Capítulo XII

Aspectos processuais dos crimes praticados pela internet

Bernardo Chezzi*

Sumário • 1. Considerações iniciais – 2. Ocorrência do crime. A ata notarial – 3. O procedimento da Autoridade Policial na fase de inquérito – 4. A notificação ao provedor de conteúdo – 5. Jurisdição e competência – 5.1. A jurisdição penal brasileira – 5.2. Justiça Estadual ou Federal?– 5.3. Foro competente – 5.4. Juízo competente – 6. Conclusões necessárias – 7. Referências bibliográficas

1. CONSIDERAÇÕES INICIAIS

A Internet teve o seu formato embrionário no ano de 1969, quando, em plena Guerra Fria, os EUA desenvolviam um eficiente mecanismo de comunicação militar, imune a bombardeios e de difícil sabotagem, conhecido como ARPANET (nome oriundo de *Advanced Research Projects Agency*). Algumas décadas depois, notadamente em meados de 1980, a lógica comunicacional passou a ser adotada entre universidades americanas, com o fito de troca de conhecimento e unificação de bancos de dados.

Somente a partir dos anos 90 é que se verifica a comercialização da Rede, com a respectiva massificação do mecanismo, e a sua utilização pelos mais variados segmentos sociais, por todo o mundo. Neste novo e atual formato, a Rede Mundial ficou sem dono e controle hierárquico.

A Rede, que não é um fim em si mesmo, consubstancia-se em instrumento eficaz para a formação, informação e para o empreendimento de diversas das ações humanas – através das infindáveis formas de interação direta e indireta entre indivíduos e coletividades. Tamanho é o grau de entrelaçamento que guardam sociedade e Internet, que não se cogita mais em um bom funcionamento dos organismos sociais sem que se tenha à disposição a Rede Mundial de Computadores.

Todavia, a transposição das vicissitudes do mundo pós-moderno à Internet acarretou também o surgimento de condutas, para cujo resultado no "mundo real", o Direito define como ilícitos civis ou penais. Como não podia ser diferente, num

---

* Graduando da Faculdade de Direito da Universidade Federal da Bahia, desenvolveu pesquisa do tema através do Programa Institucional de Bolsas de Iniciação Científica (PIBIC), com a orientação da professora Maria Auxiliadora Minahim, durante o biênio 2006/2007. É presidente do Centro de Estudos e Pesquisas Jurídicas da UFBA (CEPEJ).

sentido amplo, o homem que, sem o uso de computadores, furta, frauda, difama e abusa de menores é o mesmo homem que realiza tais condutas típicas por meio digital, eletrônico. Para este rol de ações praticadas na Internet criou-se a nomenclatura de crimes virtuais.

Há que, no entanto, fazer-se de logo a correta ponderação acerca deste nome, pois, embora sejam praticados por meio de caracteres virtuais, os seus resultados são fáticos e consistem, no mais das vezes, em reais lesões ou ameaças de lesões a bens jurídicos penalmente tutelados. Por isso, estas condutas merecem igualmente a sanção do Estado-Juiz. Porém, é preciso cuidado ao examinar o tema, haja vista que há características dos crimes praticados na Internet que impõem dificuldades, com destaque à extraterritorialidade, ao aparente anonimato e à facilidade na propagação de conteúdo criminoso.

O objetivo deste estudo é dirimir algumas das questões de processo penal que aparentam ser obscuras ou de difícil solução ao jurista, quando defrontado com crimes praticados na Internet. Seguir-se-á, destarte, um roteiro lógico, que tem início na ocorrência do crime dito virtual, até a correta propositura da ação penal, debruçando-se também sobre os aspectos relativos à competência. Ressalva-se, de logo, que o foco de nossos destes estudos será a estirpe de crimes virtuais praticados por meio de um *website*[1], para a útil sistematização de suas propriedades, embora saibamos que os delitos na Rede não estão a isto subsumidos.

2. OCORRÊNCIA DO CRIME. A ATA NOTARIAL

Quando o indivíduo toma conhecimento de um crime praticado por meio da Internet de que é vítima, o primeiro desafio é assegurar-se da prova de sua ocorrência, dada a volatilidade do que disposto na Rede. Na maioria das vezes, a mesma pessoa que veicula conteúdo ilícito é capaz de retirá-lo. As provas da ocorrência do ilícito virtual são fundamentais para o correto e efetivo desenvolvimento da *persecutio criminis*.

Para isso, os operadores do direito deram nova dimensão ao instituto da ata notarial, estabelecido pelo Art. 7º, III, da Lei 8935/94. Em termos genéricos, a ata notarial é a narração de fatos verificados pessoalmente pelo tabelião e compreende: local, data e horário de sua lavratura; nome e qualificação do solicitante; narração circunstanciada dos fatos; declaração de haver sido lida ao solicitante e, sendo

1. *Websites* são os domínios virtuais disponíveis ao livre acesso pela Internet. Estas páginas costumam ser visitadas por meio de um código virtual, o *World wide web*, conhecido como www. Em verdade, este endereço virtual traduz um número IP daquele conteúdo, que se visa ao acesso. Também chamaremos o *website* de sítio, *site*, ou simplesmente página.

o caso, às testemunhas; assinatura do solicitante e das testemunhas; assinatura e sinal público do tabelião.

Com fins de assegurar ao juiz que determinado crime virtual ocorreu, ou está ocorrendo, a ata notarial passou a ser usada para que reste certificado pelo notário o conteúdo disposto em determinado endereço eletrônico da Internet, em certa data e horário. Através da ata, o tabelião acessa o sítio eletrônico solicitado e descreve o que viu, imprime imagens e documentos da página virtual, dando fé pública a cada item transcrito e transladado. A vítima pode solicitar ata notarial em qualquer Tabelionato de Notas.

Através da referida ata será possível também a identificação do servidor de conteúdo[2] por meio do qual o crime foi praticado (porque especificado o endereço eletrônico) e os dados necessários para a requisição do endereço IP (Internet Protocol)[3].

De posse da prova da ocorrência daquele ilícito, o próximo passo é retirar o fino véu de anonimato que paira sobre o crime, chegando ao real autor do ilícito virtual. Faz-se mister que a vítima, agora, requeira à Autoridade Policial competente[4] a instauração de inquérito para apuração do delito, através da conhecida *noticia criminis*.

3. O PROCEDIMENTO DA AUTORIDADE POLICIAL NA FASE DE INQUÉRITO

Todo usuário da Internet, ao conectar-se, o faz através de um servidor de acesso (ex. Velox, Uol, Terra, SpeedZone, UFBA etc). Geralmente, para cada conexão há um número IP (Internet Protocol), que é capaz de identificar tanto o provedor de acesso quanto o endereço físico do usuário que dele utilizou-se. O IP não costuma ser estático, sendo na verdade a expressão em uma seqüência de números de um protocolo de que, naquele momento, naquela conexão, se valeu o provedor de acesso para ligar o computador do usuário à Rede.

---

2. Ver-se-á mais tarde a sua devida conceituação, diferenciando servidor de conteúdo e servidor de acesso.
3. O IP é expresso através de uma seqüência de número, e.g. 200.152.00.30. Expressa o protocolo que se utilizou o servidor de acesso para conectar o usuário à Internet, na conexão daquela data e instante.
4. Aqui acompanhamos a idéia de Fernando da Costa Tourinho Filho (2006), no sentido de que a expressão autoridade competente é empregada no sentido de poder atribuído a um funcionário para tomar conhecimento de determinado assunto. Os Estados costumam regular esta matéria de acordo com a sua Lei de Organização Judiciária, e a maioria deles já criou uma delegacia especializada para tratar de crimes praticados na Internet. Nestes casos, são estas unidades as competentes para receber a *noticia criminis*. Há de se observar, ainda, que quando se tratar de crime relacionado às hipóteses elencadas no art. 109 da CF, a Autoridade Policial competente será a federal.

De outro lado, há também os servidores de conteúdo. Seus formatos podem ser dos mais diferentes, mas, em linhas gerais, os provedores de conteúdo hospedam outras páginas em seu domínio, ás vezes milhares delas, como acontece com o *geocities.com*, uol.com.br, e assim por diante. É no conteúdo hospedado pelo servidor de conteúdo que costuma ser verificado o crime virtual.

Quando alguém se conecta à Internet, através de um servidor de acesso, e de um IP específico para aquela conexão, e pratica um delito através da Rede em um sítio de um servidor de conteúdo, deixa nos registros do provedor hospedeiro o número de seu IP. É com esteio neste fato, que a Autoridade Policial deve perquirir, nesta seqüência lógica: I) Qual o provedor de conteúdo daquele crime; II) Qual o provedor de acesso; III) Qual o endereço físico do usuário[5].

Portanto, deve o investigador, primeiramente, solicitar ao juiz a quebra de sigilo de dados telemáticos, para que o magistrado determine ao provedor de conteúdo o fornecimento do número IP naquela hora e data em que foi verificado o crime. Para o caso de se tratar de provedor estrangeiro, mas com filial no Brasil, a ordem deve ser a esta endereçada. Com o número IP obtido, identifica-se o servidor de acesso, através de sítios especializados e gratuitos na própria Internet.

Será então necessária nova requisição judicial de quebra de dados telemáticos, desta vez para que obrigue o provedor de acesso a dizer quem, naquela data, hora, respectivo fuso horário, e com aquele IP, utilizou-se de seus serviços. Dependendo do caso, identificado o endereço físico onde se acometeu o injusto penal, pode-se determinar em seguida a busca e apreensão do computador e de materiais correlatos.

Por último, impende destacar que se a vítima preferir agir sozinha, sem a instauração de inquérito, pode fazê-lo. Para tanto, deve utilizar-se de ação cautelar de exibição de documentos (art. 844, II do CPC), conforme admitido hoje na jurisprudência, primeiramente para obter o número IP junto ao provedor de conteúdo, e depois para saber o endereço físico junto ao provedor de acesso. Esta metodologia tem sido também adotada na inquirição de ilícitos cíveis, para os quais não caberia, na maioria das vezes, a instauração de inquérito policial.

4. A NOTIFICAÇÃO AO PROVEDOR DE CONTEÚDO

Concomitante à lavratura da ata notarial, deve a vítima notificar o provedor de conteúdo por meio do qual foi cometido o crime, solicitando[6]: a) retirada imediata do conteúdo ilegal e/ou ofensivo do serviço onde o material está hospedado,

---

5. MINISTÉRIO PÚBLICO FEDERAL; COMITÊ GESTOR DA INTERNET. Crimes Cibernéticos. Manual prático de investigação. São Paulo, 2006.
6. SAFERNET BRASIL. Disponível em: <www.denunciar.org.br>. Acesso em: 07 de Agosto de 2007.

incluindo o(s) *link(s)* pertinentes, sob pena de ajuizamento da competente ação de responsabilidade e b) 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.

Embora discutível a responsabilidade penal do provedor de conteúdo no que se refere ao crime virtual através dele cometido, claro está que é responsável civilmente o servidor que, sabendo do teor ilícito que hospeda, não o retira do ar. Portanto, é aconselhável que se notifique o provedor por meio idôneo, como por exemplo, uma carta registrada, para fins de prova em uma posterior ação de indenização contra o servidor que foi devidamente notificado, e não agiu (*verbi gratia*, Resp 566468 – RJ / STJ).

Esta conduta é importante para a vítima porque, muitas vezes, a depender do tipo de crime cometido, dada a facilidade de propagação de informação, não é razoável que a vítima espere a Justiça retirar o *site* do ar, quando puder fazê-lo por vias diretas.

Por fim, ainda no que concerne a este tópico, é importante que o ofendido notifique o provedor hospedeiro para que este guarde as informações técnicas necessárias a fim de que seja possível a identificação do usuário infrator, na fase de inquérito ou na instrução criminal. Exceto nos casos de pornografia infantil (Lei 10.764/03), ainda não há norma que obrigue os provedores a fazê-lo, a despeito de Termos de Compromisso entre órgãos públicos e provedores[7], celebrados nesse sentido.

5. JURISDIÇÃO E COMPETÊNCIA

5.1. A jurisdição penal brasileira

Concluído o inquérito ou reunidas as provas necessárias, é hora de se propor a correta ação penal. Mas, quando é competente a justiça brasileira?

Com efeito, o Código Penal adotou, em seu art. 6º, a Teoria da Ubiqüidade Mista, a qual preceitua que, para efeitos de competência pátria, lugar do crime tanto pode ser o da ação como o do resultado, ou ainda o lugar do bem jurídico ameaçado ou lesado[8], visando assim evitar o conflito negativo de jurisdição. Para apuração da jurisdição penal brasileira, deve ser, portanto, levado em conta o que disposto na referida norma[9].

---

7. Ibid.
8. Bitencourt (2005).
9. Neste sentido, o STJ, no Conflito de Competência nº 62.949 – Pr (2006/0090645-3), em que se discutia se e quem era competente para apurar incitação ao uso de drogas veiculada num sítio a

Neste sentido, verifica-se, casuisticamente, que os delitos virtuais em voga são *praticados* dentro dos limites da competência pátria. Para fins de apuração do momento e do lugar em que se *praticou* o tipo, há de se verificar o verbo núcleo do tipo do dispositivo incriminador. Assim, difamar, caluniar, injuriar (crimes contra a honra), publicar, divulgar (pornografia infantil), danificar (crimes de dano, provocado através de vírus), falsificar (crimes contra a fé pública), obter vantagem mantendo outrem em erro (estelionato), são condutas que, quando realizadas no mundo material, diz-se que houve a prática do tipo a que se referem. No caso de crimes virtuais, ocorre o mesmo, só que serão realizadas por meio de um computador e do acesso à Internet.

O agente ativo *pratica* o delito quando se dirige a um PC, acessa a Rede e acondiciona nela o que de teor ilícito[10]. V.g., alguém pratica falsidade ideológica quando, usando a Internet, através de algum computador, cria uma identidade falsa dentro da comunidade virtual. É de fácil compreensão, com esteio neste raciocínio, que os crimes virtuais, com os quais lide a Justiça Brasileira, sejam, em quase toda a sua totalidade, praticados em território nacional, porque a natureza dos delitos virtuais denunciados ou para os quais houve queixa diz respeito à nossa realidade (não há notícias de quadrilhas que cometam furto eletrônico mediante fraude[11] de forma transnacional, quando se difama alguém o autor é conhecido da vítima, e assim por diante[12]).

De outro modo, a Teoria da Ubiqüidade Mista abrange as hipóteses mais remotas ao determinar que terá jurisdição o Estado brasileiro quando, mesmo que aqui não praticado o delito, cá seu resultado seja produzido ou projetado. Vale dizer, toda vez que um cidadão seja ofendido ou lesado por crime virtual, toda vez que um bem jurídico nacional for ofendido ou lesado, restará competente a justiça para propositura da respectiva ação, porquanto o resultado produziu-se para dentro dos limites nacionais.

Ressaltemos, entrementes, que nem tudo são flores. O fato de haver jurisdição brasileira para dirimir esta sorte de litígios não quer dizer que será eficaz a sentença penal condenatória brasileira que possa advir. O que se tem em concreto

---

americano, veiculado em língua portuguesa. O STJ acolheu a Teoria da Ubiqüidade Mista, reconhecendo a jurisdição brasileira e determinando a competência da justiça estadual: "As informações são, pois, no sentido de hospedeiro fora do âmbito nacional – hipoteticamente, na Califórnia. Malgrado tal acontecimento – se verdadeiro –, o fato repercutiu mesmo foi no território nacional".

10. Nesta linha, Túlio Vianna (2005).
11. A este respeito, vide dados das ações do Departamento de Polícia Federal: www.dpf.gov.br.
12. Há rigorosas exceções para esta regra, a exemplo da pornografia infantil que, graças ao advento da Internet, virou uma verdadeira indústria internacional, sem fronteiras, de difícil combate por parte inclusive das autoridades brasileiras. Para mais informações, www.safernet.org.br.

é que, por serem crimes que em sua maioria são aqui praticados e que também aqui são verificados os seus resultados, mediante ofensa a bens jurídicos tutelados nacionalmente, a maioria dos agentes ativos do crime são brasileiros. Isto quer dizer que, em tese, para a maioria dos casos, a efetividade do Direito será verificada, porque, identificado o autor do crime, poderá ele ser punido. Diferentemente para as hipóteses em que resida o autor do crime em outro país, quando hão de ser observadas as condições do art. 7º do Código Penal, conjuntamente aos acordos bilaterais e multilaterais que o Brasil haja assinado com o país do infrator estrangeiro.[13]

Sob a tela de delitos inseridos num parâmetro de macrocriminalidade, já se cogita da edificação de uma jurisdição internacional específica[14], algo para que já engatinha o Velho Continente, desde que celebrada a Convenção de Budapeste[15].

5.2. Justiça Estadual ou Federal?

Há uma falsa idéia de que todo injusto penal praticado por meio da Internet seja da alçada da Justiça Federal. Este pensamento deflui de duas errôneas premissas: 1) que a Rede não tem fronteiras e, assim, tratar-se-ia de crime de caráter internacional e 2) a Internet seria um serviço público da União (VIANNA, 2003, p.95)[16]. Rechaçando essas afirmações, embora o *alcance* da Internet seja mundial, os efeitos de um crime são verificados em certa comunidade, localidade (obviamente quando o bem jurídico protegido não resida em mais de um país). Ademais, o crime é praticado de um lugar certo, e não indeterminado, embora assim se mostre num primeiro momento. Sobre o segundo argumento, a União não gere ou está obrigada a gerir a Internet, nem é a Rede uma delegação sua, apenas, por vezes, dela se utiliza. Deve restar claro que serviços públicos prestados pela União são aqueles determinados pela Carta Magna, o que de longe parece ser o caso.

Como supra mencionado, os crimes praticados na Internet nos quais é competente a Justiça Federal são aqueles a que alude o art. 109 da Constituição

---

13. Outro problema está na falta de cooperação de alguns provedores de conteúdo não nacionais, como a Google Inc. O rastreamento técnico só pode ser feito se houver colaboração dos envolvidos, o que por vezes não acontece.
14. A este respeito, FERREIRA (2007).
15. Também chamada de Convenção Internacional contra o Cibercrime, já foi assinada por 47 países (43 estados-membros do Conselho da Europa, mais Estados Unidos, Japão, Canadá e África do Sul). Estabelece padrões de políticas públicas no tratamento do ilícito virtual, bem como facilidades recíprocas para a persecução dos incidentes ilícitos virtuais, quando perniciosos a mais de uma daquelas nações. O Brasil ainda não é signatário.
16. Como decorrência desta conjectura, inúmeros são os casos em que são registradas erroneamente noticia criminis na Polícia Federal, quando deviam sê-lo na Polícia Estadual. Assim, a boa parte dos inquéritos hoje em andamento tanto no Ministério Público Estadual quanto na Polícia Civil tiveram início na Polícia Federal, que envia os expedientes ao reconhecer estes órgãos como os competentes para perquirir aquele tipo penal suscitado.

Federal. No seu inciso IV, a Carta Magna determina que são de alçada federal os crimes praticados em detrimento de bens, serviços ou interesses da União, suas entidades autárquicas ou empresas públicas. Os crimes eletrônicos praticados contra os entes da Administração Federal estão abarcados por este inciso.[17]

O inciso V do referido dispositivo constitucional é o que enseja o mais amplo rol de crimes eletrônicos de competência da justiça federal. A Constituição determina que serão apurados pela justiça da federação os crimes previstos em tratado e convenção nacional, quando iniciada a execução no país o resultado tenha ou devesse ter ocorrido no estrangeiro. Destaques destes delitos são aquelas condutas tipificadas no art. 241 do Estatuto da Criança e do Adolescente e na Lei anti-racismo 7.716/89[18].

Excluídas as hipóteses de competência da Justiça Eleitoral – tal como os crimes tipificados nos arts. 289 a 354 do Código Eleitoral (Lei 4.737/65) – e da Justiça Militar (Decreto-lei nº 1.001/69), residualmente, todas as outras condutas típicas praticadas pela Internet são de competência da Justiça Comum.

Neste sentido tem se posicionado o Superior Tribunal de Justiça:

> PENAL. CONFLITO DE COMPETÊNCIA. CRIME DE INFORMÁTICA. INEXISTÊNCIA DE TRATADO ENTRE OS PAÍSES. NÃO-INCIDÊNCIA DO DISPOSTO NO ART. 109, V, DA CF/88. COMPETÊNCIA DA JUSTIÇA ESTADUAL.
>
> 1. Para a incidência da regra de fixação da competência do art. 109, V, da CF/88, é imperativa a análise da existência ou não de tratado ou convenção internacional entre os países envolvidos na prática criminosa.
>
> 2. A qualidade do órgão policial conducente da investigação é irrelevante para a fixação da competência do Juízo, pois a Carta da República prevê regras distintas na fixação das competências jurisdicional e policial.
>
> 3. Conflito conhecido para declarar a competência do Juízo de Direito da 1ª Vara Criminal da Comarca de Santa Cruz do Sul/RS, suscitado.
>
> (CC 33.871/RS, Rel. Ministro ARNALDO ESTEVES LIMA, TERCEIRA SEÇÃO, julgado em 13.12.2004, DJ 01.02.2005 p. 403).

---

17. O Manual Prático de Investigação do MPF (2006) traz exemplo vistoso, qual seja, o de advogada que por falsidade ideológica na Internet visava a restituições do Imposto de Renda em nome de laranjas. Trata-se de estelionato eletrônico praticado contra a Receita Federal. Neste sentido, as ações que dizem respeito aos correntistas da Caixa Econômica Federal, que tiveram contra si aplicados golpes eletrônicos de furto de senha e respectiva transferência de valores de sua conta, também correm perante os tribunais federais.
18. Cit., CRIMES Cibernéticos: Manual prático de investigação. (2006).

5.3. Foro competente

Para exercer de forma organizada e eficaz o poder de dizer qual o Direito que deve ser aplicado no caso concreto, e, na lide penal, julgando e aplicando a respectiva sanção – se necessário –, o Estado-Juiz repartiu sua jurisdição (*juris*, *dição*) em diferentes competências ordinárias, estabelecendo regras para determinação do foro e do juízo competente.

Para melhor compreensão de o que se trata foro e juízo, institutos comuns ao direito processual civil e penal, valer-nos-emos dos ensinamentos de Fredie Didier Jr. (Vol. I, 6ª Ed., 2006, p. 114):

> Foro é o local onde o juiz exerce as suas funções; é a unidade territorial sobre a qual se exerce o poder jurisdicional (lembre-se que o Estado é soberania de um povo sobre dado território). No mesmo local, conforme as leis de organização judiciária podem funcionar vários juízes com atribuições iguais ou diversas. Assim, para uma mesma causa, verifica-se primeiro qual o foro competente, depois o juízo, que é a vara, o cartório, a unidade administrativa.

Assim é que, *verbi gratia*, a competência da Justiça Comum em cada ente federado é dividida, repartida entre as diversas comarcas (foros) existentes. Para o caso da Justiça Comum baiana, segundo a Lei de Organização do Poder Judiciário daquele Estado, a delimitação territorial da cidade de Salvador corresponde a um foro, a que se chama de comarca. Em cada foro, há diferentes juízos (varas), com diferentes competências materiais. Em grandes foros, como o da capital baiana, onde a demanda ao poder judiciário é maior, há uma contumaz especialização dos diversos juízos sediados naquela comarca. Nestes casos sempre haverá varas (juízos) voltadas para certos assuntos, e que devam apenas deles tratar, de forma distinta e individualmente. Assim é que existem a 1ª Vara da Infância e Juventude, 3ª Vara Cível de Família, Sucessões e Interditos, 8ª Vara da Fazenda Pública, 2ª Vara Crímen, o 11º Juizado Especial Criminal, da Comarca de Salvador (diversos juízos de um mesmo foro, destarte).

Nesta esteira de intelecção, hão de ser adiante dirimidas as regras que conduzem certo ilícito penal para apreciação por parte de predeterminado foro, e para um juízo específico, ou gênero de juízos específicos, porquanto ao se tratar de crimes virtuais, restem elas, ao menos inicialmente, um tanto trabalhosas.

Com efeito, no sistema processual penal pátrio, o legislador ordinário entendeu por estabelecer como foro competente para a causa criminal o lugar onde a infração consumou-se (*locus delicti commissi*)[19]. É o que erigido no art. 70 do Código de Processo Penal.

---

19. TOURINHO FILHO (2006).

Uma vez que a consumação de um delito dá-se pela ocorrência dos elementos de sua definição legal, com esteio nas propriedades da Internet, é possível estabelecer-se critérios comuns a todos os crimes nela praticados para fins de aferição do lugar do delito e, assim, do foro competente.

Preliminarmente, há de se perquirir se o injusto penal investigado trata-se de crime material, formal ou de mera conduta. Crimes materiais (ou de resultado), segundo Paulo Queiroz (3ª Ed., 2006, p. 171), "são aqueles em que o tipo penal descreve um comportamento cuja consumação – entendida como completa realização dos elementos do tipo – somente ocorre com a produção do resultado nele previsto". Cita como exemplo o homicídio (CP, art. 121) e o aborto, quando a consumação do delito implementa-se pela morte da pessoa ou do feto. É necessário, para verificação do momento e do lugar de consumação dos crimes materiais, o resultado típico que transforma o mundo material.

Diferentemente sucede com os crimes formais e de mera conduta, que englobaremos, ambos, num mesmo rol. Nos crimes formais (também chamados de consumação antecipada), o crime consuma-se com a realização da ação típica, sendo despiciendo a verificação do resultado (v.g. concussão art. 116 do CP, basta que se exija a vantagem indevida). De modo similar, a consumação dos delitos de mera conduta dá-se pela ação descrita no tipo, não havendo inclusive menção a qualquer resultado (v.g. invasão de domicílio, art. 150, basta que se *entre, se permaneça*, em casa alheia, clandestina ou astuciosamente).[20]

Retome-se, portanto, que a aferição de qual a natureza do crime virtual (material, formal ou de mera conduta) será relevante para determinação do foro porque o art. 70 do CPP determina que será competente o lugar em que houve a consumação do delito. Por isso, para os casos em que basta que se *pratique* aquela conduta típica para que se *consume* o delito (crimes formais e de mera conduta), o foro competente será aquele em que o agente ativo acessou a Internet através de um computador e veiculou na Rede o conteúdo criminoso ou empreendeu por meio desta aquela ação típica. Exemplifique-se. Se Durval resolve elaborar uma página virtual caluniando o seu síndico, e o fez através do computador de sua casa, o foro competente será aquele de sua cidade, porque os crimes contra a honra são delitos formais, consumam-se tão somente pela prática da conduta típica (*caluniar,* art. 138, no caso, *caluniar pela Internet*)[21]. Ainda que Durval caluniasse, mediante a Rede, alguém de outra cidade, como seu chefe, por exemplo, o foro competente ainda seria o da cidade de Durval, porque o crime contra a honra, por ser formal, consuma-se no lugar que foi *praticado*, e não no espaço em que foram verificados os seus resultados (no caso, na cidade de seu chefe).

---

20. op. cit., QUEIROZ (2006, p. 171)
21. Rezamos que aqui também se amolda o art. 241 do ECA, por se tratar de crime formal.

Neste diapasão, quando se tratar de furto mediante fraude[22] pela Internet, conduta do art. 155, § 4º do CP, por tratar-se de crime material, é necessário para consumação do delito que o agente ativo aproprie-se da coisa alheia móvel (dinheiro em conta bancária) mediante fraude na Rede (por meio de um *trojan* no computador da vítima, por exemplo). A este respeito, inclusive, tem decidido o STJ (CC 86241, CC 86862) que o foro competente será aquele em que a *res furtiva* deixa de estar na posse da vítima, no local de subtração do bem. Se a conta da vítima estava na cidade A, e a do criminoso na cidade B, para onde foram transferidos os valores, o foro competente é o da primeira, porque deve ser fixada a competência para investigação e, eventual, processamento da ação penal no local onde o correntista detém a conta fraudada, no local do dano real – mormente se trate de crime material, de resultado.

Assim, de modo geral, determina-se o foro no caso de crimes praticados na Internet de acordo com a natureza do crime, ou seja, como material, formal ou de mera conduta. Se material, há de se perquirir onde o resultado típico foi produzido, já que a consumação aqui se dá pela ocorrência de modificação na realidade material. Se formal ou de mera conduta, o crime consumou-se pela prática do crime pela Internet, então há de se perquirir de que computador o criminoso teve acesso à Internet para cometimento daquele ilícito.

Superada esta etapa, é necessária a correta análise acerca de qual o juízo competente.

5.4. Juízo competente

Como já colocado, num foro há diversos juízos. Quando em determinada seção judiciária (justiça federal) ou comarca (justiça estadual) houver mais de um juízo que trate de questões penais, dois sucedâneos ganham relevo para os casos de crimes praticados na Rede: I) quando se tratar de crimes de menor potencial ofensivo segundo a Lei 9.099/95 II) quando um deles tornar-se prevento no decorrer das investigações.

Com efeito, a Lei dos Juizados Especiais Cíveis e Criminais (Lei 9.099/95), modificada pela Lei 11.313/2006, define, em seu art. 61, como crimes de menor potencial ofensivo "as contravenções penais e os crimes a que a lei comine pena máxima não superior a 2 (dois) anos, cumulada ou não com multa". E determina

22. Até pouco tempo predominava o entendimento de que quando se tratava de um usuário da Internet que, mantido em erro, fornecia dados bancários ao criminoso, que depois deles se valia para realizar transferências ou saques, seria tipificada tal conduta como estelionato eletrônico (art. 171 do CP). O STJ no Conflito de Competência 2007/0137098-6 rechaçou esta tese, para qualificar a conduta como furto mediante fraude (art. 155, § 4º). Acreditamos que a figura do estelionato eletrônico permanece como típica para inúmeras condutas na Internet, a exemplo de fraude a órgãos públicos, fraude para obtenção de dados de um usuário, como CPF, cartão de crédito, correlatos.

que serão competentes, absolutamente, os juízos especiais criminais para apuração destes crimes de menor potencial ofensivo. Vale dizer, estes delitos não poderiam ser apurados pela Vara crime comum, senão pelos juizados especiais.

Sucede que o rito procedimental nos juizados especiais criminais, não oferta, no mais das vezes, condições apropriadas para o correto destrinchamento dos crimes praticados na Internet. Pela maior complexidade destes delitos, notadamente graças às dificuldades na produção de provas, não seria adequado manter em sua competência crimes tais quais os contra a honra e o de dano, provocados pela Rede.

Parece perfeitamente aplicável, para o caso, o disposto no § 2º, art. 77, da referida Lei. Lá está assinalado que: "Se a complexidade ou circunstâncias do caso não permitirem a formulação da denúncia, o Ministério Público poderá requerer ao Juiz o encaminhamento das peças existentes, na forma do parágrafo único do art. 66 desta Lei". Tal foi o entendimento próspero do Superior Tribunal de Justiça, ao julgar o Conflito de Competência nº 56.786 do Distrito Federal. Vejamos a correspondente ementa.

> CONFLITO DE COMPETÊNCIA. VIOLAÇÃO DO SÍTIO DA EMBAIXADA DOS EUA. POSSÍVEL CRIME DE DANO. AUTORIA DESCONHECIDA. PEDIDO DE QUEBRA DE SIGILO DE DADOS. COMPLEXIDADE. INCOMPATIBILIDADE COM OS PRINCÍPIOS QUE REGEM O JUIZADO ESPECIAL.
>
> 1. O caso em tela não se subsume a nenhuma das hipóteses descritas nos incisos do art. 109 da Constituição Federal. Incompetência da Justiça Federal.
>
> 2. Há evidente necessidade de diligências de maior complexidade para apuração dos fatos e da autoria, providências essas que incluem, aliás, o pedido em questão de quebra de sigilo de dados. Nesse contexto, muito embora o crime de dano, por definição legal, esteja enquadrado como de menor potencial ofensivo, dada as circunstâncias, incompatíveis com os princípios que regem os Juizados Especiais, mormente o da celeridade e o da informalidade, deve o feito ser processado perante o Juízo de Direito Comum.
>
> 3. Conflito conhecido para declarar a competência do Juízo de Direito da 3.ª Vara Criminal da Circunscrição Especial de Brasília/DF.
>
> (CC 56.786/DF, Rel. Ministra LAURITA VAZ, TERCEIRA SEÇÃO, julgado em 27.09.2006, DJ 23.10.2006 p. 256)

Igualmente, sugere-se que já possa o querelante, no caso de crimes de menor potencial ofensivo praticados na Rede, de iniciativa privada, propor a respectiva ação penal privada diretamente na distribuição correspondente aos juízos comuns (vara criminal), ou diretamente no próprio juízo, acaso só houver um no referido foro competente.

Por último, há de se analisar a seguinte situação. Como se sabe, no decorrer da *persecutio criminis*, especialmente no caso dos delitos virtuais, é necessária a

realização de diligências para as quais é imprescindível a autorização judicial. O agente policial competente, invariavelmente, pede a um juiz que ou o autorize a agir ou que determine a outrem que aja, para que se chegue ao resultado útil do processo. Na matéria sob exame, temos que a requisição da Autoridade Policial ao juiz, para que este determine ao provedor que forneça os dados de acesso relativos àquele ilícito penal, torna prevento o juízo, dentre aqueles da mesma circunscrição territorial jurisdicional. Isto de acordo com a lógica adotada no parágrafo único do art. 75 do CPP.

Não obstante, pode ocorrer de que as investigações apontem para um outro foro, verdadeiro lugar do delito, que não aquele no qual foi instaurado o inquérito e em que ficou prevento um juízo. V.g., Ada tem seus dados pessoais indevidamente usados por alguém na Rede, e realiza a *noticia criminis* na Autoridade Competente para esse assunto na cidade em que mora, município de Cidadela. Desta forma, o delegado identifica o provedor de conteúdo e pede a um juiz de Cidadela que solicite os logs de acesso. O pedido é distribuído entre os juízos criminais de Cidadela e o juiz X, da 3ª Vara Crime, é sorteado e assim tornado prevento da futura ação penal que se instaurará. Expedida a ordem judicial, obtido o *log* de acesso junto ao hospedeiro, é identificado o provedor de acesso, e nova ordem é determinada, identificando-se que o acesso criminoso ocorreu na cidade de Vizinhança, perto de Cidadela. As investigações apontam para a tipificação da conduta de que Ada foi vítima como o crime de falsa identidade (art. 307), crime formal, que teria sido consumado, destarte, mediante acesso em Vizinhança, foro competente, em verdade, para a propositura da ação penal.

Soa claro que aquela prevenção não deve prevalecer, porque decorreu de uma presunção segundo a qual o juiz de Cidadela era o competente para conhecer da ação principal[23]. Não é nula, também, a prova produzida, porque consubstanciada em contexto que a fazia perfeitamente legal.[24]

6. CONCLUSÕES NECESSÁRIAS

O surgimento da criminalidade na Rede Mundial impôs ao aplicador do Direito dificuldades para lidar com uma *societas* diferente daquela a que estava habituado e, a rigor, não idealizada pelo legislador penal do século XX. Por este trabalho, viu-se perfeitamente aplicáveis as normas penais, notadamente as de processo penal, às condutas de teor ilícito praticadas pela Internet, sobretudo porque embora implementadas no mundo virtual, traduzem efeitos reais na sociedade já tutelada pelo Direito, resultados que guardam absoluta identidade com aqueles típicos, preconizados e individualizados pelo Direito Penal de Beccaria, Carrara, Roxin.

23. STJ, HC 10243, Edson Vidigal,5ª T., un., 18.12.00
24. STF, HC81260/ES, Sepúlveda Pertence, Pl., un., 19.4.02

Não há outro caminho senão a jurisdicionalização do Estado na Rede, e aqui não se alude à legalização, que perpassa sob outros prismas. Como corolário do brocardo *ubi societas, ubi iuris*, seria impossível crer que um sistema de comunicação desenvolvido e atuado por pessoas não esteja sob o crivo social institucionalizado (o Direito). Este, como última instância reguladora da sociedade – sociedade em sentido amplo para também abarcar a sociedade eletrônica – é ínsito a toda e qualquer relação humana, seja ela travada por artifícios usuais ou contemporâneos.

Resta premente, consoante esta digressão, que o aplicador da norma penal, portanto, ao lidar com os delitos em voga, deve retirar o fino véu de anonimato e extraterritorialidade que, *a priore*, parecem residir na Rede. Não se identifica um objeto pelo que parece ser, senão pelo que de fato é. Reiterando, malgrado seja diverso o seu modo de prática, os seus resultados são previstos pela norma incriminadora e imputados como típicos. *Mutatis mutandi*, segue os moldes de qualquer conduta típica assim já conformada pela *praxis* e pela *legis* tradicional.

Por último, é preciso salutar as iniciativas de órgãos não governamentais, por todo o mundo, como a Safernet Brasil, que lutam para que esta barreira entre sociedade eletrônica e o Estado sejam vencidas. O primeiro passo a ser dado, nesta corrente, é o de demonstrar, aos agentes intervenientes, meios existentes e eficazes para dirimir a maioria dos impasses virtuais que se amontam, para, depois, galgar soluções para outros de maior remonte, como sucede em crimes de pornografia infantil, em que a falta de cooperação internacional tem dificultado a *persecutio criminis*.

7. REFERÊNCIAS BIBLIOGRÁFICAS

FERREIRA, Érica Lourenço de Lima. *Internet. Macrocriminalidade e Jurisdição Internacional.* Curitiba: Ed. Juruá, 2007.

INELLAS, Gabriel César Zaccaria. *Crimes na Internet.* São Paulo: Ed. Juarez de Oliveira, 2004.

KAMINSKI, Omar (Org.). *Internet legal. O Direito na Tecnologia da Informação*. Curitiba: Ed. Juruá, 2003

VIANNA, Túlio Lima. *Fundamentos de Direito Penal Informático. Do acesso não autorizado a sistemas computacionais.* Rio de Janeiro: Ed. Forense, 2003.

MINISTÉRIO PÚBLICO FEDERAL; COMITÊ GESTOR DA INTERNET. *Crimes Cibernéticos. Manual prático de investigação.* São Paulo, 2006.

SAFERNET BRASIL. Disponível em: <www.denunciar.org.br>. Acesso em: 07 de Agosto de 2007.

PRADO, Luiz Regis. *Curso de Direito Penal Brasileiro.* 5ª Edição. São Paulo: Ed. Revista dos Tribunais, 2005.

BITENCOURT, Cezar Roberto. *Código Penal Comentado.* 3ª Edição. São Paulo: Ed. Saraiva, 2005.

TOURINHO FILHO, Fernando da Costa. *Manual de Processo Penal.* 8ª Edição. São Paulo: Ed. Saraiva, 2006.

QUEIROZ, Paulo. *Direito Penal Parte Geral.* 3ª Edição. São Paulo: Ed. Saraiva, 2006.