação.