A PRÁTICA DE CRIMES NA REDE INTERNET E SUAS CONSEQUENTES IMPLICAÇÕES NA APURAÇÃO DA RESPONSABILIDADE CIVIL

Fernando A. Vasconcelos
Professor do Curso de Direito na UFPB e no UNIPÊ

Resumo

A internet tem se mostrado campo fértil para a prática de delitos, dada a facilidade de anonimato dos agentes delituosos. Várias tentativas têm sido feitas com o intuito de coibir e punir esses infocriminosos, muitas delas sem êxito. Neste artigo, busca-se correlacionar os efeitos criminais dessas condutas à responsabilização civil, evidenciando os aspectos modernos da responsabilidade objetiva.
Palavras-chave: Internet. Crimes. Responsabilidade civil

Abstract

The internet has proved fertile ground for the commission of delicts, given the ease of anonymity criminal agents. Several attempts have been made in order to prevent and punish these info-criminals, many of them unsuccessful. In this article we seek to correlate the effects of such conduct criminal civil responsibility, highlighting the modern aspects of strict liability.
Keywords: Internet. Crimes. Liability

1 Introdução

O objetivo do presente trabalho não passa, necessariamente, pela análise criminal das relações que se verificam no mundo da internet. Entretanto, como a prática criminosa e algumas condutas levarão, com certeza, a alguma avaliação de possíveis aspectos da responsabilidade civil, entendemos por bem abordar, no presente estudo, alguns crimes cometidos na rede, com repercussões no mundo civil, especialmente quando afetam os direitos dos usuários da internet.

A internet, quando foi concebida com finalidade de uso militar, estava projetada, inclusive, para resistir a guerras e revoluções. Mas, àquela época, não se sabia ainda sobre a velocidade dos acontecimentos

que a esperavam. Também não se sonhava com o poder dos *hackers*. Estudos recentes revelam que a internet, apesar de aparentar fortaleza e robustez, pode entrar em colapso, caso os *hackers* do mundo todo promovam atos intencionais de bloqueio e destruição. Pela concepção inicial da rede, seria algo inimaginável.

Analisando essa nova criminalidade na internet, principalmente através dos *hackers,* Eduardo Marcelo Castella[1] adverte que os avanços nas áreas das telecomunicações e da informática vêm causando transformações cada vez mais rápidas. Estamos vivendo realmente um "novo tempo", quando informações e serviços circulam com uma rapidez nunca antes imaginada, fazendo com que as pessoas conversem em tempo real de locais tão distantes quanto improváveis.

E quanto aos *hackers*, salienta Castella que, devido a toda essa explosão de conceitos, de comércio e de delitos, os conceitos sobre aqueles têm se tornado bastante comuns. Alguns autores procuram mostrar facetas desses seres habilidosos, salientando os transtornos por eles causados, seja com relação ao tumulto que provocam na vida das pessoas, seja causando transtornos com consequências criminais.

Assim, partindo dessa constatação do aumento da criminalidade na Rede Internet, buscar-se-á um comparativo das consequências desses atos culposos ou dolosos na apuração da responsabilidade civil.

2 Aspectos legais do uso da internet

Muito se tem discutido no Brasil acerca da aplicabilidade da lei no uso da internet. Vários aspectos podem ser enfocados, desde os contratuais aos decorrentes da prática de ilícitos. Se a lei não acompanhou a evolução tecnológica, os juristas e operadores do direito não podem ficar de braços cruzados, esperando por milagres. Hoje já se constata que dispositivos de códigos os mais distintos têm aplicação imediata às relações jurídicas decorrentes do uso dessa ferramenta tecnológica.

Através da internet, pode-se comprar, vender, oferecer toda espécie de serviço, trocar correspondências, informações e ideias. Tudo isso em tempo real e de forma mais barata e rápida do que jamais seria imaginável, já que os custos de manutenção de sites, páginas e "correios" são muito

[1]CASTELLA, Eduardo M. *Investigação criminal e informática*: inteligência artificial x boletim de ocorrência. Curitiba: Juruá, 2005. p.107. Internet: novos aspectos da responsabilidade civil.

inferiores aos de uma empresa do mundo físico, não virtual. Sem esses custos, é possível oferecer produtos e serviços a preços inferiores àqueles que a concorrência tradicional pode praticar. Por isso mesmo, leis internas e internacionais estão sendo preparadas e adotadas em todos os países e blocos econômicos do planeta, dentro de uma lógica comum, para a proteção dos indivíduos que fazem parte dessa nova comunidade.

Certificação eletrônica, segurança na rede, privacidade, são temas em destaque. O comércio eletrônico é uma realidade indiscutível. Novos problemas surgem a cada minuto e deverão ser enfrentados com rapidez, tirocínio, bom senso. As compras coletivas, através de *sites* especializados, tiveram o seu auge há poucos anos, mas, da forma como surgiram rapidamente, também estão desaparecendo da preferência dos internautas consumidores[2].

Problema jurídico relevante é a utilização da internet para transferência ilegal de moeda, a célebre "lavagem de dinheiro". Bancos Centrais de alguns países já estão tomando medidas preventivas para coibir esse campo fértil da ilicitude. Novos sistemas de financiamento, de troca eletrônica de moedas e de pagamentos *on-line*, deverão sofrer regulamentação mais adequada, a fim de que não se constituam ameaça aos sistemas existentes de controle de moedas.

Ainda hoje, para a maioria dos que se preocupam com a informática e a internet, há dificuldades para uma ação policial eficaz, pela utilização de cadastros falsos nos registros em provedores, roubo de senhas em *cybercafés*, mecanismos pelos quais agem *hackers* e outros especialistas em crimes e danos internéticos. Quando não há registro do usuário, a polícia busca localizar a linha da qual é feito o acesso. Esse tipo de identificação só é possível se o criminoso voltar ao local do crime, tentando conectar-se novamente.

Quando se analisa a necessidade de adaptação da legislação aos fenômenos sociais, verifica-se que uma das características fundamentais do ordenamento jurídico é o dinamismo de seus preceitos, que permite a adequação das normas jurídicas às constantes evoluções nos diversos campos da atividade humana. Seria temerário se o Poder Legislativo permanecesse inerte ante os relevantes fenômenos sociais, não editando os postulados legais a reger as novas situações de fato.

2VASCONCELOS, Fernando A. *Internet*: responsabilidade do provedor pelos danos praticados. Curitiba: Juruá, 2005. p.45.

Evidentemente, seria impossível uma abrangência integral do texto da lei para todos os casos que fossem surgindo, em lugares e situações as mais diversificadas. Não seria coerente nem salutar que os operadores do direito fossem obrigados a utilizar, por longo lapso temporal, as fontes subsidiárias para a resolução das pendências. A necessidade de criação da norma pode ser indicada por diversos fatores, dentre estes, os econômicos, os políticos e os sociais.

3 Informática e invasão de computadores

Especialistas em manutenção e supervisão técnica da rede internet vêm alertando, com dados precisos, sobre a possibilidade de falhas na estrutura da rede, vulnerável a um ataque maciço de *hackers*. Um ataque aos servidores que armazenam endereços de todos os *sites* registrados na *Web* poderia travar a internet. O papel desses servidores é redirecionar o tráfico na rede, para que o usuário possa chegar ao domínio requisitado.

Um estudo realizado pelo CERT (*Computer Emergency Response Team*[3]) , do governo norte-americano, revelou que, em entre 2001 e 2011, aconteceram milhares de ataques a computadores em todo o mundo, ocasionando não só responsabilidade criminal, mas também a possibilidade de reparação de danos. Por outro lado, os relatos de fraudes em aquisições de produtos na internet já congestionam a própria rede mundial de computadores. Vários *sites* dedicam páginas e mais páginas ao assunto. Ofertas mirabolantes, produtos inacessíveis, negócios impossíveis são detectados a todo o momento, ocasionando grande desconfiança no meio virtual e, consequentemente, descrédito em relação aos que lidam com a internet.

À medida que a tecnologia do mundo virtual vai-se sofisticando e tornando-se mais poderosa, pode chegar o momento em que a sociedade precisará regulamentar a realidade virtual, do mesmo modo como regula o mundo real, físico. Mas as dificuldades serão inúmeras. Tome-se, como exemplo, a decisão, no longínquo ano de 2002, da Suprema Corte dos Estados Unidos, que rejeitou, por sete votos a dois, um projeto de lei que teria transformado em delito penal "fazer, vender ou possuir pornografia infantil virtual que utilize imagens computadorizadas de crianças, em vez de fotos reais". Nessa decisão, o juiz da Suprema Corte, Anthony

[3]Cf. Disponível em:<http://www.cert.org/>. Acesso em: 24 jun. 2012.

Kennedy, no seu voto em favor da maioria, afirmou que essa lei tornaria ilegal a retratação virtual de uma ideia - neste caso, adolescentes praticando atividades sexuais. Mas, como adolescentes reais fazem sexo e como crianças imaginárias não podem ser vítimas de um crime, a lei proíbe uma linguagem, ou expressão, que não registra nenhum crime e não cria nenhuma vítima[4].

Registrar domínios com nomes ou expressões características de outrem, além das sanções civis, pode ser considerado crime. A FAPESP[5], que é a entidade responsável pelo registro de domínio na internet, aponta que ultimamente ocorreram vários casos de registro de domínio de nomes famosos por terceiros, que geralmente agem de má-fé. Assim, para adquirir o domínio, o nome deve ser "registrável". Entende-se por não registrável, dentre outros, o nome que possa "induzir terceiro a erro", como aqueles que representam marcas famosas ou notoriamente conhecidas.

Ainda de acordo com a FAPESP, a marca é, com certeza, o patrimônio mais importante de qualquer negócio. O nome da sua marca representa a identidade e a reputação de um negócio, seja ele baseado em uma atividade de profissional liberal ou de uma empresa. O nome de domínio é, no mundo negocial, a identidade digital, permitindo que pessoas físicas ou empresas sejam localizadas na Internet. Registrar e proteger nomes de domínio são tão importantes quanto garantir direitos sobre marcas e patentes. Ter uma identidade digital não é um luxo, e sim uma necessidade para qualquer empresa ou profissional que pretende atuar na rede.

4 Danos e possíveis soluções

A nova era da intercomunicação traz problemas gravíssimos, ainda não devidamente debatidos. A internet é alvo de novas espécies de meliantes, os "infocriminosos", que agem anonimamente e se consideram inatingíveis. Chegar a esses criminosos não é tão difícil como pode parecer, desde que certos fatos estejam sob controle. Como a conexão à rede se dá por meio de um protocolo denominado IP (*Internet Protocol*), cada provedor tem números próprios, concedendo a seus usuários

[4]Cf. JORNAL O ESTADO DE SÃO PAULO. Disponível em:< www.estadao.com.br >. Acesso em: 20 abr. 2002.

[5]Cf. Disponível em: <http://www.fapesp.org/oque_e.htm>. Acesso em: 24 jun. 2012.

números IP subordinados ao seu. Rastreado o IP do infrator (o que é simples), chega-se a seu provedor. Mediante ordem judicial, é então possível obter o cadastro do agente delitivo, que pode então ser detido. Já os provedores gratuitos, que oferecem prestação de serviços não remunerada, deixam à disposição dos usuários uma senha coletiva e um único nome de referência, proporcionando o aparecimento de questões de suma gravidade, envolvendo responsabilidade civil e criminal.

Os provedores de acesso podem parar de guardar registros individuais dos seus usuários, pois não mais necessitam deles para cobrança. De igual modo, não têm mais interesse econômico em manter esses registros de acesso. Embora os cadastros tenham valor econômico, a guarda desses dados torna-se cara e inútil, para os provedores gratuitos.

Dadas as facilidades de acesso, qualquer pessoa pode entrar anonimamente na internet com objetivos criminosos, com mínima chance de identificação. A segurança só aumentará quando instrumentos eficazes de combate ao crime forem criados. Entidades de certificação, autorizadas pelo Estado na forma do art. 174 da Constituição, podem certificar registros internos de sistemas e assinaturas eletrônicas em documentos e contratos, oferecendo maior segurança ao sistema de intercomunicação e contratação eletrônica.

Uma providência que minimizaria alguns problemas poderia ser tomada, determinando-se aos provedores de acesso à internet que mantenham em seus sistemas os cadastros individuais de seus usuários e, durante certo período, os registros de acesso e identificadores de chamada nas linhas de acesso. A manutenção desses cadastros e registros, visando a preservar os macrointeresses da sociedade cibernética, contribuiria para a evolução segura das comunicações virtuais, exercendo os provedores papel relevante nesse emaranhado de sistemas intercomunicativos.

O acesso gratuito à rede mundial se constituiu, quando da implantação da internet no Brasil, uma revolução dentro da informática, praticada por alguns provedores e bancos, que oferecem, com relativa frequência, esse serviço à sua clientela. A competição entre os provedores de acesso tornou simples e grátis o acesso à rede, popularizando rapidamente esse revolucionário instrumento de comunicação coletiva.

Através da internet, pode-se comprar, vender, oferecer e fornecer serviços, trocar correspondências, informações e ideias, tudo em tempo real e de forma mais barata e rápida nunca antes imaginada. Com o baratea-

mento dos custos, é possível oferecer produtos e serviços a preços inferiores àqueles normalmente praticados no mundo real. Por isso mesmo, leis de caráter interno e internacional estão sendo preparadas e adotadas em todos os países e blocos econômicos do planeta, dentro de uma lógica comum, visando à proteção dos indivíduos e da comunidade chamada cibernética[6].

5 Massificação e atitudes delitivas

Existe certo receio do que poderá advir com a massificação das comunicações eletrônicas. O temor decorrente da utilização dos cartões de crédito, por exemplo, será superado pelos usuários da rede se cartões de compra ou de negociação eletrônica existirem, transferindo o risco para empresas ou determinados profissionais.

A lavagem de dinheiro pela internet, que já é perfeitamente constatável, necessita ser coibida. De acordo com os estudos até agora realizados, principalmente através de matérias publicadas em jornais e em *sites* jurídicos, os *hackers* e criminosos internéticos dificultam a ação policial, utilizando cadastros falsos nos registros dos provedores, roubando senhas em *cybercafés*, além das mais variadas formas de invasão.

Quando não consegue interceptar o registro do usuário, a polícia busca localizar a linha através da qual é feito o acesso a determinado ponto. Esse tipo de identificação só é possível se o criminoso voltar ao local do crime, ou seja, se vier a conectar-se novamente, sob certas condições. Exemplo recente foi relatado pela grande imprensa e ocorreu quando conhecido empresário brasileiro foi acusado de ter cometido crime eletrônico, tendo sido localizado apenas porque acessou novamente seu *e-mail* anônimo. Se não o tivesse feito, nunca teria sido encontrado.

O colunista Patrick Collinson, do jornal londrino *The Guardian*[7], publicou interessante matéria a respeito das facilidades para obter-se o número do cartão de crédito, data de vencimento, número de telefone e endereço para cobrança de uma pessoa. Precisa-se só de alguns segundos para obterem-se essas informações, penetrando nos florescentes *cyber-bazares* operados pela internet, nos quais especialistas criminosos e organizados compram e vendem cartões de crédito e identidades.

---

[6]VASCONCELOS, Fernando A. *Internet*: responsabilidade do provedor pelos danos praticados. Curitiba: Juruá, 2005. p.56

[7]Cf. <www.guardian.co.uk/profile/patrickcollinson>. Acesso em: 5 set. 2011.

Mas esses são participantes em pequena escala. Segundo a matéria jornalística enfocada, o centro de comércio de cartões de crédito do mundo é São Petersburgo, na Rússia. É o local de muitos mercados secretos na internet, onde detalhes sobre cartões são oferecidos no atacado, geralmente custando US$ 1,00 por cartão, vendidos em lotes de quinhentos a cinco mil.

O negócio geralmente é feito por meio de *websites* de acesso aberto ou em *newsgroups*, que são sessões de *chat* ponto a ponto, que fazem a ligação de pessoas interessadas num determinado assunto. Nesses *chats*, podem se reunir grupos de *hackers* com objetivos comuns. *Hackers* de menor potencial ofensivo podem ser convidados para um canal de escalão superior, mais limitado, onde pessoas trocam dicas, truques e cartões de crédito. Piratear um cartão de crédito está se tornando um ato normal no mundo criminoso dos que se utilizam da internet com objetivos pouco convencionais.

Uma prova alarmante da tendência de globalização da fraude com cartões é o fato de que um terço do uso fraudulento de cartões, registrados em território britânico, ocorre no estrangeiro, pois "chupadores de dados" e *hackers* recolhem as informações no Reino Unido, mas usam-nas longe do domicílio de seu detentor. Avanços na tecnologia facilitam que quadrilhas movimentem informações ao redor do mundo com extrema facilidade.

Hackers raramente buscam os bancos de dados das instituições bancárias e dos emissores de cartões de crédito ou os sistemas de transmissão conhecidos. Estes são sistemas ferozmente protegidos que até agora se revelaram impenetráveis a quadrilhas. Mas existe um meio muito mais fácil de obter detalhes sobre cartões de crédito: os criminosos visam aos servidores de empresas *on-line* onde são mantidos os detalhes dos cartões dos clientes. A insegurança da internet não está na transmissão, por uma pessoa, de seus detalhes sobre o cartão de crédito através da Rede ou do telefone, mas no modo como esses detalhes são guardados nos seus arquivos pessoais.

Alguns casos relatados na grande imprensa nos dão uma ideia da sofisticação dos criminosos virtuais. Senão vejamos: números de cartões de crédito revelados em *websites* para adultos, quando *hackers* penetraram em suas páginas e acessaram detalhes sobre números; números de mais de cem mil cartões de crédito furtados de Administradoras; revendedoras de obras musicais, que perderam detalhes sobre cartões de

crédito de milhares de seus clientes para *hackers*; fechamento de *websites* por vários dias, depois que uma falha na segurança permitiu a *hackers* acesso a milhões de registros contendo detalhes sobre cartões de crédito e de débito.

6 Soluções legislativas

No Brasil, embora timidamente, já se começam a esboçar reações legislativas. Figuras delitivas inimagináveis pelo legislador de 1940 foram tipificadas por intermédio da Lei 9.983, de 2000, modificando a parte especial do Código Penal, com vistas a combater os delitos previdenciários e a utilização da informática ou banco de dados dos órgãos de seguridade social e do Estado de forma geral. E a reforma do Código Penal, em tramitação no Congresso Nacional (Projeto de revisão do Código Penal - PLS 236/2012) promete mudanças na área dos crimes virtuais[8].

Entre os novos tipos penais, merece destaque a alteração do art. 325 do CP, que prevê o crime de violação do sigilo funcional inserto no Título XI: "Dos Crimes Praticados contra a Administração Pública". O legislador de 1940 buscou proteger a pessoa no tocante à inviolabilidade do segredo, pois o agente revela um fato da vida íntima de alguém que tinha o interesse no sigilo, mas que confia a outrem em razão de sua especialidade profissional. Daí estarem previstos no capítulo que trata dos crimes contra a pessoa, protegendo especificamente o atributo liberdade individual: os segredos.

Na redação atual, os modos de execução do crime foram ampliados. O legislador estabeleceu uma forma de falsidade ideológica especial, quando o modo de execução do crime consiste ''na manipulação dos dados contidos no sistema de informação ou banco de dados da administração''. O sigilo profissional pode ser violado quando o funcionário público não comunica, verbalmente ou por escrito, o fato a terceiro. Entretanto, permite ou facilita que o particular ou funcionário não autorizado ingresse no sistema de informação ou banco de dados da administração pública, de forma a ter acesso a todas as informações ou dados desejados, que deveriam

[8]SENADO FEDERAL. Disponível em: <www.senado.gov.br/atividade/materia/detalhes>. Acesso em: 5 ago. 2015.

permanecer em segredo, mediante o empréstimo ou a cessão de senha ou possibilitando outra forma de ingresso no sistema de informações.

O delito tem como autor aquele que possui acesso, lícito ou ilícito, ao sistema ou banco de dados, seja servidor público ou particular. O funcionário público, autor da infração penal, pode ser o que tem por função atribuir ou fornecer a senha, logo, quem tenha controle de acesso ao sistema, ou que recebe, mediante atribuição ou fornecimento da autoridade competente, ou ainda na terceira hipótese, o que empresta a senha a outrem.

O receptor, igualmente autor do ilícito, é pessoa que não tem acesso ao sistema ou apenas a determinadas informações que não englobam aquelas que foram objeto de violação, só tendo conhecimento em decorrência do ilícito penal ocorrido. O particular, por sua vez, será autor do crime quando agir em concurso com o servidor público, nos termos do art. 30 do Código Penal.

Poderá ainda ser autor do delito aquele que viola o sistema mediante "quebra de acesso restrito", implicando dizer que irá ingressar no banco de dados ou sistema sem possuir autorização, mas usando um procedimento dos chamados *hackers*, que invadem sistema ou banco de dados em razão do conhecimento de equipamentos com tecnologia cibernética avançada e do fato de se depararem com sistema de segurança fragilizado. Não escapam à ação penal aqueles que realizam função pública terceirizada, porque a alteração penal ocorrida visou precipuamente a proteger o sistema de informação da Previdência Social.

Note-se, por fim, que a modificação do Código Penal vem corroborar a premente necessidade de previsão de crimes praticados com o auxílio da informática, através do computador ou contra o sistema de Internet: informação ou bancos de dados nele contidos, resguardando a integridade dos órgãos que compõem a Previdência Social.

Casos de difamação e injúria vêm se tornando cada vez mais frequentes em meio virtual. Por conta disso, magistrados e tribunais já estão fazendo o necessário relacionamento entre o crime e o dano, para efeito de responsabilização civil. Entretanto, é necessário que se tenha sempre em mente a ideia de que não é só pelo simples fato de uma conduta ter sido praticada pela internet, que irá, necessariamente, ser analisada

sob os princípios do Direito Eletrônico (Cibernético), esquecendo-se dos operadores jurídicos das normas penais[9].

Se a conduta ou o fato constituírem crime, já previsto expressamente no Código Penal, a apuração e punibilidade pertencem a este ramo do Direito, independentemente do meio através do qual é cometido (seja verbalmente, por escrito, pela internet) e sem prejuízo da possível reparação. Pertencem, pois, à área dos crimes de informática comuns, já que estão tipificados no Código Penal apenas pelo fato de terem sido praticados através da internet.

Constantemente, pessoas procuram órgãos policiais, denunciando que foram alvo de alguma brincadeira ofensiva ou maldosa pela internet, desde a criação de *sites* em que se expõem fotos da ex-namorada em situações constrangedoras, até a produção de informações falsas contra a honra, passando por aqueles que divulgam, pela rede, casos falsos de traição de terceiros ou a realização de fotomontagens.

Nesses casos, estaremos diante dos crimes previstos nos artigos 139 e 140 do Código Penal, respectivamente, injúria e difamação. São crimes que atingem a honra subjetiva da pessoa e o sentimento quanto aos seus atributos físicos, morais, intelectuais e demais valores da pessoa humana, tendo o autor do crime plena consciência de que está lesando voluntariamente a honra do outro, ofendendo a sua moral e expondo ao público um ato agressivo à sua reputação.

Ao praticar estes crimes, muitas vezes o autor tem a falsa ideia de que irá conseguir se manter no anonimato, usando *e-mails* gratuitos criados livremente, ou montando páginas em *sites* que não exigem os dados do autor. Entretanto, para a polícia não é difícil descobrir quem está por trás da agressão. A investigação baseia-se em um número que cada computador recebe toda vez que acessa a internet e fica registrado nos provedores: é a chamada sequência IP. Identificando-se o autor e quando a vítima possui a mensagem difamatória, abrem-se para ela duas opções:

a) o ingresso imediato com a ação penal por injúria ou difamação (buscando a condenação criminal do agente), com posterior execução na esfera civil da sentença criminal, para fins de indenização;

b) o ingresso, unicamente, com a ação civil de indenização por danos morais, devendo, neste caso, ser provadas a autoria e a materiali-

[9]ARRUDA JR. Itamar. *Provedores não colaboram com processos de ofensas pela web*. Disponível em: <http://www.conjur.com.br/2001-dez-14/provedores_colaborar_informacoes_acoes>. Acesso em: 12 maio 2012.

dade do fato. Ressalte-se, aqui, que, ao optar por esta segunda alternativa, a vítima pugna apenas pelo recebimento da indenização em dinheiro, abrindo mão da condenação criminal do agente. Embora a questão aparente simplicidade, há grande dificuldade de ordem prática de localizar-se o agente criminoso, em virtude da ausência de cooperação dos provedores de internet. Estes, na maioria das vezes, se negam a fornecer informações às vítimas, somente o fazendo mediante determinação judicial, ocasionando danos de natureza às vezes irreversível. Como exemplo desse tipo de ocorrência, citamos um caso envolvendo aspectos criminais e reparação de danos de natureza civil, em que o provedor somente forneceu as informações necessárias judicialmente.

A conhecida "Lei *Carolina Dieckmann*" (Lei n.º 12.737/2012) foi sancionada em 3 de dezembro de 2012 pela Presidente *Dilma Rousseff* e promoveu alterações no *Código Penal Brasileiro*, tipificando os chamados delitos ou crimes informáticos. A legislação pune, principalmente, os delitos praticados por *hackers*, incluindo os crimes de sabotagem, falsidade e fraude informática. O texto legal autoriza ainda as autoridades a interceptarem dados dos provedores e prevê a pena de reclusão para quem armazena, em meio eletrônico, material pornográfico, envolvendo criança ou adolescente.

Referida lei tem merecido críticas de juristas, peritos, especialistas e profissionais de segurança da informação, pois seus dispositivos são amplos, confusos e podem gerar dupla interpretação, ou mesmo interpretação subjetiva. Isso poderá ensejar enquadramento criminal de condutas triviais ou mesmo para a defesa e respaldo de infratores cibernéticos, o que tornaria a lei injusta e ineficaz. Para outros, as penas são pouco inibidoras, sendo muitas situações enquadráveis nos procedimentos dos Juizados Especiais, o que poderia contribuir para a não eficiência no combate ao crime cibernético no Brasil.

De novidade, tivemos, finalmente, a sanção da Lei Nº 12.965, de 23 abril de 2014, o denominado Marco Civil, que "estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil". Não é um texto que cuida da parte criminal da área tecnológica. Aliás, ficou muito aquém das expectativas dos estudiosos da área. No artigo 2.º, percebe-se que "a disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais". São, ainda, respeitadas a pluralidade e a diversidade, a livre

iniciativa, a livre concorrência, a defesa do consumidor e a finalidade social da rede.

O Marco Civil poderá ajudar na discussão sobre os efeitos civis da responsabilidade criminal quando trata do "direito de acesso à internet a todos, acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos". Ainda consta do texto a guarda e utilização dos dados, muito pertinente à preservação da privacidade.

6.1 O caso e a decisão

Foram postadas no serviço de um determinado provedor diversas mensagens de cunho difamatório, assinadas supostamente por um advogado, inclusive constando seu *e-mail* utilizado na época. Diversas pessoas chegaram a "conversar" com o falso "advogado", tendo inclusive colocado no ar mensagens altamente ofensivas e ameaçadoras em relação ao mesmo. O advogado real somente tomou conhecimento do fato ao ser avisado por terceiros, pois nunca teria utilizado aquele serviço.

Como o provedor se negou a fornecer o nome do responsável pelas mensagens, o prejudicado ajuizou "ação de obrigação de fazer, com pedido de antecipação de tutela" contra a empresa provedora, tendo sido deferida a tutela antecipada para imediata retirada das mensagens da internet. Em audiência de conciliação, o provedor de acesso informou que o responsável por todas as mensagens assinadas em nome do advogado era um antigo desafeto deste.

Posteriormente, foi ajuizada uma ação de reparação de danos extrapatrimoniais contra o indigitado falsário[10], encerrada através de composição amigável e sendo plenamente esclarecido o lamentável episódio. Todavia, não se podem esquecer os prejuízos sofridos pelo advogado, personagem do mundo jurídico real, fato que poderá ocorrer rotineiramente, afetando cada um dos que atuam no mundo cibernético.

Constata-se, com certa facilidade, que as ocorrências criminosas, envolvendo difamação ou injúria praticadas na *Web*, devem ser apuradas de acordo com as disposições constantes do Código Penal, sendo rapidamente resolvidas se houver uma maior cooperação dos provedores para

[10]Disponível em:< www.tjsp.jus.br>. Acesso em: 12 dez. 2010.

com os ofendidos. E, uma vez apuradas ou não essas práticas, ao ofendido cabe buscar a reparação pelos danos contra ele praticados.

6.2 Pesquisa e as soluções

Nos Estados Unidos, de acordo com a legislação de cibercrimes do país e uma pesquisa realizada pela empresa de segurança digital *Symantec*[11], onde a preocupação com esses criminosos beiram às raias da paranoia, *hackers* que colocarem vidas humanas em risco, invadindo computadores pela internet, poderão ser condenados à prisão perpétua. A punição para os cibercriminosos se baseia no dano econômico que eles tenham causados, o que muitas vezes isenta os responsáveis de penas mais severas.

A pesquisa estimou que o prejuízo global com golpes virtuais passou dos US$ 110 bilhões (ou R$ 224,35 bilhões) no último ano. O estudo ouviu treze mil pessoas de dezoito a 64 anos em 24 países, entre eles o Brasil. Somente por aqui, o valor desperdiçado com cibercrimes giraria em torno de US$ 8 bilhões (cerca de R$ 16,3 bilhões), enquanto em países como Estados Unidos (US$ 21 bilhões ou R$ 42,8 bilhões) e China (US$ 46 bilhões ou R$ 93,8 bilhões), a perda seria ainda maior.

O levantamento descobriu, ainda, que, apenas nos últimos doze meses, 556 milhões foram vítimas de golpes virtuais, o que representa mais de 1,5 milhão de vítimas por dia ou dezoito por segundo. Assim, tudo está a indicar que o prejuízo médio com golpes virtuais ficou em torno de US$ 197 (cerca de R$ 400) por pessoa.

Por outro lado, o governo americano diminuiu as restrições de monitoramento antes tomadas pelos provedores de acesso, o que garantia a privacidade na internet. Desde algum tempo, os provedores podem informar a polícia sobre atividades suspeitas em suas redes, mesmo que elas não representem ameaça imediata. A legislação anterior proibia os provedores de abrirem informações sobre seus usuários, a não ser que elas causassem perigo imediato de morte ou ferimento. Também permitia aos usuários processarem as empresas em caso de violação de privacidade.

Estudiosos querem que a Justiça dos EUA também leve em conta as intenções do criminoso e outros fatores, a exemplo do alvo do ataque:

[11] Cf. Disponível em:< http://www.modulo.com.br/comunidade/noticias/2862>. Acesso em: 19 set. 2012.

computadores importantes do governo ou de empresas. Por outro lado, na onda de paranoia que tomou conta dos EUA depois dos atentados de 11 de setembro, o governo diminuiu as restrições de monitoramento antes tomadas pelos provedores de acesso, o que garantia a privacidade na internet.

A partir de então, os provedores passaram a informar à polícia sobre atividades suspeitas em suas redes, mesmo que elas não representem ameaça imediata. A legislação anterior proibia os provedores de abrir informações de seus usuários, a não ser que elas causassem perigo imediato de morte ou ferimento. Também permitia aos usuários processar as empresas em caso de violação de privacidade.

7 Conclusão

Pelo que foi visto acima, é fácil se concluir quão difícil é separar, no mundo virtual, a responsabilidade civil da criminal, pois as várias formas de conduta estão intimamente relacionadas, mesmo que o autor do dano não aja de forma dolosa. Espera-se, num futuro próximo, que o legislador trate das duas formas punitivas de maneira interligada, a fim de facilitar o trabalho dos operadores do direito na análise do crime e do dano.

Ações como invasão de computadores, furto de senhas e conteúdo de *e-mails*, além da comercialização do material obtido de forma ilegal, são consideradas crime. Condutas mais danosas, como obter pela invasão conteúdo de "comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas" podem ter pena de três meses a dois anos de prisão, além de multa. Também agrava o quadro a divulgação, comercialização ou transmissão a terceiros, por meio de venda ou repasse gratuito, do material obtido com a invasão.

Todas essas condutas criminosas geram, por consequência, possibilidade de reparação de danos. A modernidade caminha para uma responsabilidade civil de caráter objetivo, sem aquelas dificuldades da apuração subjetiva de uma conduta delituosa. E, com a consolidação dessa relação fato/dano/nexo de causalidade, sem as artimanhas da dupla culpa/dolo, com certeza os julgadores terão maior campo de atuação para responsabilizar civilmente os criminosos cibernéticos.

Referências

ARRUDA JR. Itamar. *Provedores não colaboram com processos de ofensas pela web*. Disponívelem:<http://www.conjur.com.br/2001-dez-14/provedores_colaborar_informacoes_acoes>. Acesso em: 12 maio 2012.

CASTELLA, Eduardo M. *Investigação criminal e informática*: inteligência artificial x boletim de ocorrência. Curitiba: Juruá, 2005. p.107. Internet: novos aspectos da responsabilidade civil.

CERT. Disponível em: < http://www.cert.org/>. Acesso em: 24 jun. 2012.

FAPESP. Disponível em:< http://www.fapesp.org/oque_e.htm>. Acesso em: 24 jun. 2012.

JORNAL O ESTADO DE SÃO PAULO. Disponível em: <www.estadao.com.br>. Acesso em: 20 abr. 2002.

MÓDULO COMUNIDADE. Disponível em: <http://www.modulo.com.br/comunidade/noticias/2862>. Acesso em: 19 set. 2012.

SENADO FEDERAL. Disponível em: <www.senado.gov.br/atividade/materia/detalhes>. Acesso em: 5 ago. 2014.

THE GUARDIAN. Disponível em: <www.guardian.co-.uk/profile/patrickcollinson>. Acesso em: 5 set. 2011.

TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Disponível em: <www.tjsp.jus.br>. Acesso em: 12 dez. 2010.

VASCONCELOS, Fernando A. *Internet*: responsabilidade do provedor pelos danos praticados. Curitiba: Juruá, 2005.