CRIMES ELETRÔNICOS

EMÍLIA MALGUEIRO CAMPOS
Advogada, pós-graduada em Direito Processual pela Universidade Paulista, MBA pela Business School of São Paulo. Sócia do escritório Malgueiro Campos Advocacia. E-mail: emilia@malgueirocampos.com.br

MAÍRA LINS PRADO
Advogada, graduada pela Faculdade de Direito de São Bernardo do Campo, atuante na área da Propriedade Intelectual desde 2012. E-mail: mlp.maira@gmail.com

1. INTRODUÇÃO

Ao considerarmos o desenvolvimento tecnológico das últimas décadas e sua influência nas relações interpessoais e comerciais, bem como o compartilhamento de dados e informações advindo destas novidades em escala global, pouca reflexão é necessária para se admitir a existência de novos gêneros de práticas ilícitas, a que se tem chamado de criminalidade digital.

Justamente graças à expansão mundial dos sistemas computadorizados e da internet é que estas condutas são especialmente perigosas, já que a possibilidade de acesso remoto por aqueles capazes de decifrar sistemas dá origem a crimes sem fronteiras e de difícil rastreamento.

Através da internet qualquer informação, lícita ou não, pode ser rapidamente divulgada aos quatro cantos do mundo e a cada dia cresce a parcela da população mundial que tem acesso aos sistemas informatizados.

Justamente por conta da dificuldade de rastreamento dos atos praticados na rede mundial, THIEFFRY,[1] citado por Bruno MIRAGEM,[2] afirma que a internet é a "ilusão efêmera de uma zona de *não-direito*". Ocorre certa dificuldade de adaptação das normas tradicionais da sociedade ao universo virtual, em que as relações são mais distanciadas.

No entanto, trata-se de uma ilusão efêmera, pois tal distanciamento não torna impossível o rastreamento das condutas ilícitas e sua consequente punição.

Os crimes eletrônicos constituem, portanto, uma novidade em nosso sistema jurídico, sendo também denominados de crimes de informática, crimes com computador, *e-crimes*, *cybercrimes* etc. (FERREIRA e JÚNIOR, 2010).

Paulo Marco FERREIRA LIMA descreve os crimes de computador como sendo "qualquer conduta humana (omissiva ou comissiva) típica, antijurídica e culpável, em que a máquina computadorizada tenha sido utilizada e, de alguma forma, facilitado sobremodo a execução ou a consumação da figura delituosa, ainda que cause um prejuízo a pessoas sem que necessariamente se beneficie o autor ou que, pelo contrário, produza um benefício ilícito ao seu autor, embora não prejudique a vítima de forma direta ou indireta."[3]

Se por um lado a utilização da internet e dos sistemas informatizados é uma realidade cada vez maior, é fato que a transmissão e o arquivamento de dados pela rede ainda não são operações totalmente seguras, estando suscetíveis a invasões e usos ilícitos, gerando prejuízos e danos aos usuários.

Diante dessa nova realidade, coube ao Direito adaptar a legislação existente para o mundo digital, verificando as hipóteses impossíveis de serem resolvidas pelo arcabouço jurídico atual, com a proposição de legislação que regulasse a matéria em todos os seus aspectos.

Ora, tendo em vista que o Código Penal brasileiro foi elaborado na década de 1930, realmente seria de difícil aplicação aos crimes eletrônicos a Parte Especial do Código. Contudo, sempre será possível aplicar os princípios gerais do Direito Penal, previstos na Parte Geral do Código, a esses tipos de conduta.

Existe ainda certa ressalva na classificação de algumas destas condutas do meio digital como crimes, já que, para tanto, seria necessário atenção aos princípios da legalidade e da anterioridade, devendo existir prévia tipificação legal como crime, para que se tornem passíveis de punição. É neste quadro que encontramos, talvez, a maior problemática do tema.

Enfrenta-se não apenas a questão da suficiência das normas, no sentido de se decidir pela aplicação das normas já existentes aos novos casos, ou pela criação de regulamentação específica para o mundo virtual, mas também a adequação e efetividade destas normas, às já vigentes, ou às que se pretendem criar.

Pensamos que uma solução intermediária seria a ideal: aproveitar-se o quanto possível a legislação existente, deixando para nova regulamentação apenas as hipóteses realmente novas, não abrangidas pelos textos atuais.

1. THIEFFRY, Patrick. Commerce électronique. Droit international et européen. Paris: Éditions Litec, p. 2, 2002.
2. MIRAGEM, Bruno. Responsabilidade por danos na sociedade de informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. *Revista de Direito do Consumidor*, vol. 70, p. 41, abril de 2009.
3. Crimes de computador e segurança computacional, p. 31.

. Nomenclatura

A nomenclatura utilizada no espaço virtual rapidamente evoluiu para identificar aqueles que praticam atos eletrônicos ilícitos. Crime de informática ou crime eletrônico é qualquer conduta ilegal, não ética ou não autorizada, que envolva processamento automático e/ou transmissão de dados, de acordo com a Organização para a Cooperação Econômica e Desenvolvimento).

Além disso, podemos encontrar na literatura específica outras importantes definições:

Hacker (fuçador, em inglês) é aquele que, através de sua grande habilidade técnica específica em sistemas informatizados, procura invadir máquinas ou servidores de terceiros com a finalidade, a princípio, de demonstrar a vulnerabilidade do sistema e sua capacidade de invadi-lo. Nem sempre o objetivo é a obtenção de informações.

Cracker (pirata virtual) é o especialista, tal como o *hacker* acima mencionado, mas cujo objetivo não é apenas "vencer" o sistema, mas, sobretudo, adulterar programas, dados, furtar informações, valores ou praticar outros ilícitos.

Carder é aquele que se apropria de informações de cartões de créditos obtidos através da invasão de sistemas em sites de compras pela internet, por meio da instalação de programas espiões.

Cyberterrorista é aquele que desenvolve vírus e sistemas de computador chamados de "bombas lógicas", com a finalidade de sabotar computadores e sistemas, provocando queda do mesmo e prejuízos aos seus usuários.

. Lei nº 12.737/2012 - "Lei Carolina Dieckmann"

No contexto desse cenário de vulnerabilidade, foi a grande repercussão do caso da atriz Carolina Dieckmann, que, em 2011, tornou-se mais uma vítima de crime cometido por meio da internet, o que acelerou o processo legislativo sobre o tema.

O aumento da cobrança sobre o Poder Legislativo para a criação de normas de maior efetividade culminou, então, na promulgação das Leis nº 12.735 e nº 12.737, ambas em 30 de novembro de 2012. Em razão de sua maior relevância, trataremos primeiramente da Lei nº 12.737/2012.

A Lei nº 12.737/2012 acresce ao Código Penal os artigos 154-A e 154-B. O artigo 154-A tipifica como crime a invasão de dispositivo informático alheio, "conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita".

Pela redação acima apresentada, entendem-se tipificadas as condutas de instalação de quaisquer sistemas, como vírus, Cavalos de Tróia, ou controle remoto de *webcam*, com a finalidade de extorsão, por exemplo.

Pode-se entender, contudo, que o acesso não autorizado a dispositivo informático só será criminoso se realizado mediante violação indevida de senha ou algum outro dispositivo de segurança, de forma que a invasão a dispositivo desprotegido tornaria, em tese, a conduta atípica e não punível, gerando questionamentos sobre a possibilidade de lacunas terem sido deixadas pela lei mencionada.

O parágrafo 1º do artigo 154-A inclui também como sujeito ativo deste crime aquele que "produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida" acima.

O parágrafo 2º aumenta a pena até um terço para os crimes que tenham como resultado prejuízo econômico, enquanto que o parágrafo 3º considera crime se da invasão do sistema resultar obtenção de comunicações eletrônicas privadas, sigilosas, segredos comerciais ou industriais, aumentando-se a pena em até 2/3, conforme parágrafo 4º, se houver a divulgação a terceiros dos dados obtidos. Por fim, o parágrafo 5º também aumenta a pena até metade se o crime for cometido contra determinados funcionários da Administração Pública que, pela importância de seus cargos, tenham sua vulnerabilidade tratada diferenciadamente.

A lei também altera a redação dos artigos 266 e 298 do Código Penal, incluindo as condutas de interrupção ou perturbação de serviço telemático ou de informação de utilidade pública e falsificação de cartões de crédito ou débito, crimes cuja incidência por meio da internet tem aumentado constantemente nos últimos anos.

4. Lei nº 12.735/2012

Essa lei, cuja visibilidade foi consideravelmente menor, introduziu a obrigatoriedade dos órgãos da polícia judiciária de estruturar, nos

termos de regulamento, setores e equipes especializados nos meios eletrônicos e de informática.

Já podemos encontrar essas Delegacias Especializadas em Crimes Eletrônicos em alguns dos principais centros urbanos do País, quais sejam, São Paulo, Rio de Janeiro, Belo Horizonte, Curitiba e Brasília, provendo atendimento mais direcionado às especificidades dos meios utilizados para prática desses crimes.

Além disso, a Lei também inseriu, no artigo 20, parágrafo 3º, II, da Lei nº 7.716/1989, que a discriminação ou preconceito incitados por quaisquer meios deverão ter suas transmissões interrompidas, ampliando o objeto do dispositivo que antes se limitava à transmissões radiofônicas ou televisivas.

Nesse aspecto, novamente cabe questionar se não seria o caso de simplesmente alterar-se a legislação para incluir todos os meios de comunicação possíveis e não apenas radiofônicos ou televisivos. Alterando-se a legislação para abranger todas as formas de comunicação possíveis, caso surja em 10 anos, por exemplo, outra forma ainda não imaginada de comunicação, esta já estaria abrangida pela definição e não seria necessário, em tese, criar outra lei.

5. Classificação dos crimes eletrônicos

Podemos classificar os crimes de informática como próprios ou impróprios (FERREIRA e JÚNIOR, 2010).

Denominam-se crimes próprios de informática aqueles que só podem ser praticados utilizando-se da tecnologia da informação.

São eles, por exemplo, os crimes de invasão não autorizada a um dispositivo computadorizado, previsto na Lei nº 12.737/2012; a alteração ou destruição de dados nestes dispositivos; permissão ou facilitação, por funcionário público, do acesso a sistemas e dados da Administração Pública a terceiros não autorizados, entre outros, cuja prática só é possível no mundo digital.

Já os crimes impróprios de informática são condutas que já existem no mundo físico, mas que podem igualmente ser praticadas na esfera virtual.

Exemplos dessa classe de crimes são: a pirataria de *software*, que consiste na cópia indevida de programas de computador e passível de sanção, de acordo com a Lei de *Software* (Lei nº 9.609/1998); a corrupção de menores por meios eletrônicos, inclusive por meio de salas de bate-papos – conduta que se tornou expressamente punível pela inclusão ao Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) do artigo 244-B; a invasão de privacidade, já que a Constituição Federal protege o direito à intimidade e à vida privada; o furto ou roubo de dados e informações acessados, o que já pressupõe a violação da privacidade, punível pela Lei nº 12.737/2012, entre diversas outras condutas praticáveis no mundo virtual, mas dele independentes.

6. A questão da privacidade de dados

A coleta indevida e o mau uso de dados ferem a garantia constitucional do sigilo de dados e o direito à intimidade. O mundo virtual tem possibilitado a coleta indevida de dados de terceiros, os quais são armazenados e distribuídos de forma rápida e simples pela internet.

Nelson NERY afirma que a defesa da privacidade deve proteger a pessoa contra: (i) a interferência em sua vida privada, familiar e doméstica; (ii) a ingerência em sua integridade física ou mental ou em sua liberdade intelectual e moral; (iii) os ataques à sua honra e reputação; (iv) a comunicação de fatos relevantes e embaraçosos relativos à sua intimidade; (v) o uso de seu nome, identidade e foto, (vi) a espionagem e a espreita; (vii) a intervenção na correspondência, dentre outros.

7. Norma de referência da privacidade online

Essa norma, editada em junho de 2000, foi elaborada visando estabelecer princípios éticos que devem ser seguidos por aqueles que atuam na internet. O objetivo principal é proteger as informações pessoais identificáveis dos usuários.

Tal norma foi elaborada pela Fundação Carlos Alberto Vanzolini com base no direito pátrio e internacional referente à proteção à privacidade, além de princípios gerais sobre privacidade *online* publicados pelo Conselho Europeu, OECD, dentre outros.

São consideradas informações pessoais identificáveis, dados de contato, dados de cobrança ou financeiros, documentos de identidade e profissionais, informações sócio-demográficas, dados médicos, escolaridade, imagens da pessoa, *hobbies*, área de interesse social, entretenimento, troca de mensagem em programas de conversas, listas de discussão, etc.

8. Relacionamento provedores x usuários

A mais clara relação jurídica existente na internet é aquela entre os usuários e os provedores. Segundo MIRAGEM,[4] estes provedores podem ser de três espécies distintas:

(a) os provedores de conteúdo, caracterizados como autores, editores ou outros titulares de direito que apresentam seu trabalho na rede, estando sujeitos à proteção, em conjunto com as empresas de *software*, das normas relativas aos diretos autorais;

(b) os provedores de serviços, identificados tanto com os provedores de acesso, que contratam e oferecem o meio de acesso à internet, quanto também os provedores de serviços e conteúdos que oferecem no ambiente da internet conteúdos a serem acessados ou prestam serviços a serem fruídos por intermédio da internet ou a partir desta, desenvolvendo-se ou concluindo-se o serviço fora da rede de computadores, pelo oferecimento de produto ou execução de serviço; e por fim,

(c) os provedores de rede, quais sejam, aqueles que fornecem a infraestrutura física de acesso, ou seja, as linhas de comunicação

4. MIRAGEM, Bruno. Responsabilidade por danos na sociedade de informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. *Revista de Direito do Consumidor*, vol. 70, p. 49, abril de 2009.

que permitem a conexão à internet, tais como as companhias telefônicas ou as empresas de serviços via cabo." (grifamos)

Pela maneira como a relação entre os provedores e usuários se desenvolve, percebemos uma caracterização da relação jurídica como de natureza consumerista, posto que os provedores assumem, na maior parte dos casos, posição de prestadores ou fornecedores de algum serviço ou produto, direta ou indiretamente. Dessa forma, os provedores de internet são responsáveis como fornecedores de produtos e prestadores de serviços, aos quais se aplicam as normas do Código de Defesa do Consumidor.

Em muitos outros casos, porém, sendo a internet um meio que permite ampla liberdade de comunicação e divulgação de conteúdos imateriais que nem sempre visam a obtenção de lucro, a relação é mais bem caracterizada como de natureza civil. Desta maneira, a responsabilização dos provedores pela reparação de possíveis danos causados dependerá tanto da caracterização de ato ilícito, conforme os artigos 186 ou 187 do Código Civil, ou da habitualidade com que exerce atividade que coloca em risco direitos alheios, configurando o parágrafo único do artigo 927, também do Código Civil.

9. Ciberterrorismo

O terrorismo tradicional é conduta praticada historicamente por diversos povos, pelas mais variadas motivações. É ingrata a tarefa de buscar a definição exata de quais condutas caracterizam esta prática, e se ela deve necessariamente possuir cunho político, como forma de questionamento e desmoralização do poder vigente, ou se pode ser baseada, por exemplo, em honra, moral ou religião.

A essência dessa prática se esclarece no mote utilizado por Sun TZU: "mate um, amedronte dez mil".[5] Isto porque o terrorismo não é um crime que possua a finalidade em si mesmo, mas em demonstração de poder através da violência e do medo gerados pelo dano efetivamente causado, sendo apenas a maneira escolhida para transmitir a ideia de poder e intimidação. É por esta razão – ser instrumento questionador do poder – que é quase inseparavelmente atrelado às causas políticas e sociais.

O ciberterrorismo tem sua base na dependência dos indivíduos do mundo virtual, internacionalmente, para a prática de atos de sua vida privada e, sobretudo, de seus negócios. As mesmas características do terrorismo tradicional se mantêm em sua versão cibernética, com a diferença de que esta corre primariamente nos sistemas binários virtuais, para depois afetar o mundo físico. Temos como exemplo de ações de ciberterrorismo a invasão de um sistema de controle alimentício para adulterar sua qualidade, ou acesso ao controle remoto do tráfego aéreo viando causar acidentes de grandes proporções.

É importante diferenciar o ciberterrorista do *hacker*: o primeiro tem as motivações que vimos acima, enquanto o último, utilizando-se de vasto conhecimento em tecnologia da informação, pratica atos inofensivos ou perpetra crimes comuns, sem considerar a finalidade política de protesto.

5. TZU, Sun. A arte da guerra. São Paulo: Códice, p. 45, 1995.

10. Conclusão

O arcabouço penal e processual atual certamente não retrata a evolução dos meios tecnológicos, o avanço dos sistemas computadorizados e da internet. Nesse sentido, é inquestionável que algumas inclusões na legislação são necessárias de forma a contemplar os inúmeros ilícitos penais e condutas lesivas praticadas nesse meio e utilizando tais dispositivos.

No entanto, é importante o exercício de se analisar exatamente quais são as alterações imprescindíveis na legislação para albergar a investigação e a punição de tais práticas, a fim de não se criarem leis repetitivas, contraditórias ou até mesmo redundantes.

Como vimos, os crimes eletrônicos próprios são aqueles que só existem com a participação do meio digital, como, por exemplo, o acesso a sistema alheio para furtar ou danificar dados ou informações. Nessa situação, efetivamente era necessária a criação de legislação específica.

Por outro lado, os crimes contra a honra podem ser praticados com ou sem a participação dos sistemas virtuais. Entendemos que nesses casos a criação de legislação nova seria redundante, pois a única novidade é o meio utilizado para a prática do delito, o que, salvo melhor juízo, não carece de regulamentação própria.

Por fim, acreditamos que a legislação existente é suficiente para garantir a punição das condutas criminosas eletrônicas, bastando apenas um exercício mais atento de interpretação da legislação já existente pelo Poder Judiciário.

Referências bibliográficas

DE BARROS, Marco Antonio; GARBOSSA, Daniela D'Arco; CONTE, Christiany Pegorari. Crimes informáticos e a proposição legislativa: considerações para uma reflexão preliminar. *Revista dos Tribunais*, vol. 865, p. 399, novembro de 2007.

FERREIRA, Lóren Formiga de Pinto; JÚNIOR, José Carlos Macedo de Pinto Ferreira. Os "crimes de informática" e seu enquadramento no direito penal pátrio. *Revista dos Tribunais*, vol. 893, p. 407, março de 2010LEITE FILHO, Jaime de Carvalho. Ciberterrorismo – o terrorismo na era da informação, p. 41. In ROVER, Aires José. *Direito e Informática*. São Paulo: Editora Manole, 2004.

MIRAGEM, Bruno. Responsabilidade por danos na sociedade de informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. *Revista de Direito do Consumidor*, vol. 70, p. 41, abril de 2009.

NERY JUNIOR, Nelson; NERY, Rosa Maria de Andrade. Constituição Federal comentada e legislação constitucional. São Paulo: Ed. RT, 2006.

ZANELLATO, Marco Antonio. Revista de Direito do Consumidor, vol. 44, p. 206, outubro de 2002.

Delegacias Especializadas em crimes virtuais. Jurisway, Belo Horizonte. Disponível em [http://www.jurisway.org.br/v2/dropsjornal.asp?pagina=&idarea=&iddrops=391]. Acesso em 22/07/2013.

Lei Carolina Dieckmann entra em vigor, entenda. INFO online, São Paulo, 03/04/2013. Disponível em [http://info.abril.com.br/noticias/seguranca/lei-carolina-dieckmann-entra-em-vigor-entenda-03042013-33.shl]. Acesso em 22/07/2013.