Escola da Magistratura do Estado do Rio de Janeiro

Lei n. 12.737: a nova tipificação criminal de delitos informáticos

Juliana Motta de Barros

Rio de Janeiro
2015

JULIANA MOTTA DE BARROS

Lei n. 12.737: a nova tipificação criminal de delitos informáticos

Artigo Científico apresentado à Escola de Magistratura do Estado do Rio de Janeiro, como exigência para obtenção do título de Pós-graduação
Orientadores:
Profª. Mônica Areal
Profª. Néli Fetzner
Prof. Nelson Tavares

Rio de Janeiro
2015

LEI N. 12.737: A NOVA TIPIFICAÇÃO CRIMINAL DE DELITOS INFORMÁTICOS

Juliana Motta de Barros

Graduada pela Faculdade de Direito da Universidade do Estado do Rio de Janeiro. Advogada.

Resumo: O delito de invasão de dispositivo informático é preceito recente introduzido pelo legislador pela Lei n. 12.737/2012. Será explicitado na pesquisa a aplicação do novo art. 154-A do Código Penal, bem como as lacunas normativas e falhas na redação dos tipos penais. Por fim, debate-se os demais crimes cometidos no meio virtual, que apresentam maior vulnerabilidade da vítima. A pesquisa, portanto, visa a esclarecer o tema dos crimes virtuais próprios e impróprios, tão em evidência atualmente, sugerindo o que pode ser feito para melhor atuação no âmbito do direito penal e fora dele.

Palavras-chave: Direito Penal. Crimes Virtuais. Lei n.12.737.

INTRODUÇÃO

O trabalho enfoca a Lei n. 12.737/2012, especialmente o art. 154-A, CP, analisando a questão dos crimes virtuais próprios, com toda a problemática da nova redação e o que ainda deixou de ser tratado pela nova lei.

O mundo virtual ganha suma importância nos tempos atuais. As pessoas estão permanentemente conectadas a computadores, celulares, *tablets*, dentre outros dispositivos informáticos, muitas vezes por meio de uso da Internet.

Com o crescimento da cibernética, surgem também os crimes virtuais. Esses crimes podem ser de dois tipos: os próprios e os impróprios. Os crimes virtuais impróprios já estão tipificados no Código Penal e ganham um novo instrumento para a sua prática. Eles são, por exemplo, o furto mediante fraude praticado contra o cliente de agência bancária ao capturar

sua senha, a injúria praticada constantemente nas redes sociais.

Os crimes virtuais próprios são aqueles cometidos contra dispositivos informáticos. Esses eram impuníveis até o surgimento da Lei n. 12.737/2012. Antes da introdução do art. 154-A no Código Penal, não tínha-se como tipificar a invasão de um computador, de um celular, de um *tablet*, e a destruição de seu conteúdo.

Assim, a nova lei surgiu de anseios sociais cada vez mais urgentes. A prática dos delitos informáticos é recorrente, diária, e precisava o legislador de uma solução para o problema.

Inicia-se o primeiro capítulo com a análise da aplicação do art. 154-A do Código Penal e quais os limites de sua proteção no âmbito dos crimes virtuais. Classifica-se o novo delito, demonstra-se seus especiais fins de agir, e que o art. 154-A, do CP, limita-se aos casos específicos de invasão de dispositivos informáticos, ou seja, uma tipificação de crime virtual próprio.

Ainda, no segundo capítulo, a análise passará às possíveis obscuridades, falhas e omissões na tipificação do delito de invasão de dispositivo informático. Assim, será possível verificar as falhas na tipificação do artigo, que deixa de proteger os dispositivos informáticos sem mecanismos de segurança ou que não estejam em funcionamento, como se não merecessem proteção. Ademais, com a redação do dispositivo há necessidade de fim especial de agir, pois não se pune a simples invasão. Desse modo, pode-se destacar hipóteses não abrangidas pelo tipo penal.

Por fim, no último capítulo, considerando que os crimes virtuais são crescentes hoje em dia, será abordado se há necessidade de uma nova legislação para tais crimes virtuais próprios. Ademais, se deve haver um novo enfoque quanto aos crimes virtuais impróprios. Procura-se defender a solução por outros ramos do direito, como o direito civil, além de por meio dos crimes já existentes no Código Penal.

A pesquisa utilizará a metodologia do tipo bibliográfica, parcialmente exploratória e qualitativa.

1. ANÁLISE DA LEI N. 12.737 E INTRODUÇÃO DO ART. 154-A, CP

A Lei n. 12.737/2012 veio superar uma lacuna normativa a respeito dos crimes virtuais próprios[1]. A lei equipara à falsificação de documento particular a falsificação de cartões de crédito e débito, no art. 298, CP, importante equiparação no mundo atual em que grande parte dos pagamentos são feitos de tal forma. Além disso, introduz a interrupção de serviço telemático ou de informação de utilidade pública no art. 266, CP, também importante no mundo atual.

Entretanto, a principal inovação da lei foi a introdução do art. 154-A e 154-B no Código Penal. Para iniciar o estudo desse delito, deve-se transcrever o primeiro[2]:

> Art. 154-A. 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:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º 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:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

1 A Lei n. 12.737/2012 é frequentemente apelidada de "Lei Carolina Dieckmann". A Lei surgiu após o vazamento de fotos íntimas da atriz de seu computador pessoal, mas já havia projetos de lei para que fosse definido o crime de invasão de dispositivo informático. A opinião pública, porém, impulsionou a aprovação do projeto. Nesse sentido: MASSON, Cleber. *Direito Penal esquematizado*: parte especial. v. 2. 6. ed. Rio de Janeiro: Forense; São Paulo: Método, 2014., p. 310.

2 BRASIL. Código Penal. Decreto-lei 2848/1940. Disponível em: <htttp://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 11 mar. de 2015.

> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

O delito está inserido no capítulo "dos crimes contra a liberdade individual", especialmente na seção "dos crimes contra a inviolabilidade dos segredos". Segundo Cezar Roberto Bitencourt[3], a proteção que o dispositivo busca é da privacidade individual, e não da rede mundial de computadores. Para Fernando Capez[4], a parte final do dispositivo tutela também o patrimônio do titular do dispositivo, porque pune quem procura obter vantagem ilícita.

O objeto material do crime é o dispositivo informático alheio. Se o dispositivo é próprio, o fato é atípico. Outra elementar típica importante de se destacar é: "sem autorização expressa ou tácita do titular do dispositivo". Assim, se o proprietário autoriza a invasão, o fato também se torna atípico, e o consentimento do ofendido aqui será uma excludente da tipicidade.

O crime do art. 154-A, *caput* é um crime comum no aspecto do sujeito ativo, ou seja, qualquer um poderá praticá-lo. No âmbito do sujeito passivo também, qualquer pessoa, inclusive jurídica, poderá ser vítima do crime de violação de dispositivo informático.

Há uma certa discussão na doutrina acerca dos núcleos do tipo. Para Guilherme de Souza Nucci[5], o *caput* do dispositivo prevê duas condutas, "invadir" e "instalar", mas se o agente pratica ambas as condutas, o crime será único. Já Rogério Greco[6] e Cezar Roberto

3 BITENCOURT, Cezar Roberto. *Código Penal comentado*. 8. ed. São Paulo: Saraiva, 2014. p. 679.
4 CAPEZ, Fernando. PRADO, Stela. *Código Penal comentado*, 5. ed. São Paulo: Saraiva, 2014. p. 346.
5 NUCCI, Guilherme de Souza. *Código penal comentado*: estudo integrado com processo e execução penal. 14 ed. Rio de Janeiro: Forense, 2014, p. 812/813.
6 GRECO, Rogério. *Código penal comentado*. 8. ed. Niterói, RJ: Impetus, 2014, p. 470.

Bitencourt[7] analisam apenas "invadir" como núcleo do tipo penal, e "instalar" passa a ser secundário, dentro da conduta de "invadir" um fim especial de agir, como será visto.

O crime desse artigo é doloso, pois não há sua previsão na modalidade culposa. Há também um especial fim de agir exigido no tipo, caracterizado após a locução "com o fim de". Luis Régis Prado e Cezar Roberto Bitencourt dizem tratar-se de um elemento subjetivo especial do tipo[8].

O especial fim de agir é, na verdade, alternativo, de acordo com Cezar Roberto Bitencourt[9]. Primeiramente, há a possibilidade de o agente agir com a intenção de "obter, adulterar ou destruir dados ou informações sem autorização" e depois a possibilidade de o agente "instalar vulnerabilidades para obter vantagem ilícita". Como são alternativos, apenas um deles precisa estar presente para a configuração do tipo penal. No mesmo sentido é a posição de Rogério Greco[10].

Já na visão de Fernando Capez[11], Luiz Régis Prado[12], e Guilherme de Souza Nucci[13], o tipo penal do *caput* se subdivide de outra forma. A primeira conduta seria de "invadir" o dispositivo informático com os fins que seguem, e a segunda conduta seria de "instalar vulnerabilidades" e o fim especial, nesse caso, seria "para obter vantagem ilícita".

No entanto, é importante salientar que se não estiverem presentes quaisquer dos fins especiais de agir, o fato praticado pelo agente é atípico. O legislador vinculou a prática do delito a essas finalidades, assim, devem ser demonstradas para a adequação típica e oferecimento da denúncia pelo crime de invasão de dispositivo informático.

---

7 BITENCOURT, op. cit., p. 680.
8 PRADO, Luis Regis.*Comentários ao Código Penal*: jurisprudência: conexões lógicas com os vários ramos do direito. 9. ed. São Paulo: Revista dos Tribunais, 2014, p. 595. BITENCOURT, op. cit., p. 688.
9 BITENCOURT, op. cit., p. 682-683.
10 GRECO, op. cit., p. 472.
11 CAPEZ, op.cit., p. 347.
12 PRADO, op. cit., p. 595.
13 NUCCI, op.cit., p. 813.

O crime, segundo a doutrina[14], é formal. Assim, o momento de sua consumação é o momento em que o agente invade o computador, *tablet*, ou qualquer outro dispositivo informático. O fato de obter, adulterar, destruir dados e informações ou mesmo instalar as vulnerabilidades e obter a vantagem ilícita não é relevante. O objetivo do agente não precisa ser alcançado.

No entanto, o §2º do dispositivo já prevê um aumento de pena de 1/6 a 1/3 se resultar prejuízo econômico para a vítima. Seja esse ou não o fim do agente, em ocorrendo o dano, trata-se de uma causa de aumento de pena. Como o crime é formal, ocorre mero exaurimento do delito, e o tamanho do prejuízo, para Guilherme de Souza Nucci[15], que graduará o aumento de pena.

No §1º do dispositivo, há a previsão de uma modalidade equiparada. Há também previsão de um especial fim de agir: "com o intuito de permitir a prática da conduta definida no caput". Assim, o legislador traz a punição a todo aquele que esteja ligado ao crime de violação de dispositivo informático.

Cleber Masson[16] aponta que o legislador trouxe uma exceção à teoria monista do art. 29 do Código Penal, pois quem oferta condições para a invasão do dispositivo informático alheio é punido pelo §1º do art. 154-A. Aponta Guilherme de Souza Nucci[17] que o legislador está punindo os atos preparatórios à invasão do dispositivo informático, pois essa se concretiza por meio de mecanismo que a viabiliza.

O §1º tem como sujeito ativo qualquer pessoa, sendo também crime comum. O sujeito passivo desse crime, porém, é a sociedade. Como no *caput*, esse crime também é formal. Segundo Rogério Greco[18], não há necessidade de o agente utilizar o dispositivo ou programa

14 Nesse sentido aponta-se: CAPEZ, op. cit., p. 347., GRECO, op. cit., p. 476, BITENCOURT, p. 688, dentre outros.
15 NUCCI, op. cit., p. 816.
16 MASSON, op. cit, p. 316.
17 NUCCI, op. cit., p. 814.
18 GRECO, op. cit., p. 476.

de computador, basta que o agente pratique uma das condutas previstas no tipo penal com o fim de permitir a conduta do *caput*. Atente-se que se o agente pratica as condutas do *caput*, não poderá ser punido pelo §1º também. Cezar Roberto Bitencourt[19] aponta que se o agente produz o material (§1º) e distribui, vende ou difunde (*caput*), o crime é único.

Ademais, o delito de invasão de dispositivo informático somente pode ser praticado de maneira comissiva. O tipo penal prevê condutas que são praticadas por meio de ação. No entanto, como bem aponta Rogério Greco[20], não está excluída a possibilidade de responsabilizar o agente garantidor, caso fique caracterizada uma das hipóteses do art. 13, §2º, CP. Assim, seria possível também o cometimento do delito por conduta omissiva imprópria se o agente for garante.

O §3º do dispositivo prevê uma modalidade qualificada do delito de invasão de dispositivo informático, que pode ser dividido em duas partes. A primeira parte se o agente obtém conteúdo de comunicações privadas ou segredos comerciais ou industriais, bem como informações sigilosas. Ele faz referências às "assim definidas em lei", tratando-se de norma penal em branco, complementada pelo próprio Código Penal que define os segredos e informações invioláveis (seções II e IV), segundo Luis Régis Prado[21].

Na segunda parte do §3º, o agente mantém o controle remoto do dispositivo informático por ele violado. Desse modo, o agente opera o dispositivo invadido por meio de outro computador, e como bem coloca Cezar Roberto Bitencourt[22] "o sujeito passivo fica nas mãos do autor do crime (…) O maior desvalor desta conduta reside na permanência dos efeitos nocivos da conduta do agente, que mantém sob o seu controle as ações da vítima, observando, controlando e lesando à distância os bens jurídicos tutelados desta".

19 BITENCOURT, op. cit, p. 683.
20 GRECO, op. cit., p. 476,
21 PRADO, op. cit., p. 596.
22 BITENCOURT, op. cit., p. 686.

O §4º prevê uma causa de aumento de pena que apenas se aplica ao §3º. Quis o legislador proteger tais segredos, comunicações privadas, informações sigilosas, e por isso aumenta a pena de 1/3 a 2/3 de quem divulga, transmite ou comercializa outrem, seja a título oneroso ou gratuito.

No §5º há mais uma hipótese de aumento de pena, que se aplica em qualquer caso, ou seja, ao *caput* e todos os parágrafos anteriores. Para Cezar Roberto Bitencourt, no entanto, essa causa de aumento de pena não pode ser aplicada em cascata com o §4º, caso contrário, a pena seria elevada em excesso, tornando-se desproporcional[23].

Nesse dispositivo há um aumento de pena em virtude da vítima do crime. A doutrina, como Guilherme de Souza Nucci[24], aponta que como o crime atinge determinados governantes ou autoridades, atinge também a sociedade, atinge o interesse coletivo, merecendo maior reprovação.

2. CRÍTICAS À REDAÇÃO DO DISPOSITIVO

O tipo penal exige que a conduta do agente seja de invadir o dispositivo informático "mediante a violação indevida de mecanismo de segurança". Segundo Cezar Roberto Bitencourt[25], trata-se de um "pressuposto a satisfazer" da conduta criminosa que o dispositivo informático esteja com mecanismo de segurança acionado.

Guilherme de Souza Nucci[26] aponta que se trata de um elemento normativo do tipo. O autor entende ser desnecessária a sua inclusão, e mais, aponta que é o "calcanhar de Aquiles" do tipo penal.

Essa previsão legal é uma lacuna normativa. Os dispositivos informáticos que

23 Ibid., p. 689.
24 NUCCI, op.cit., p. 817.
25 BITENCOURT, op. cit., p. 680.
26 NUCCI, op. cit., p. 813.

porventura não possuam antivírus, *antispyware*, ou outro mecanismo de segurança não estão sob a proteção legal. No entanto, diversos computadores, *tablets*, celulares, não possuem qualquer mecanismo de segurança, nem mesmo senhas de acesso. Assim, a invasão de qualquer deles será considerada fato atípico[27].

Não há justificativa para a restrição legal. O fato de alguém não inserir mecanismos de segurança em seu dispositivo informático não significa que outrem possa invadi-lo, pois a própria conotação do verbo "invadir" demonstra que o ato se deu contra a vontade do titular. Melhor teria sido que o legislador previsse apenas o núcleo do tipo "invadir", sem prever o meio pelo qual se daria a invasão.

O autor Guilherme de Souza Nucci[28] segue na mesma linha. Se o dispositivo não possui o mecanismo de proteção ou esse não se encontra ativado porque a pessoa se esqueceu, não há proteção, o que não seria correto, diz ele. Cezar Roberto Bitencourt[29] entende que o mais correto seria simplesmente a previsão de "mediante violação indevida", exatamente porque muitos dispositivos não possuem mecanismos de segurança ou esses não se encontram acionados, e, assim, não poderiam ser violados indevidamente para enquadramento no tipo penal.

O legislador esquece que, se mesmo com diversos mecanismos de proteção ativados, ainda há a possibilidade de se invadir um dispositivo, uma pessoa pode entender por desnecessária a inclusão desses mecanismos de segurança, preferindo simplesmente evitar *sites*, *downloads*, aplicativos inseguros. Se ainda assim, tem seu computador, *tablet*, invadido, não mereceria proteção?

Como se vê, o bem jurídico protegido pelo tipo penal é a privacidade, a intimidade,

---

27 No caso recente, de grande repercussão, das fotos íntimas vazadas do ator Stênio Garcia e de sua mulher, há a possibilidade de que não se configure crime exatamente pela lacuna legal. Segundo reportagem do *site* G1 (Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2015/10/stenio-garcia-e-mulher-registram-queixa-por-fotos-intimas-divulgadas.html>. Acesso em: 17 out. 2015), apenas um dos três celulares do casal possuía senha de acesso. Se as imagens foram obtidas sem violação a mecanismo de segurança, não há adequação típica.
28 Ibid., p. 813.
29 BITENCOURT, op. cit., p. 681.

inserido no Capítulo "dos crimes contra a liberdade individual". A *ratio* da norma deveria ser de proteção à liberdade individual e o dispositivo informático de todos. Não se justifica essa restrição legal, pois ninguém que deixa de instalar mecanismos de segurança está abrindo mão de sua privacidade, apenas entende – às vezes por falta de conhecimento, às vezes porque conhece as falhas de tais mecanismos[30] – que esses não seriam necessários. O bem jurídico privacidade não merece ficar desguarnecido simplesmente pela falta dessa elementar típica.

Muitos celulares e *tablets* não possuem senhas de acesso. Ademais, pode ser que alguém entenda por não acioná-los em determinado momento, e outrém se aproveite dessa situação. Por exemplo, alguém que confie nas pessoas que residam em sua casa e a frequentem, deixando seu dispositivo sem senhas, ou quaisquer outros mecanismos de segurança ligados naquele momento. No entanto, alguém, abusando dessa confiança, invade o dispositivo e obtém, adultera, ou destrói dados ou informações dele, essa conduta seria atípica, apesar de ser mais reprovável do que a conduta de um estranho que invade o computador por meio da rede mundial de computadores, ou qualquer outro meio.

Outra questão a ser analisada no dispositivo é a previsão do especial fim de agir junto ao tipo penal. Conforme visto no capítulo anterior, há uma divergência doutrinária a respeito do especial fim de agir. Isso já demonstra que a redação do dispositivo não é a melhor, pois gera uma interpretação dúbia a respeito de haver duas condutas pevistas no tipo penal – como entende Guilherme de Souza Nucci[31] e Fernando Capez[32] – ou apenas uma conduta com fins especiais de agir alternativos – como entendem Rogério Greco[33] e Cezar Roberto Bitencourt[34].

---

30 Sobre essa questão, um executivo da empresa Symantec, fabricante do Norton Antivírus declarou recentemente que "o antivírus está morto", pois estaria cada vez mais difícil de impedir a invasão de *hackers* a computadores e demais dispositivos, o que levaria a indústria a um novo caminho. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2014/05/symantec-fabricante-do-norton-cre-que-antivirus-esta-morto-entenda.html>. Acesso em: 2 de set. de 2015.
31 NUCCI, op. cit., p. 813.
32 CAPEZ; PRADO, op. Cit., p. 347.
33 GRECO, op. cit., 682-683.
34 BITENCOURT, op. cit., p. 472.

Apesar de parecer uma questão meramente doutrinária, no caso concreto pode haver uma situação em que o agente não invada dispositivo, porque já tinha acesso a este, mas instala vulnerabilidades para obter vantagem ilícita. Tratar-se-ia de uma conduta autônoma "instalar" para a primeira corrente, de modo que típica a conduta descrita, ou sem a conduta de "invadir" do dispositivo, que é sempre núcleo do tipo para a segunda corrente, haveria situação atípica?

O simples fato de a redação dar margem a mais de uma interpretação a respeito dos núcleos do tipo e os especiais fins de agir faz perceber que este mereceria uma correção, a fim de não deixar quaisquer dúvidas a respeito de sua aplicação. Como está, porém, fica a análise dos dois núcleos ou de apenas um núcleo com mais de um especial fim de agir para a jurisprudência dos Tribunais.

Independentemente de como se interprete o *caput* do dispositivo, porém, identifica-se que se não estiver presente o especial fim de agir previsto, o fato é atípico. Assim, se o agente invadir o computador de alguém, mas não visar a "obter, adulterar ou destruir dados ou informações sem autorização" ou "instalar vulnerabilidades para obter vantagem ilícita", sua conduta é atípica, seguindo o segundo entendimento[35]. Para o primeiro entendimento[36] não é diferente, já que há dois fins especiais de agir previstos, apenas seriam a conduta invadir com o necessário fim especial "obter, adulterar ou destruir dados ou informações sem autorização" e a conduta de "instalar vulnerabilidades" necessariamente para a obtenção de vantagem ilícita.

A previsão do fim especial de "obter vantagem ilícita" traz a maior omissão ao tipo penal. É possível imaginar que o agente poderá instalar vulnerabilidades sem intencionar qualquer vantagem, mas por simples intenção de prejudicar outrém, danificar o dispositivo. Alguém que simplesmente desgoste da vítima a ponto de deixar seu dispositivo vulnerável,

35 Ibid. e GRECO, op. cit., p. 472.
36 CAPEZ, op. cit., p. 347; NUCCI, p. 813.

por exemplo, instala o mecanismo, e não visa a obter qualquer vantagem, de cunho patrimonial ou não.

Desse modo, para Fernando Capez[37], a previsão de obtenção de vantagem ilícita, restrita para ele à segunda figura típica de instalar vulnerabilidades, é "equivocada e desvirtua o crime", já que não se tutela aqui o patrimônio, mas a intimidade. Segundo ele, isso pode ser demonstrado pelo Capítulo no qual se insere.

A previsão de obtenção de vantagem ilícita não significa que venha a ser uma vantagem patrimonial, apesar do que apresenta Fernando Capez. Por não se tratar de crime contra o patrimônio, a vantagem poderá ser qualquer vantagem obtida pelo agente, desde que seja ilícita. Ainda assim, é equivocado pensar que o agente sempre obterá ganho pessoal com a instalação das vulnerabilidades.

Na figura de equiparação do §1º do dispositivo existe outro equívoco do legislador. Conforme visto, o sujeito passivo desse crime é a sociedade, pois aquele que "produz, oferece, distribui, vende ou difunde" o dispositivo ou programa para que seja praticada a conduta descrita no *caput* não atinge apenas uma pessoa, mas pode atingir qualquer pessoa, é indeterminado.

Nesse sentido, Guilherme de Souza Nucci[38] aponta que o delito pode não ser autonomamente punido, já que o art. 154-B do Código Penal, também inserido pela Lei n. 12.737/2012, exige a representação da vítima do crime, exceto se o crime for cometido contra a Administração Pública direta ou indireta. Desse modo, se o agente produzir programa para que se invada dispositivo informático que não seja da Administração, o crime é de ação pública condicionada e não poderei puni-lo se não estiver atrelado a um crime do *caput*.

Assim, se a intenção do legislador com o §1º foi transformar em condutas típicas o que, normalmente, só seria alcançado por concurso de pessoas – como nos lembra Cezar

37 CAPEZ, op. cit., p. 347.
38 NUCCI, op. cit., p. 815.

Roberto Bitencourt[39] –, independentemente da aplicação do art. 154-A *caput* c/c art. 29, do Código Penal, essa intenção cai por terra com a necessidade de representação pelo art. 154-B, do Código Penal. O fato não deixará de ser típico, mas tornar-se-á impunível, pois não há quem possa representá-lo.

Para que possa haver de fato a punição dos agentes que cometem a conduta do art. 154-A, §1º, mas não incidem no *caput*, tampouco atuam em concurso de agentes, é necessário que se abra uma exceção à previsão do art. 154-B, CP, e tal crime se torne de ação penal pública incondicionada. Aliás, nada mais justo, pois se atinge à coletividade, apenas ao Ministério Público deve caber a decisão pela persecução penal.

Há ainda uma hipótese de aumento de pena do §4º para o caso do §3º do art. 154-A, em que se pune um pós-fato, normalmente impunível. Segundo Cezar Roberto Bitencourt[40], "contrariando princípios básicos do direito penal da culpabilidade, ignora-se o conflito aparente de normas e pune-se, cumulativamente, o crime-meio e crime-fim", que seria um "aproveitamento do resultado da conduta criminosa". Comercializar o produto de um crime é natural, conforme o próprio autor aponta, e haveria uma punição do pós-fato com risco de *bis in idem.* O mesmo quando houver a transmissão gratuita a terceiros.

Aqui o legislador exagera no seu viés punitivo. A partir do momento que o agente invadiu o dispositivo informático, obteve conteúdo de comunicações privadas, segredos informações sigilosas, o crime se consumou. O fato de divulgar, comercializar ou transmitir a terceiros esses dados e informações deveria ser considerado pós-fato impunível.

Entretanto, Cleber Masson[41] discorda, entendendo que o exaurimento da conduta justifica o aumento de pena previsto. Data vênia, o exaurimento do crime não deve ser punido mais gravemente, questão normalmente aplicada a diversos outros crimes, como no caso de furto, em que posterior comercialização do produto não traz nenhuma consequência.

39 BITENCOURT, op. cit., p. 684.
40 BITENCOURT, op. cit. p. 687.
41 MASSON, op. cit., p. 318.

Apesar das críticas, acerta o legislador quando traz a previsão do crime de invasão de dispositivo informático como crime autônomo. Conforme será visto no próximo capítulo, há a necessidade de prever tal crime, diante das questões atuais e aumento de invasão e vulnerabilidade dos dispositivos.

3. DEBATE SOBRE A NECESSIDADE DE NOVAS PREVISÕES LEGAIS

Conforme visto, o tipo penal do art. 154-A, CP apresenta certas falhas. Além disso, deve ser analisado que o art. 154-A, CP é apenas um tipo penal específico para os crimes virtuais, no caso o crime virtual próprio, mas que por si só não exaure a possibilidade normativa.

A *internet* não é mais dispensável pela sociedade. Não há como voltar atrás em um mundo sem o uso cotidiano e globalizado da rede. Nessa linha, o doutrinador Rogério Greco cita os ensinamentos de Cinta Castillo Jimenez[42]:

> A *internet* pressupõe um sonho para seus usuários e um pesadelo para os práticos do direito. (...) todo conjunto de atividades sociais precisa de uma regulamentação. As legislações nacionais avançam com muito atraso no que diz respeito as novas tecnologias. Isso faz com que sejam dificultosas as respostas legais a numerosos litígios que podem suscitar as operações na *internet.*

O meio virtual cria novos delitos, mas também incrementa outros. Segundo Lucrecio Delgado[43], há nos crimes informáticos "celeridade e distância no tempo e no espaço", não é necessária a presença física nem temporal, a ação pode ser preparada, temos "a facilidade de encobrimento", pois é muito simples se encobrir os fatos, e a "dificuldade probatória", já que é fácil fazer desaparecer de forma fraudulenta as atividades após sua realização.

Adeneele Garcia Carneiro[44] aponta diversos crimes cometidos por meio da rede

42 JIMENEZ, apud GRECO, op. cit., p. 469.
43 DELGADO, apud GRECO, op. cit., p. 470.
44 CARNEIRO, Adeneele Garcia. Crimes Virtuais: elementos para uma reflexão sobre o problema na tipificação. In: Âmbito Jurídico, Rio Grande, XV, n. 99, abril 2012. Disponível em: Disponível em: <http://www.ambito-

mundial de computadores, previstos no Código Penal, mas quando cometidos pela *internet*, a punibilidade de tais crimes resta prejudicada pela identificação dos agentes que o cometeram, "uma vez que a produção de provas que evidenciem a configuração do crime e a adequação dessa modalidade de crime praticado em âmbito virtual com os crimes em espécie já previstos em lei é precária".

O crime de furto vem previsto no art. 155, CP, e o tipo penal prevê "subtrair, para si ou para outrem, coisa alheia móvel". Por se tratar de espécie de crime patrimonial, a doutrina majoritária entende que deve haver "lesão a interesse economicamente apreciável"[45].

Nesse sentido é a subtração de cartões de crédito. Não possuindo valor econômico sozinho – seria insignificante seu valor intrínseco – tampouco valor moral, o furto de cartão de crédito é fato atípico. Guilherme de Souza Nucci[46] aponta que será caso de crime de bagatela, e que a administradora ou banco repõe o cartão ao cliente sem nenhum custo, em regra, diferentemente do que ocorre nos casos de talões de cheque[47].

Sabe-se que com o furto de um cartão de crédito diversas fraudes podem ser praticadas, principalmente por meio da rede mundial de computadores, e isso pode levar à uma perda patrimonial imensa à vítima e também à administradora do cartão de crédito. Guilherme de Souza Nucci[48] entende que nesse caso o estelionato restará configurado.

Seguindo nessa linha, há os crimes de estelionato e de furto mediante fraude praticados por meio virtual, seja por cartões furtados/roubados ou clonados, ou por meio de captação ilegal de senhas. Apesar de o tipo penal não ser específico e estar previsto no Código Penal, aqui também visualiza-se uma maior vulnerabilidade das vítimas.

As compras pela *internet*, as transações eletrônicas dos bancos vieram para facilitar a

---

juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17>. Acesso em: 16 set. 2015.

45 BITENCOURT, Cezar Roberto. *Tratado de Direito Penal:* Parte Especial, Volume 3. 6 ed. São Paulo: Saraiva, 2010, p. 38.

46 NUCCI, op. cit., p. 827.

47 No mesmo sentido, MASSON, op. cit., p. 340-341.

48 NUCCI, op. cit., p. 827.

vida de todos, mas também trazem diversos problemas quando o sistema tem uma dificuldade muito maior de saber quem está do outro lado do dispositivo. Com o uso de senhas e cartões de outrem, a verificação se torna falha. O agente se passa pelo titular da conta, pelo titular do cartão, e há uma dificuldade muito grande de se provar o crime descobrir seu autor.

Nesse sentido, Fernando Capez[49] aponta que a *internet* tornou-se um meio muito comum de furto de valores de instituições financeiras. O crime é consumado, segundo o autor, no momento em que os valores são transferidos para a conta do agente, e o furto, nesse caso, é sempre qualificado, pois mediante fraude.

Desse modo, quando um agente se utiliza de dados e informações de outrem, como cartões de banco e/ou de crédito, e pratica estelionatos, furtos mediante fraude, por meio da *internet*, também comete crime mais grave por conta da vulnerabilidade da vítima. Sabe-se que os crimes não são novos nesses casos, apenas as formas de os praticá-los. No entanto, não há, a princípio, a necessidade de prever novos tipos, mas sim de buscar uma resposta eficaz com a legislação atual, inclusive com a responsabilização civil e pagamento de indenização pelos agentes.

Ainda, há os crimes que são praticados por diversos meios, dentre eles, o meio cibernético. Diariamente ofensas são proferidas contra as pessoas em redes sociais, *blogs*, comentários em diversos *sites*, que caracterizam os crimes de calúnia, difamação e injúria. As pessoas que praticam tais crimes muitas vezes estão acobertadas por um véu de anonimato e as vítimas desses crimes estão cada vez mais expostas.

A respeito disso, Aline Gabriela Pescaroli Casado[50] fala do *cyber bullyng:*

> O núcleo central do *cyber bullying* está circunscrito à honra do indivíduo mas também pode atingir ainda outros bens tais como a paz de espírito, a tranqüilidade espiritual como é o caso de crimes cometidos através de meios eletrônicos que esteja coadunada com o delito de ameaça, descrito no artigo 147 do Código Penal.

49 CAPEZ, op. cit, p. 352-353.
50 CASADO, Aline Gabriela Pescaroli. *Cyber bullying*: violência virtual e o enquadramento penal no Brasil. In: Âmbito Jurídico, Rio Grande, XIV, n. 95, dez 2011. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=10882>. Acesso em 16 set 2015.

No seu entendimento, todos os crimes cibernéticos de *cyberbullyng* podem ser alcançados pela lei penal em vigor, recebendo a resposta firme do Estado-juiz. Esses crimes estão já expressamente previstos no Código Penal, artigos 138 a 140, e que se encaixam perfeitamente à descrição.

Ao comentar o crime de difamação, Cezar Roberto Bitencourt[51] entende que a publicidade da difamação é mais desvaliosa do que a simples imputação, porque causa mais danosidade. Partindo desse entendimento, pode-se fazer uma correspondência à difamação praticada por meio da *internet*, que já leva a um dano muito maior às vitimas quando publicado em *sites*, redes sociais.

A solução, tanto para a difamação, quanto para os demais crimes virtuais impróprios – como o estelionato e furto mediante fraude – não passa por uma punição estatal maior no âmbito do direito penal. O direito civil prevê que a responsabilidade será conforme a extensão do dano[52], portanto, o julgador poderá analisar a vulnerabilidade da vítima e a maior danosidade da conduta do agente na seara cível.

Por fim, deve-se analisar a previsão de novos crimes virtuais próprios. Em seu trabalho, Adeneele Garcia Carneiro[53] defende que o *spam* – envio de *e-mails* indesejáveis – deve ser criminalizado por conta dos danos materiais e morais que causa, já que muitas vezes são propagandas indesejáveis ou pior, vírus. Atenta-se que a vítima de um *spam* tem invadida sua privacidade e autodeterminação, por receber *e-mails* os quais não consegue impedir.

Há projetos de lei que buscaram criminalizar o *spam*, como o PL 169/2007, mas que, no entanto, não foram aprovados. Apesar da ideia, o *spam* não parece ser uma questão que deva ser criminalizada. A sua danosidade pode ser resolvida em âmbito da responsabilidade civil, sem que se envolva o direito penal. A exceção ficaria no caso de o *spam* esconder um

51 BITENCOURT, op. cit., 2014, p. 581.
52 BRASIL. Código Civil. Lei n. 10.406/2002. Art. 944: A indenização mede-se pela extensão do dano. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 17 out. 2015.
53 CARNEIRO, op. cit., p. 1.

código malicioso para que com isso houvesse a prática do crime do art. 154-A, CP, exorbitando a esfera do dano moral.

Atente-se que o direito penal deve obedecer ao princípio da intervenção mínima ou *ultima ratio*, de modo que só atua quando os demais ramos do direito não forem capazes de dar a decida tutela aos bens jurídicos. Segundo Cezar Roberto Bitencourt[54], a criminalização de uma conduta é legítima quando meio necessário para a proteção de determinado bem jurídico, se não, a criminalização é inadequada.

No entanto, segundo o autor[55], o legislador caminha no sentido contrário, com abuso da criminalização e penalização "em franca contradição com o princípio em exame, levando a descrédito não apenas o Direito Penal, mas a sanção criminal, que acaba perdendo sua força diante da "inflação legislativa" reinante nos ordenamentos positivos".

O projeto de novo Código prevê crimes cibernéticos mais específicos, como sabotagem informática e dano a dados informatizados[56], mas o legislador já previu diversos crimes no Código Penal e em leis especiais, como o apresentado neste trabalho. Portanto, a previsão de novos tipos legais para os crimes virtuais próprios e impróprios deve passar pela análise do princípio da intervenção mínima, buscando-se evitar um viés punitivista.

CONCLUSÃO

Os crimes virtuais próprios e impróprios são hoje um desafio ao legislador e operador do Direito. Não se pode negar que há uma maior vulnerabilidade da vítima quando os crimes são praticados mediante a *internet*, sejam crimes próprios ou impróprios.

A Lei n. 12.737 trouxe grandes benefícios à proteção do meio virtual, protegendo bem

54 BITENCOURT, Cezar Roberto. *Tratado de Direito Penal:* Parte Especial, V. 1. 13 ed. São Paulo: Saraiva, 2008, p. 13.
55 Ibid., p. 14.
56 O projeto do novo Código Penal pode ser visualizado no *site* do Senado Federal. PL 236/2012. Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/106404> Acesso em 17 out 2015.

jurídico relevante que é a liberdade individual, a intimidade, a privacidade. O dispositivo informático é, finalmente, protegido diante de quem pretenda invadi-lo indevidamente.

No entanto, o tipo penal apresenta diversas falhas em sua redação, conforme apresentado. Assim, deve-se pensar em rediscutir a previsão do crime de invasão do dispositivo informático e solucionar as questões apontadas, sem, contudo, extirpá-lo do ordenamento jurídico, já que representa grande avanço no combate às violações de *tablets*, computadores, celulares multifuncionais etc.

No tocante aos demais crimes cometidos pelo meio virtual, a previsão que já existe no Código Penal mostra-se suficiente para a punição de quem os comete. Os denominados crimes virtuais impróprios nada mais são do que crimes comuns que ganham mais espaço e destaque com a utilização de dispositivos informáticos e, mormente, a *internet*.

Ainda que haja uma vulnerabilidade da vítima maior, conforme destacado, não há necessidade de trazer nesses casos uma nova punição. Trata-se de efetivamente responsabilizar os agentes que cometeram tais crimes e ampliar os meios investigativos para viabilizar essa punição. Ademais, a responsabilidade civil é inerente à tais condutas, cabendo às outras esferas do direito também a sua parte, sob pena de se violar o princípio do direito penal como *ultima ratio*.

Toda a discussão aqui apresentada não impede que surjam novas questões a serem analisadas para a configuração ou não de novos tipos penais. No âmbito da informática sempre há algo novo, que vem a surpreender a todos, de modo que não está excluída a necessidade de se proteger bem jurídico de igual relevância futuramente, como foi feito diante do vácuo normativo que existia antes da lei debatida no presente trabalho. Apesar disso, diante das previsões normativas atuais, o Código Penal com os artigos 154-A, 154-B, tutela o que há de mais relevante em âmbito de crimes virtuais próprios.

Em termos preventivos, a sociedade deve se conscientizar que as pessoas físicas e

jurídicas devem se proteger ante ataques virtuais. As pessoas físicas com mecanismos de segurança, que, sabe-se, não são totalmente eficazes, mas ajudam, evitando acessar *sites* desconhecidos, clicar em *links* inseguros, e principalmente saber em quais *sites* há segurança para a compra *online*. As pessoas jurídicas necessitam de verdadeira segurança para a proteção dos dados dos consumidores, bloqueando o acesso por *firewall*, e diversos outros mecanismos.

As pessoas jurídicas também precisam ser mais transparentes quanto aos ataques que sofrem. Os crimes cibernéticos são subnotificados[57], pois não há obrigação legal na notificação. Há projeto de lei para que isso se torne obrigatório, mas independentemente de qualquer obrigação legal, trata-se de boa fé das empresas e questão de segurança no meio cibernético.

Com o crime de invasão de dispositivo informático, soluciona-se muitas questões antes não respondidas pelo direito penal. Assim, deve-se buscar a segurança nos meios virtuais, responsabilizando os autores dos crimes virtuais.

REFERÊNCIAS

BRASIL. Código Penal. Decreto-lei 2848/1940. Disponível em: <htttp://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 11 mar. de 2015.

_____. Código Civil. Lei n. 10.406/2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 17 out. de 2015

_____. PLS 236/2012. Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/106404>. Acesso em: 17 out. 2015.

BITENCOURT, Cezar Roberto. *Código Penal comentado*. 8. ed. São Paulo: Saraiva, 2014.

_____. *Tratado de Direito Penal*: Parte Especial, V. 1. 13. ed. São Paulo: Saraiva, 2008.

57 MATSUURA, Sérgio e JANSEN, Thiago. JORNAL O GLOBO, Caderno Sociedade, Rio de Janeiro: Editora O Globo. 17 ago 2015. Disponível em: <http://oglobo.globo.com/sociedade/tecnologia/empresas-brasileiras-alvos-de-hackers-se-omitem-sobre-ataques-17203285>. Acesso em: 17 out. 2015.

_____. *Tratado de Direito Penal*: Parte Especial, V. 3. 6. ed. São Paulo: Saraiva, 2010.

CAPEZ, Fernando; PRADO, Stela. *Código Penal comentado.* 5. ed. São Paulo: Saraiva, 2014.

CARNEIRO, Adeneele Garcia. *Crimes virtuais*: elementos para uma reflexão sobre o problema na tipificação. In: Âmbito Jurídico, Rio Grande, XV, n. 99, abr 2012. Disponível em: <http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17>. Acesso em 11 mar 2015.

CASADO, Aline Gabriela Pescaroli. *Cyber bullying*: violência virtual e o enquadramento penal no Brasil. In: Âmbito Jurídico, Rio Grande, XIV, n. 95, dez 2011. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=10882>. Acesso em 16 set 2015.

GRECO, Rogério. *Código penal comentado*. 8. ed. Niterói, RJ: Impetus, 2014.

G1. Rio de Janeiro: <http://g1.globo.com/rio-de-janeiro/noticia/2015/10/stenio-garcia-e-mulher-registram-queixa-por-fotos-intimas-divulgadas.html>. Acesso em: 17 out. 2015

MASSON, Cleber. *Direito Penal esquematizado*: parte especial. V. 2. 6. ed. Rio de Janeiro: Forense; São Paulo: Método, 2014.

MATSUURA, Sérgio e JANSEN, Thiago. JORNAL O GLOBO, Caderno Sociedade, Rio de Janeiro: Editora O Globo. 17 ago 2015. Disponível em: <http://oglobo.globo.com/sociedade/tecnologia/empresas-brasileiras-alvos-de-hackers-se-omitem-sobre-ataques-17203285>. Acesso em: 17 out. 2015.

NUCCI, Guilherme de Souza. *Código penal comentado*: estudo integrado com processo e execução penal. 14. ed. Rio de Janeiro: Forense, 2014.

PRADO, Luis Regis. *Comentários ao Código Penal*: jurisprudência: conexões lógicas com os vários ramos do direito. 9. ed. São Paulo: Revista dos Tribunais, 2014.

TECHTUDO: <http://www.techtudo.com.br/noticias/noticia/2014/05/symantec-fabricante-do-norton-cre-que-antivirus-esta-morto-entenda.html>. Acesso em: 2 de set. de 2015.