DELITOS CIBERNÉTICOS: IMPLICAÇÕES DA LEI Nº 12.737/12

Wanderlei José dos Reis[1]

Resumo: O presente estudo se propõe a demonstrar que a alteração da legislação penal para a tipificação dos crimes cometidos via internet, que se deu com o advento da Lei nº 12.737/12, veio ao encontro das necessidades sociais, principalmente para coibir práticas delituosas nesse ambiente que visam, de alguma forma, auferir vantagem indevida, causando intranquilidade social.

Abstract: This study aims to demonstrate that the change of criminal law for the definition of crimes committed via the Internet, which occurred with the enactment of LawNo.12.737/12, came to meet social needs, especially to curb criminal activities in this environment that aim, somehow, obtaining unfair advantage, causing social unrest.

Palavras-Chave: Direito Penal – Internet – Delitos cibernéticos – Legislador.

Sumário: I – Considerações Iniciais II – Análise do Tema III – Considerações Finais IV – Referências.

[1] Juiz de Direito em Mato Grosso e Ex-Delegado de Polícia. Mestrando em Direito Constitucional pela Universidade Clássica de Lisboa. MBA em Poder Judiciário pela FGV Rio. Escritor. Professor. Palestrante. Conferencista. Doutrinador. Graduado em Matemática (com ênfase em informática). Especialista em Educação, em Direito Constitucional, em Direito Público Avançado e em Direito Processual Civil Avançado. Especializando em Direito Internacional. Autor de inúmeras obras e artigos jurídicos publicados em revistas especializadas. Membro Vitalício da Academia Mato-grossense de Letras (AML) e da Academia Mato-grossense de Magistrados (AMA). Atua como Juiz Titular da 1ª Vara Especializada de Família e Sucessões e Juiz Titular da 46ª Zona Eleitoral em Rondonópolis/MT.

I. CONSIDERAÇÕES INICIAIS

Consabido que o Direito Penal ostenta um caráter dúplice: servir à sociedade, protegendo-a de condutas danosas de seus membros; e servir às pessoas, limitando a atuação punitiva estatal – o *jus puniendi*. A interface entre suas duas utilidades, igualmente calcadas na Constituição, é que lhe dá o perfil, não sendo o Direito Penal um fim em si mesmo.

Neste sentido, cabe ao Direito Penal a proteção dos bens jurídicos mais relevantes para o meio social, ou seja, este ramo do ordenamento jurídico tutela o que é basilar para a própria existência da sociedade, que é o direito à vida; a liberdade; o patrimônio; a propriedade imaterial; a organização do trabalho; o sentimento religioso e o respeito aos mortos; a honra, imagem e privacidade; a dignidade sexual; a família; a incolumidade pública; a paz pública; a fé pública; a Administração Pública; o meio ambiente e tantos outros bens.

Por este viés, observa-se que a concepção de bem jurídico deve estar atrelada aos valores da realidade social que, em um dado momento histórico-cultural, é alterada, principalmente quando há uma ruptura com o modelo social até então existente. Assim, a partir dos anos 90, do século passado, com a disseminação da internet, ocorreu o que se conhece como "revolução digital".

No Brasil, a popularização da internet originou-se no final da década de 90 e início do século XXI. Segundo dados do Ibope, no ano de 2002, o Brasil contava com 7,68 milhões de usuários, contudo, com base na última pesquisa realizada por este Instituto, em 2013, tem-se que atualmente o País já conta com mais de 102,3 milhões de usuários.

Cumpre esclarecer que a internet é um conjunto de redes de computadores ligados entre si através de roteadores e

gateways, cujo principal objetivo é transmitir informações diminuindo as distâncias e dissipando as fronteiras traçadas pela geografia.

Nota-se que a internet instituiu um processo de globalização e diminuição das distâncias. Fatos e culturas que muitas vezes eram restritas a determinadas regiões ganham uma notoriedade mundial e se tornam relevantes. Essa onda digital de informações trouxe a possibilidade de armazenamento de dados industriais e individuais, dados relativos a contas bancárias, números de cartões de crédito, senhas de acesso, trocas de experiências interpessoais, criação e difusão do comércio eletrônico e, consequentemente, certo comodismo.

Neste passo, o mundo moderno requer do Direito um acompanhamento atento às mudanças e transformações ocorridas no seio da sociedade, notadamente no que atine ao ramo da informática, que se encontra em franco desenvolvimento. Por sua vez, por conta desses avanços tecnológicos, a internet se tornou um campo propício para a prática de novos delitos, principalmente ligados à honra, cabendo destacar que essas condutas já se amoldam aos delitos existentes previstos no Capítulo V do Título I da Parte Especial do Código Penal, quais sejam, calúnia, injúria e difamação.

Por outro lado, há certas situações em que o agente utiliza o dispositivo de informática para obter algum tipo de vantagem, ou seja, nestes casos, o aparelho digital não é o meio para o cometimento da infração e, sim, o objeto desta.

Pode-se exemplificar a prática com o caso da atriz global Carolina Dieckmann, que, em maio de 2012, teve seu e-mail invadido por *crackers*[2]. Eles se apropriaram de fotos íntimas da atriz e este conteúdo foi divulgado na internet, após a

[2] A distinção entre *crackers* e *hackers* é a de que estes são compulsivos estudiosos e pesquisadores que agem movidos pelo afã do saber, enquanto que aqueles agem pelo sentimento de destruição e da obtenção de ganhos ilícitos. (VALLE, Regina Ribeiro do. *E-Dicas: o direito na sociedade da informação*. São Paulo: Usina do Livro, 2005, p. 159.)

atriz não ceder às chantagens dos criminosos, que pediam dez mil reais pela não publicação das imagens.

Com efeito, até então, não havia em nosso ordenamento jurídico a tipificação de crimes cometidos via internet, o que obrigava o magistrado a se utilizar da analogia para aplicar a legislação que versava sobre condutas semelhantes já tipificadas. Assim, a violação de e-mail era enquadrada como crime de violação de correspondência, previsto na Lei nº 6.538/78, que, em seu art. 40, estatui que é crime devassar indevidamente o conteúdo de correspondência fechada dirigida a outrem, estabelecendo a pena de detenção, de até seis meses, ou o pagamento não excedente a vinte dias-multa.

Dessa forma, o legislador editou a Lei nº 12.737, de 30 de novembro de 2012, mais conhecida como "Lei Carolina Dieckmann", que teve um período de vacância de 120 dias e entrou em vigor em 2 de abril de 2013, dispondo exatamente sobre a tipificação criminal de delitos informáticos, inserindo no Código Penal brasileiro os arts. 154-A e 154-B, no art. 266 do diploma legal dois parágrafos e, na redação do art. 298 do Estatuto Penal em vigor, o parágrafo único.

Traçadas estas premissas, mister se faz realizar uma análise crítica dos principais aspectos introduzidos pelo novo diploma criminal.

II. ANÁLISE DO TEMA

O art. 154-A, disposto no Código Penal, topograficamente, na Parte Especial, Título I – Dos Crimes Contra a Pessoa; Capítulo VI – Dos Crimes Contra a Liberdade Individual; Seção IV – Dos Crimes Contra a Inviolabilidade dos Segredos; inserido pela Lei nº 12.737/12, objetiva proteger a privacidade do indivíduo no tocante aos dados e informações pessoais ou profissionais armazenados em dispositivo de informática que, de alguma forma, teve a sua segurança violada sem a autoriza-

ção do titular. Assim, o novo diploma legal protege o dispositivo informático, visando evitar a violação deste.

Nessa esteira, estabelece o art. 154-A do Estatuto Repressivo que invadir 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 é conduta a ser apenada com detenção, de três meses a um ano, e multa.

Trata-se de um tipo penal misto que dispõe de duas condutas incriminadoras, sendo a primeira relacionada à invasão de dispositivo de informática alheio (computadores domésticos, *notebooks*, *tablets*, *smartphones*, *ipads*ou aparelhos celulares), conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança (senha, assinatura digital, chave de segurança) com o fim de obter, adulterar ou destruir dados ou informações sem a autorização expressa ou tácita do titular do dispositivo; já a segunda conduta está associada à instalação de vulnerabilidades (*softwares* maliciosos) para obter vantagem ilícita.

Observa-se que, para a caracterização das condutas dispostas no tipo penal, é fundamental o dolo e o especial fim de agir, ou seja, a obtenção, a adulteração ou a destruição de dados ou informações para a primeira conduta; e a obtenção de vantagem ilícita (não necessariamente econômica) para a segunda conduta. Ausente o especial fim de agir, o fato passará a ser um indiferente penal.

Ademais, é necessário que o dispositivo de informática disponha de mecanismo de segurança, podendo-se afirmar que a ausência de mecanismo de segurança, ou o não acionamento deste, impede a configuração do tipo penal.

Contudo, é de se perquirir, neste caso, se o dispositivo de informática desprovido de algum mecanismo de segurança

também encontra proteção jurídica na nova Lei, haja vista que o legislador infraconstitucional se referiu expressamente àqueles aparelhos digitais que contenham antivírus, *firewall*, senhas e outras defesas digitais.

De outra banda, a redação do *caput* do dispositivo foi duramente criticada no seio doutrinário, tendo em vista que o verbo nuclear do art. 154-A, qual seja, "invadir", exprime, consoante a definição do *Dicionário Aurélio*, o ato de "entrar à força, apoderar-se violentamente", e, a julgar pela redação do novel artigo, somente se configuraria o crime se o agente acessasse o sistema de informática à força.

Ocorre que a prática desses ilícitos que o art. 154-A pretende coibir, em sua maior parte, não se dá de forma casual, mas somente com o agir do agente mal-intencionado, pois só há dois meios de se ter acesso a banco de dados de forma indevida: quando o agente acessa fisicamente o dispositivo ou quando o usuário, de forma inadvertida, permite que sejam instalados em seu computador os chamados *malwares*, que aparecem na forma de arquivos enviados por e-mail, *links* na internet ou em dispositivos móveis como *pendrives*, o que permite concluir que, em ambos os casos, o agente não agiu com violência, mas tão somente com o emprego de ardil para a obtenção de dados. A solução legal teria sido substituir o verbo "invadir" por "acessar", e exigiria mais esclarecimentos do legislador sobre o que são os *malwares.*

Portanto, com relação ao *caput* do art. 154-A, pode-se concluir que se trata de crime comum, comissivo, instantâneo, formal, unissubjetivo, plurissubsistente e doloso.

No que toca ao seu § 1º, objetivou o legislador equiparar a conduta do agente que produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador àquela tipificada no *caput*. Buscou-se sancionar, desta forma, a conduta daquele agente que desenvolve, difunde, distribui de forma gratuita ou onerosa o *software* malicioso.

O § 2º do art. 154-A majorou a pena base do delito de 1/6 a 1/3, se a invasão ao equipamento informático causar prejuízo econômico à vítima, ou seja, a Lei sanciona de modo mais severo quando a invasão atingir a esfera patrimonial.

Já o § 3º do art. 154-A dispõe que, se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em Lei, ou o controle remoto não autorizado do dispositivo invadido, a pena-base será a de reclusão, de seis meses a dois anos, e multa, se a conduta não constituir crime mais grave.

Observa-se que o intuito do legislador foi o de punir de forma mais eficaz o agente que consegue controlar de forma remota o dispositivo informático, bem como obtenha conteúdo de comunicação eletrônica privada, segredo comercial ou industrial e informações sigilosas e, neste ponto, é importante destacar que se mostra irrelevante que venha se tratar de segredo temporário.

O § 4º, por sua vez, prevê causa de aumento de pena aplicável na hipótese em que as informações obtidas por intermédio das ações previstas no § 3º forem divulgadas, comercializadas ou transmitidas a terceiros.

Importante inovação é disposta no § 5º, que estabelece o aumento de pena de 1/3 à metade se o crime for praticado contra: (i) o Presidente da República, governadores e prefeitos; (ii) Presidente do Supremo Tribunal Federal; (iii) Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa do Estado, da Câmara Legislativa do Distrito Federal ou da Câmara Municipal; ou (iv) dirigente máximo da Administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

De outro turno, a Lei nº 12.737/12 também estabeleceu, no art. 154-B do Código Penal, que os crimes previstos no seu art. 154-A somente se procederão mediante representação, ex-

ceto às hipóteses em que a prática delituosa se efetivar contra a Administração Pública direta ou indireta de qualquer dos Poderes da União, Estados, Municípios e Distrito Federal ou contra empresas concessionárias de serviços públicos.

Por oportuno, a Lei dos Crimes Cibernéticos ampliou a redação do art. 266 do *Codex* Penal, etiquetado no Título VIII – Dos Crimes Contra a Incolumidade Pública, que passou a versar sobre a interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.

Esta alteração feita no *caput* do art. 266 se justifica com a inserção do § 1º, que aduz que incorre na mesma pena do *caput* quem interromper serviço telemático ou de informação de utilidade pública, ou impedir ou dificultar o restabelecimento. Entende-se como serviço telemático a junção dos serviços de telecomunicações e informática, ou seja, é o serviço prestado por operadoras para a transmissão de informações digitais; já os serviços de informação de utilidade pública são aqueles dispostos ao cidadão através da telefonia, informática, telemática e telegrafia.

Trata-se de um tipo penal que visa proteger a incolumidade pública no que tange à regularidade dos serviços telegráficos, telefônicos, informáticos, telemáticos e de utilidade pública. É um delito comum que admite a tentativa, cuja pena possibilita a suspensão condicional do processo, desde que o delito não seja cometido por ocasião de calamidade pública (art. 266, § 2º).

De outro giro, o diploma legal em comento acrescentou também o parágrafo único ao art. 298 do Código Penal, o qual equiparou o cartão de crédito ou débito a documento particular. A nova redação, ao equiparar o cartão magnético bancário, seja ele de débito ou crédito, a documento particular, revela-se de um avanço significativo, cujo objetivo foi evitar danos patrimoniais causados pelo uso indevido das novas tecnologias.

Por fim, não é de se olvidar que a Lei nº 12.737/12, que se propunha a alterar o Código Penal, o Código Penal Militar e a Lei nº 7.716/89, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares praticadas contra sistemas informatizados e similares, e acabou sendo parcialmente vetada, ainda quando em estágio embrionário, no Congresso Nacional (PLC nº 89/03), foi duramente vergastada, conforme se depreende do Parecer emitido pelo Instituto dos Advogados Brasileiros, de onde se extrai que a grande dificuldade na construção dos tipos relativos aos crimes informáticos repousa na intangibilidade do seu objeto. Daí alguns doutrinadores identificarem que, nos delitos praticados com o uso do sistema informático, se teria como bem jurídico a informação, a inviolabilidade de dados informáticos ou, até mesmo, a capacidade funcional dos sistemas informáticos.

No próprio Parecer ofertado no âmbito da Comissão de Constituição e Justiça da Câmara dos Deputados – confundindo crimes informativos próprios e impróprios – há a noção de que os bens jurídicos tutelados pelos tipos penais são os "originais" e a "segurança informática", cujos requisitos seriam a integridade, a disponibilidade e confidencialidade, contemplados na Constituição de Budapeste.

III. CONSIDERAÇÕES FINAIS

Conforme restou plasmado em linhas transatas, a internet constituiu um grande avanço para a sociedade, se tornando ferramenta de fundamental importância para a quebra de paradigmas e fronteiras, principalmente no que diz respeito ao acesso à cultura, à informação, à livre manifestação, bem como para a prática de negócios jurídicos, como compra e venda, transações bancárias, anúncios etc.

Na esteira desta ascensão tecnológica, surgiram também as práticas delituosas levadas a efeito pela rede mundial de

computadores, sendo nesta vertente que o Direito veio atuar, com o nítido intuito de erigir barreira contra a criminalidade virtual.

Notório que a legislação brasileira era ineficiente para penalizar as condutas praticadas através de dispositivos de informática, daí o advento da Lei nº 12.737/12, que passou a coibir, na seara penal, a prática de infrações cometidas em ambiente virtual.

Não obstante a boa intenção do legislador, alguns dispositivos da nova Lei pecam em sua qualidade técnica, em especial na redação dada ao art. 154-A da Lei Substantiva Penal, por ter em seu verbo nuclear a expressão "invadir", que significa entrar à força, o que não se coaduna com o *modus operandi* da maior parte dos delitos cibernéticos, nos quais o agente se utiliza do ardil para alcançar o seu desiderato criminoso.

Assim, o legislador brasileiro, em que pese certa demora no processo legislativo, agiu bem e de forma oportuna ao tipificar os delitos informáticos, representando a Lei nº 12.737/12 um avanço legislativo pátrio que veio ao encontro do anseio social de evolução tecnológica, já que a tutela cibernética criou um novo bem jurídico, o dispositivo informático.

IV. REFERÊNCIAS

CASTRO, Luiz Augusto Sartori de. "Lei Carolina Dieckmann" seria salvação da internet? *Migalhas.* Disponível em: <http://www.migalhas.com.br/dePeso/16,MI167980,81042-

Lei+Carolina+Dieckmann+seria+a+salvacao+da+internet>. Acesso em: 14.08.13.

GOMES, Luiz Flávio. Lei "Carolina Dieckmann" e sua (in)eficácia. *Jus Navigandi*, Teresina, ano 18, nº 3.536, 07.03.13. Disponível em: <http://jus.com.br/revista/texto/23897>. Acesso em: 15.04.13.

ISHIDA, VálterKenji. As modificações promovidas pela Lei Carolina Dieckmann no Código Penal. *Carta Forense*. Disponível em: <http://www.cartaforense.com.br/conteudo/artigos/as-modificacoes-promovidas-pela-lei-carolina-dieckmann-no-codigo-penal/9986>. Acesso em: 14.04.13.

MANZEPPI, Eduardo. Lei Carolina Dieckmann – Brasil entra na Era Digital. *Midiajur*. Disponível em: <http://www.midiajur.com.br/conteudo.php?cid=9247&sid=240>. Acesso em: 14.04.13.

OLIVEIRA JÚNIOR, Eudes Quintino de. A nova Lei Carolina Dieckmann. *Migalhas*. Disponível em: <http://www.migalhas.com.br/dePeso/16,MI169227,21048-A+nova+lei+Carolina+Dieckmann>. Acesso em: 14.08.13.

OLIVEIRA, Jane Resina F. de. Lei Carolina Dieckmann: antes tarde do que nunca. *Migalhas*. Disponível em: <http://www.migalhas.com.br/dePeso/16,MI169090,41046-Lei+Carolina+Dieckmann+antes+tarde+do+que+nunca>. Acesso em: 15.08.13.

SOBRAL, Carlos. *Considerações sobre a Lei Carolina Dieckmann*. SINDPF-RJ. Disponível em: <http://sindpfrj.blogspot.com.br/2013/02/consideracoes-sobre-lei-carilina.html>. Acesso em: 15.04.13.

VALLE, Regina Ribeiro do. *E-Dicas: o direito na sociedade da informação*. São Paulo: Usina do Livro, 2005.

VIEIRA, Victor. Lei Carolina Dieckmann enfrentará dificuldades na prática. *Conjur*. Disponível em: <http://www.conjur.com.br/2013-abr-03/aplicacao-lei-carolina-dieckmann-enfrentara-dificuldades-tribunais>. Acesso em: 14.04.13.