O NOVO CRIME DE INVASÃO DE DISPOSITIVO INFORMÁTICO

Cristina Rezende Eliezer
Advogada. Pós graduada em Ciências Criminais pela UCAM-RJ
e em Gestão de Projetos pelo UNIFOR-MG
Professora de Direito no IFMG

Tonyel de Pádua Garcia
Bacharel em Direito pela PUC-MG
Pós graduado em Criminologia pela UCAM-RJ
Pós Graduado em Direito Público-Projeção pela UNB-DF

Recebido em: 30/04/2014
Aprovado em: 23/05/2014

RESUMO

O presente artigo realizou um estudo sobre a Lei 12.737/12, a qual trouxe para o ordenamento jurídico-penal brasileiro o novo crime de “Invasão de Dispositivo Informático”. Antes do advento desta lei, para a criminalização das condutas, era necessário tipificá-las com base nos crimes comuns já existentes no Código Penal, o que nem sempre ocorria de forma perfeita e acabada. Assim, diante dos acelerados processos informáticos e da inexistência de uma norma jurídica aplicável *in concreto*, surgiu a necessidade de suprir o vazio existente no ordenamento legislativo, no que tange à tutela penal da segurança da informação. A finalidade precípua deste estudo é apresentar uma análise detalhada do crime previsto no art. 154-A, do Código Penal. Evidenciou-se, a partir da pesquisa empreendida, que algumas dificuldades poderão surgir na aplicação da nova lei, tendo em vista a ausência de definição legal de muitos termos e expressões utilizadas na norma penal, o que será superado com a jurisprudência. No entanto, a tipificação da invasão de dispositivo informático é uma inovação legislativa importante, que merece uma análise detalhada, vez que se trata de um assunto atual, o qual é alvo de várias controvérsias.

Palavras-chave: Criminalização. Invasão. Dispositivo informático. Liberdade individual.

NEW CRIME OF DEVICE COMPUTING INVASION

ABSTRACT

This paper conducted a study on the Law 12.737/12, which brought the Brazilian criminal legal system the new crime of "Invasion of Computing Device". Before the advent of this law to the criminalization of behaviors, it was necessary classifies them based on already existing in the Penal Code, which was not always the final and perfect form common crimes. Thus, before the accelerated data processing and the lack of a legal standard applicable in concrete, the need arose to fill the void existing in the legislative system, with regard to penal

protection of information security. The primary aim of this study is to present a detailed analysis of the offense provided for in art. 154-A of the Criminal Code. It was evident from the research undertaken, some difficulties may arise in the application of the new law, in view of the absence of legal definition of many terms and expressions used in the criminal standard, which will be overcome with the case. However, the characterization of the invasion of computing device is an important legislative innovation that deserves a detailed analysis, since it is a current issue, which is the subject of several controversies .

Keywords: Criminalization. Invasion. Computing device. Individual freedom.

1 INTRODUÇÃO

O século XXI está vivenciando avanços significativos no que tange à evolução e ao uso da tecnologia. Hipóteses antes denominadas futuristas ou somente visualizadas em desenhos ou filmes de ficção são facilmente identificáveis no cotidiano. A realidade demonstra que os processos acelerados e instantâneos de comunicação via internet não só contribuem para a velocidade das informações, como também para a violação da privacidade. É notório que a internet fez com que o mundo parecesse menor, mas, noutra margem, o mau uso dos aparatos (computadores, *notebooks*, discos externos, *smartphones*, celulares comuns, *tablets*, *pen-drives*, etc) desencadeou a prática de novos ilícitos, consequentemente alterados pela evidente sofisticação tecnológica. Muitas expressões foram criadas objetivando qualificar tais ilícitos, dentre elas, crimes digitais, crimes cibernéticos, crimes de internet, delitos informáticos, entre outras.

Para tipificar os "delitos informáticos" foi publicada a Lei nº 12.737, de 30 de novembro de 2012, a qual trouxe para o ordenamento jurídico-penal brasileiro o novo crime de "Invasão de Dispositivo Informático", previsto no art. 154-A, do Código Penal.

Antes de ser efetivada a publicação de mencionada lei, o respectivo Projeto (nº 35/2012) já havia recebido o apelido de "Carolina Dieckmann", fazendo referência à atriz global, que teve o computador invadido. Suas fotos íntimas foram espalhadas, rapidamente, pelas redes sociais. Tal episódio ganhou considerável repercussão midiática, fazendo com o que o fato gerasse um aceleramento no andamento de projetos que já tramitavam com o fito de regulamentar essas práticas invasivas nos meios informáticos, para modernização do Código Penal Brasileiro. Antes do advento da Lei nº 12.737/12 não era possível realizar uma tipificação adequada desse tipo de conduta criminosa. As condutas delituosas eram tipificadas com base nos crimes comuns já existentes no Código Penal.

O delito de invasão de dispositivo informático consiste na conduta de "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" (art. 154-A, caput, CP).

Não se pretende, neste trabalho, exaurir o estudo sobre o tema proposto. Aspira-se, somente, expor alguns conceitos e argumentos a respeito do assunto, que ainda será objeto de muito estudo pelos especialistas. Adiantando-se ao debate, que será mais bem enfrentado nos tópicos posteriores, denota-se que se trata de uma importante inovação legislativa, já que regulamentou os crimes praticados por intermédio dos meios informáticos.

2 BEM JURÍDICO

O bem jurídico tutelado é a liberdade individual, tendo em vista estar o dispositivo inserido no Código Penal Brasileiro, no capítulo que trata dos "crimes contra a liberdade individual" (artigos 146 a 154, CP), mais precisamente, na Seção IV, intitulada "dos crimes contra a inviolabilidade dos segredos" (artigos 153 a 154-B, CP).

Cabette (2013) entende que a tutela é individual, pois envolve interesses de pessoas (físicas e/ou jurídicas). Salienta o autor que não há nenhuma relação com a proteção à rede mundial de computadores e seu regular funcionamento.

Saliente-se que é objeto de proteção a privacidade, que possui como espécies a intimidade e a vida privada. Esse bem jurídico é tutelado pela Constituição Federal de 1988, em seu art. 5º, inciso X: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação".

Proteger os dados, informações e arquivos armazenados nos dispositivos informáticos das potenciais vítimas desse tipo de crime objetiva assegurar a inviolabilidade da intimidade e da vida privada das mesmas.

Para Mendes e Coelho (2007, p. 370):

> O direito à privacidade, em sentido mais estrito, conduz à pretensão do indivíduo de não ser foco da observação por terceiros, de não ter os seus assuntos, informações pessoais e características particulares expostas a terceiros ou ao público em geral.

Cabette (2013) também entende que o legislador acertou ao criar o tipo penal em epígrafe, principalmente, considerando o fato de que se busca tutelar um bem jurídico constitucionalmente previsto.

3 SUJEITO ATIVO E PASSIVO

De acordo com Cavalcante (2012), no crime de "invasão de dispositivo informático", o sujeito ativo pode ser qualquer pessoa (crime comum). No entanto, adverte o autor que não será sujeito ativo desse crime a pessoa que tenha autorização para acessar os dados constantes do dispositivo.

Para Cabette (2013, p. 1-2), é fácil identificar os sujeitos deste crime:

> O crime é comum, de modo que pode ser sujeito ativo qualquer pessoa. O mesmo se pode dizer com relação ao sujeito passivo. O funcionário público também pode ser sujeito ativo dessa infração, mas a lei não prevê nenhuma causa de aumento de pena. Pode-se recorrer nesse caso às agravantes genéricas previstas no artigo 61, II, "f" ou "g", CP, a depender do caso. Também pode ser sujeito passivo a pessoa jurídica. É óbvio que as pessoas jurídicas também podem ter dados ou informações sigilosos abrigados em dispositivos informáticos ligados ou não à rede mundial de computadores, os quais podem ser devassados, adulterados, alterados ou destruídos à revelia da empresa ou do órgão responsável.

Cabette (2013) lembra que isso se torna mais que patente quando se constata previsão de qualificadora para a violação de segredos comerciais ou industriais e informações sigilosas definidas em lei (artigo 154 – A, § 3º, CP). Ainda ressalta que podem ser vítimas pessoas jurídicas de direito privado ou público, inclusive a administração pública direta ou indireta de qualquer dos entes federativos (União, Estados, Municípios ou Distrito Federal). Podem ainda ser sujeitos passivos empresas privadas concessionárias ou permissionárias de serviços públicos também com relação a qualquer dos entes federativos. Acrescenta que melhor andaria o legislador se houvesse previsto um aumento de pena para a atuação do funcionário público no exercício das funções, bem como para os casos de violação de dados ou informações ligados a órgãos públicos em geral (administração direta ou indireta).

Cabette (2013, p. 2) afirma que:

> O sujeito passivo da infração é, portanto, qualquer pessoa passível de sofrer dano moral ou material decorrente da ilícita obtenção, adulteração ou destruição de dados ou informações devido à invasão ou violação de seu sistema informático, mediante vulneração de mecanismo de segurança. Assim também é sujeito passivo aquele que sofre a instalação indevida de vulnerabilidades em seu sistema para o fim de obtenção de vantagens ilícitas. São exemplos as atuações em que indivíduos inserem

> vírus espiões para obter, adulterar ou destruir dados em sistemas informáticos. Importa ressaltar que a vítima não precisa ser a proprietária ou titular do sistema informático ou do hardware ou software invadido pelo criminoso. Na verdade, qualquer pessoa que tenha sua privacidade violada pelo invasor é sujeito passivo da infração. Por exemplo: um amigo usa o computador de outro para conversas particulares via internet, cujo conteúdo é ali armazenado por meio de senha. Alguém invade o sistema informático daquele computador e viola a privacidade, não do dono do computador, mas do seu amigo. Ora, este segundo também é vítima do crime. O mesmo se pode afirmar quanto aos usuários das chamadas "Lans houses" que sofram o mesmo tipo de violação indevida.

Cavalcante (2012) salienta que o sujeito passivo no crime em comento é o titular do dispositivo, ou seja, em regra, a vítima é o proprietário do dispositivo informático (pessoa física ou jurídica).

No entanto, ressalta o autor que é possível também identificar, em algumas situações, como sujeito passivo, o indivíduo que, mesmo sem ser o dono do computador, é a pessoa que efetivamente utiliza o dispositivo para armazenar seus dados ou informações que foram acessados indevidamente.

Cavalcante (2012, p. 2) finaliza afirmando que:

> É o caso, por exemplo, de um computador utilizado por vários membros de uma casa ou no trabalho, onde cada um tem perfil e senha próprios. Outro exemplo é o da pessoa que mantém um contrato com uma empresa para armazenagem de dados de seus interesses em servidores para acesso por meio da internet ("computação em nuvem", mais conhecida pelo nome em inglês, qual seja, *cloud computing*).

Portanto, embora seja possível identificar, em tese, quais são os sujeitos ativos e passivos do crime de "invasão de dispositivo informático", é necessário frisar que os delitos praticados podem ser de difícil apuração, o que dificultará, sobremaneira, a identificação da autoria do crime (sujeito ativo). Tal dificuldade será analisada de maneira pormenorizada em tópico específico.

4 TIPO SUBJETIVO

O elemento subjetivo é o dolo, que deve ser acrescido de um específico fim de agir. A "invasão" do dispositivo informático deve ocorrer com o objetivo de "obter, adulterar ou destruir dados ou informações do titular do dispositivo" ou, ainda, "instalar vulnerabilidades para obter vantagem ilícita".

Cabette (2013, p. 2) é taxativo ao afirmar que:

> O tipo subjetivo do ilícito é informado somente pelo dolo. Não há previsão de figura culposa. O dolo é específico, pois exige a lei que a violação se dê com o especial fim de "obter, adulterar ou destruir dados ou informações" ou "instalar vulnerabilidades para obter vantagem ilícita". Note-se que há duas especificidades independentes para o dolo do agente: primeiro o fim especial de "obter, adulterar ou destruir dados ou informações", sem a exigência de que se pretenda com isso obter vantagem ilícita. Ou seja, nessa parte o tipo penal não requer do agente outra vontade senão aquela de vulnerar o sistema e suas informações ou dados, podendo agir inclusive por mera curiosidade ou bisbilhotice.

Cabette (2013) adverte que na instalação de vulnerabilidades, o intento tem de ser a obtenção de vantagem ilícita. Lembra que o legislador não foi restritivo, portanto, segundo o autor, a vantagem intencionada pode ser econômico–financeira ou de qualquer outra espécie. Cabette (2013, p. 2) salienta que:

> Por exemplo, se instalo num computador uma via de acesso a informações para obter senhas bancárias e me locupletar ou se instalo uma vulnerabilidade num computador para saber dos hábitos e preferências de uma mulher desejada para poder conquistá-la o tipo penal está perfeito.

Frise-se que é exigida, para a configuração do dolo, a vontade livre e consciente de invadir dispositivo informático alheio. Exigem-se, ainda, os elementos subjetivos específicos, quais sejam: "o fim de obter, adulterar ou destruir dados ou informações" e "para obter vantagem ilícita". O crime é instantâneo e a tentativa é admissível.

5 TIPO OBJETIVO

A conduta criminosa prevista no art. 154-A do Código Penal constitui tipo misto alternativo. De acordo com Cabette (2013), trata-se de um crime de ação múltipla ou de conteúdo variado, tendo em vista que apresenta dois núcleos de conduta (verbos invadir ou instalar), podendo o agente incidir em ambos, desde que em um mesmo contexto, e responder por crime único. Salienta o autor que não exige o tipo penal que o dispositivo informático esteja ligado à rede mundial de computadores ou mesmo rede interna empresarial ou institucional (internet ou intranet). Assim sendo, estão protegidos os dados e informações constantes de dispositivos de informática e/ou telemática.

Cabette (2013, p. 3) lembra que:

> A invasão, conforme manda a lei, deve ser de dispositivo informático "alheio" e "mediante violação indevida" de "mecanismo de segurança" (elementos normativos do tipo). É claro que não se poderia incriminar alguém que ingressasse no próprio

> dispositivo informático; seria como incriminar alguém que subtraísse coisa própria no caso do furto. Além disso, a violação deve ser "indevida", ou seja, desautorizada e sem justa causa. Obviamente que o técnico informático que supera mecanismo protetor para consertar aparelhagem não comete crime, inclusive porque tem a autorização expressa ou no mínimo tácita do cliente. Também não comete o crime a Autoridade Policial que apreende mediante ordem judicial aparelhos informáticos e manda periciar seus conteúdos para apuração criminal.

Nesse sentido, o art. 154-A do CP é preciso ao instituir que existe a necessidade de que o dispositivo informático seja alheio, ou seja, não pertença ao agente que o utiliza. Somente assim se caracterizará o delito em estudo. Anote-se também que não existe um rol taxativo no que tange aos aparelhos.

Assim sendo, a expressão "dispositivo informático" é bastante genérica, possibilitando que seja feita uma interpretação abrangente. Tendo em vista que é espantosa a velocidade com que a tecnologia se aperfeiçoa, o legislador acertou ao deixar de restringir ou limitar os aparelhos ou dispositivos informativos, inerentes ao artigo em comento.

Cabette (2013, p. 3) lembra que a justa causa ou autorização deve existir do início ao fim da conduta do agente e este deve se ater aos seus estritos limites razoáveis.

> Por exemplo, se um técnico de informática tem a autorização para violar as chaves de acesso a um sistema de alguém para fins de conserto e o faz, mas depois coleta fotos particulares ali armazenadas, corrompe dolosamente informações ou dados extrapolando os limites de seu trabalho sem autorização do titular, passa a cometer infração penal. É importante ressaltar que, como não existe figura culposa, o erro muito comum em que o técnico em informática, ao realizar um reparo, formata o computador e acaba destruindo conteúdos importantes para a pessoa sem dolo, mas por negligência ou imperícia, não constitui crime. Pode haver, contudo, infração civil passível de indenização por danos morais e/ou materiais.

Nota-se que o crime previsto no art. 154-A do Código Penal não admite a figura culposa. Em caso de inexistência de dolo, mas, presentes a negligência ou imperícia, não haverá a constituição de crime. Contudo, o autor poderá ser responsabilizado civilmente.

Cabette (2013, p. 3) salienta que:

> É ainda importante ressaltar que não é qualquer dispositivo informático invadido que conta com a proteção legal. Para que haja o crime é necessário que o dispositivo conte com "mecanismo de segurança" (v.g. antivírus, "firewall", senhas etc.). Assim sendo, o dispositivo informático despido de mecanismo de segurança não pode ser objeto material das condutas incriminadas, já que o crime exige que haja "violação indevida de mecanismo de segurança". Dessa maneira, a invasão ou instalação de vulnerabilidades em sistemas desprotegidos é fato atípico. Releva observar que na requisição da perícia nesses casos é importante que a autoridade policial formule quesito a fim de que o perito indique a presença de "mecanismo de segurança" no dispositivo informático violado, bem como que esse mecanismo foi violado,

> indicando, inclusive, se possível, a forma dessa violação, para melhor aferição e descrição do "modus operandi" do agente.

Nota-se, analisando o trecho anterior colacionado, que não é qualquer dispositivo informático invadido que conta com o amparo legal. Para que o crime seja configurado, é imprescindível que o dispositivo conte com mecanismos de segurança, tais como antivírus, *firewall* e senhas, dentre outros.

O dispositivo informático que não possui mecanismo de segurança não pode ser objeto material das condutas incriminadas, já que o crime exige que haja "violação indevida de mecanismo de segurança".

Cavalcante (2012) também entende dessa forma e ressalta que somente haverá a configuração do crime se a invasão ocorrer com a violação de mecanismo de segurança imposto pelo usuário do dispositivo. Afirma que não constituirá o crime se o indivíduo, por exemplo, na hora do almoço, aproveitar para acessar o computador do colega de trabalho, o qual não é protegido por senha ou qualquer outro mecanismo de segurança.

Lembra o autor que também não haverá crime se alguém encontrar o *pen drive* de seu colega de trabalho e o mesmo não estiver protegido por senha e, assim, vasculhar os documentos e fotos ali armazenados. Critica que há uma falha na lei, tendo em vista que a privacidade continua sendo violada, mas, no entanto, não receberá punição penal.

6 CONSUMAÇÃO

O crime previsto no art. 154-A do Código Penal é um crime formal, ou seja, é consumado com a simples invasão, independente da ocorrência do resultado.

Cabette (2013) afirma que o crime se consuma com a mera invasão ou instalação de vulnerabilidade, não importando se são obtidos os fins específicos de coleta, adulteração ou destruição de dados ou informações ou mesmo obtenção de vantagem ilícita. Assevera o mesmo autor que:

> Tais resultados constituem mero exaurimento da infração em estudo. Não obstante formal, o ilícito é plurissubsistente, de forma que admite tentativa. É plenamente possível que uma pessoa tente invadir um sistema ou instalar vulnerabilidades e não o consiga por motivos alheios à sua vontade, seja porque é fisicamente impedida, seja porque não consegue, embora tente violar os mecanismos de proteção (CABETTE, 2013, p. 4).

Nota-se que, além de se tratar de um crime formal, a tentativa é admissível. É possível que o autor do ilícito tente invadir um sistema ou instalar vulnerabilidades, mas não consiga por motivos alheios à sua vontade. Entende-se que, embora não tenha conseguido o autor cumprir a finalidade desejada, o simples fato de tentar invadir de forma dolosa o dispositivo incorreria em crime.

7 MODALIDADE EQUIPARADA (art. 154-A, § 1º, CP)

No § 1º do art. 154-A há a previsão de que "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*".

Greco (2013, p. 5) afirma que:

> Produzir significa criar, gerar, fabricar; oferecer importa em ofertar, gratuita ou onerosamente; distribuir tem o sentido de partilhar, repartir; vender tem o significado de transferir (o dispositivo ou o programa de computador) mediante um preço determinado; difundir diz respeito a propagar, divulgar, espalhar. Todas essas condutas, vale dizer, produzir, oferecer, distribuir, vender ou difundir dizem respeito à dispositivo ou programa de computador.

Cavalcante (2012) ressalta que, por exemplo, se um indivíduo desenvolver um programa do tipo "cavalo de troia" (*trojan horse*), ou seja, um *malware* (*software* malicioso) que, depois de instalado no computador, libera uma porta para que seja possível a invasão da máquina, não haverá crime. Cita também que em alguns cursos de informática, o professor desenvolve *softwares* espiões para testarem a segurança da rede e aprimorarem técnicas de contraespionagem; há também o caso das empresas que elaboram e comercializam tais programas.

Para o autor, em todas as situações acima citadas, não haverá crime, considerando que o objetivo não é o de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular. Há somente o intuito acadêmico, docente ou de melhorar a segurança das redes empresariais, descobrindo as brechas existentes. O fato seria atípico, portanto, por faltar o elemento subjetivo do injusto.

Cabette (2013) salienta que o § 1º descreve crime de ação múltipla e de dolo específico, já que exige o intuito de ensejar a prática das condutas previstas no *caput*.

8 AUMENTO DE PENA (art. 154-A, §2º, CP)

Nos termos do § 2º do art. 154-A do CP "aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico". Percebe-se que haverá um aumento na pena, de um sexto a um terço, caso venha a ocorrer prejuízo econômico.

Cabette (2013) lembra que o incremento da lesão patrimonial produz agravamento da falta de valor do resultado da conduta, justificando a exacerbação punitiva. Segundo o autor, o § 2º é bem claro, de forma que não há de se cogitar a aplicação de aumento considerando eventual dano moral. Nesse sentido Cabette (2013, p. 4-5) é categórico ao afirmar que:

> Somente o prejuízo de caráter econômico–financeiro alicerça o aumento. Pretender equipar tal situação ao dano moral constituiria analogia "in malam partem" vedada na seara penal. Também é de se atentar que o aumento de pena do § 2º, até mesmo pela topografia do dispositivo, somente tem aplicabilidade para a figura simples e a figura equiparada (artigo 154 – A, "caput" e seu § 1º, CP), não alcançando a forma qualificada do § 3º.

Percebe-se que a causa de aumento de pena, acima mencionada, refere-se apenas ao *caput* do art. 154-A, não sendo, assim, aplicada no caso do § 3º, o qual será explicado no tópico seguinte.

9 FORMAS QUALIFICADAS (art. 154-A, § 3º, CP)

Nos termos do § 3º do artigo em comento:

> 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.

Nota-se que haverá a qualificadora prevista neste § 3º se, mediante a invasão do dispositivo eletrônico, o agente obter o conteúdo de: comunicações eletrônicas privadas; segredos comerciais ou industriais; informações sigilosas ou quando possibilitar o controle não autorizado do dispositivo invadido.

Cavalcante (2012) salienta que o supracitado § 3º constitui exemplo de aplicação do "princípio da subsidiariedade" (expressa ou explícita), considerando que o próprio tipo penal prevê que não haverá invasão qualificada se a conduta do agente constituir um crime mais grave.

Maggio (2013, p. 3-4) afirma que:

> O § 3º, do art. 154-A, do Código Penal, define o crime de invasão de dispositivo informativo qualificado. O crime é qualificado quando ao tipo penal básico é acrescentada alguma circunstância específica que o torna mais grave, alterando o mínimo e o máximo das penas previstas em abstrato. Assim, enquanto a figura simples ou equiparada (tipo básico) tem pena de detenção, de três meses a um ano, e multa, as figuras qualificadas em razão das circunstâncias específicas têm pena de reclusão, de seis meses a dois anos, e multa. São figuras expressamente subsidiárias, uma vez que o legislador após descrever a sanção penal, impõe: "se a conduta não constitui crime mais grave".

Assim sendo, as figuras qualificadas do § 3º são subsidiárias, tendo em vista que há a previsão expressa de que a norma somente será aplicada se a conduta não constituir crime mais grave.

Cabette (2013) cita como exemplos de crimes mais graves a violação de sigilo bancário ou de instituição financeira, nos termos do artigo 18 da Lei 7.492/86, bem como determinadas condutas previstas na Lei de Segurança Nacional (artigos 13 e 21 da Lei 7.170/83).

9.1 Outros aumentos de pena (art. 154-A, §§ 4º e 5º, I a IV, CP)

O § 4º do artigo em análise dispõe que: "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".

De acordo com Cabette (2013, p. 6):

> O primeiro aumento, previsto no § 4º, é da ordem de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. Novamente o desvalor do resultado indica a exacerbação punitiva. Ora, diferente é o invasor obter os dados ou informações e guardá-los para si. Quando ele transmite esses dados a terceiros amplia o dano à privacidade ou ao sigilo, o que justifica a reprimenda mais gravosa. É por esse desvalor do resultado ampliado que o legislador erige em causa especial de aumento o que normalmente seria um "post factum" não punível ou mero exaurimento delitivo.

A previsão legal é de que haverá o aumento de pena, na hipótese do § 3º, se for efetivada a divulgação, comercialização ou transmissão a terceiros, dos dados ou informações obtidas. No entanto, se o invasor obtiver os dados e guardá-los para si, não haverá a ampliação do dano à privacidade ou ao sigilo. Quando há a transmissão a terceiros, consequentemente, há a reprimenda mais gravosa.

Nos termos do § 5º, do art. 154-A do Código Penal:

> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> 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;
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Nota-se que haverá um aumento de pena quando o crime qualificado tiver como sujeitos passivos as pessoas elencadas nos incisos I a IV do § 5º, do artigo em comento.

Cabette (2013) lembra que essas pessoas gozam de especial proteção legal. Tal proteção não se dá em função de um injustificado privilégio pessoal, mas em razão do cargo ocupado e da relevância de suas atribuições, bem como pela importância diferenciada dos informes sigilosos que detêm e podem envolver. Tudo isso porque envolvem, frequentemente, interesses que suplantam em muito a seara pessoal para atingir o interesse público e o bem comum.

10 PENA E AÇÃO PENAL

No *caput* do art. 154-A e no § 1º do mesmo artigo há a previsão de que a pena em abstrato para o crime simples e para a figura equiparada é de detenção, de 3 meses a 1 ano, e multa. Na forma majorada do § 2º do artigo em comento, a pena máxima seria inferior a 1 ano e 4 meses, já que o aumento máximo é de um terço. Nesse sentido, Cabette (2013, p. 7) ressalta que:

> A pena prevista para o crime simples (artigo 154 – A, "caput", CP) e para a figura equiparada (artigo 154 – A, § 1º, CP) é de detenção de 3 meses a 1 ano e multa. Dessa forma trata-se de infração de menor potencial ofensivo, afeta ao procedimento da Lei 9.099/95. Mesmo na forma majorada do § 2º, a pena máxima não ultrapassaria 1 ano e 4 messes (aumento máximo de um terço), de modo que seguiria como infração de menor potencial.

Assim, trata-se de crime de menor potencial ofensivo (Lei nº 9.099/95). Cavalcante (2012) afirma que a pena é irrisória e representa proteção insuficiente para um bem jurídico tão importante. Para o autor, em virtude desse *quantum* de pena, será muito frequente a ocorrência de prescrição retroativa pela pena concretamente aplicada.

De acordo com os ensinamentos de Cavalcante (2012, p. 4-5):

> O art. 154-A do CP é crime de menor potencial ofensivo, sujeito à competência do Juizado Especial Criminal (art. 61 da Lei n.° 9.099/95). Em regra, nos delitos sujeitos ao Juizado Especial Criminal o instrumento de apuração do fato utilizado pela autoridade policial é o termo circunstanciado (art. 69 da Lei n.° 9.099/95). Entretanto, nos casos do art. 154-A do CP muito provavelmente o termo circunstanciado não será suficiente para apurar a autoria e materialidade do delito, sendo quase que imprescindível a instauração de inquérito policial, considerando que, na grande maioria dos casos, será necessária a realização de busca e apreensão na residência do investigado, perícia e oitiva de testemunhas etc.

No que tange à pena imposta ao autor do crime de invasão de dispositivo informático, percebe-se que a mesma, além de ser irrisória, representa uma proteção insuficiente ao bem jurídico tutelado, o qual é bastante importante. Além disso, há a dificuldade de comprovação da autoria e materialidade do delito por intermédio do termo circunstanciado.

De acordo com Cabette (2013, p. 7):

> Também a forma qualificada do artigo 154 – A, § 3º, CP é abrangida pela Lei 9.099/95, eis que a pena máxima não ultrapassa dois anos (reclusão de 6 meses a dois anos e multa). Apenas nas hipóteses de aplicação dos aumentos de pena previstos nos §§ 4º ou 5º, é que a pena máxima iria ultrapassar o patamar de dois anos, de modo que não seria mais abrangida pela Lei 9.099/95. O único instituto dessa lei então aplicável seria a suspensão condicional do processo nos termos do artigo 89 daquele diploma, já que a pena mínima não ultrapassa um ano, nem mesmo com os acréscimos máximos. Somente cogitando da concomitância dos aumentos dos §§ 4º e 5º, é que o patamar, considerando os acréscimos máximos, suplantaria um ano na pena mínima de modo que nem mesmo a suspensão condicional do processo seria admissível.

A forma qualificada, prevista no art. 154 – A, § 3º, CP, também será abrangida pela Lei 9.099/95, uma vez que a pena máxima não ultrapassa dois anos. Somente nas hipóteses de aplicação dos aumentos de pena previstos nos §§ 4º ou 5º, é que a pena máxima iria ultrapassar dois anos. Nesse caso, não mais seria abrangida pela Lei 9.099/95.

No que tange à ação penal, a mesma é regulada pelo art. 154-B do CP, que dispõe: “Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos”.

Cavalcante (2012) assinala que, em regra, o crime do art. 154-A é de ação penal pública condicionada à representação. Para o autor, isso se justifica em razão da intimidade e da vida privada serem bens disponíveis e também pelo fato de que a vítima tem o direito de

avaliar se deseja evitar o processo judicial. Assim, se protegeria contra os efeitos deletérios que podem advir da divulgação das circunstâncias que envolvem o fato.

Cavalcante (2012, p. 7) ainda salienta que:

> A depender do caso concreto, a instauração da investigação e do processo penal poderão implicar nova ofensa à intimidade e privacidade do ofendido considerando que outras pessoas (investigadores, Delegados, servidores, Promotor, Juiz etc.) terão acesso ao conteúdo das informações que a vítima preferia que ficassem em sigilo, tais como fotos, correspondências, mensagens, entre outros. Dessa forma, é indispensável que a vítima ofereça representação para que seja iniciada qualquer investigação sobre o fato (art. 5º, § 4º, do CPP), bem como para que seja proposta a denúncia por parte do Ministério Público.

Excepcionalmente, se o delito for praticado contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios e empresas concessionárias de serviços públicos, o crime do art. 154-A será de ação pública incondicionada.

11 DIFICULDADES E PERSPECTIVAS COM A APLICAÇÃO DA NOVA LEI PENAL

Poderá haver algumas dificuldades na aplicação da Lei nº 12.737, de 30 de novembro de 2012, a qual inseriu a invasão de dispositivo informático alheio como crime no Código Penal Brasileiro.

Ramos Júnior (2013, p. 115) faz importantes observações sobre isso:

> A ausência de definição legal de muitos termos e expressões utilizadas na norma penal certamente será o primeiro grande desafio a ser enfrentado na aplicação da lei, por haver a necessidade de esclarecer o que se entende por dispositivo informático, mecanismo de segurança, autorização tácita, invasão, vulnerabilidades etc. Esses obstáculos serão superados com a jurisprudência. Enquanto isso não ocorre, para solucionar essas questões, pondera-se, em relação ao conceito de dispositivo informático para fins penais, que seja possível a sua abrangência aos dispositivos que funcionam por computação em nuvem; no que tange ao mecanismo de segurança, considera-se que o seu conceito não pode ser restrito a apenas algumas formas de proteção, devendo englobar todo mecanismo computacional, desde uma senha ou um anti-vírus até a tecnologia mais moderna de detecção de intrusões, invasões e ataques cibernéticos.

Conforme já mencionado alhures, não existe um rol taxativo no que tange à enumeração dos aparelhos. Portanto, a expressão “dispositivo informático” é bastante genérica, possibilitando que seja feita uma interpretação bastante abrangente.

De certa forma, o legislador acertou em não limitar quais são as espécies de dispositivos informáticos, tendo em vista a grande velocidade com que a tecnologia se modifica. Seria impossível identificar na legislação penal todos os dispositivos existentes e os que, porventura, venham a surgir. No entanto, a ausência de definição legal de muitos termos e expressões utilizadas na norma penal poderá se tornar um grande desafio na aplicação da nova lei. A jurisprudência poderá vir a suprir essas definições.

No que tange ao conceito de “invasão”, Ramos Júnior (2013) lembra que o mesmo não pode ficar adstrito às hipóteses em que ocorra um "ataque" ao dispositivo informático alheio. Segundo o autor, para efeitos penais, deve-se entender que há invasão sempre que alguém tente violar indevidamente e burlar o mecanismo de segurança do dispositivo informático.

Ramos Júnior (2013, p. 115) faz uma importante afirmação sobre essa questão:

> Caso se entenda o contrário, que só há invasão se houver um ataque ao mecanismo de segurança e desde que o hacker invasor consiga obter dados e informações do dispositivo informático, não haverá possibilidade de punição do delito na sua forma tentada. Este não é o intuito da norma penal, uma vez que se trata de crime formal que se consuma independentemente do resultado de o agente obter os dados armazenados. Desta forma, para fins de consumação do delito, a invasão pode ocorrer mesmo nos casos em que não há "ataque" ao computador, como, por exemplo, quando o invasor induz o titular do dispositivo em erro fazendo acessar algum código malicioso para ter acesso ao computador alheio, porque, nesse caso, o invasor se valeu da engenharia social como artifício fraudulento para burlar o mecanismo de segurança com o intuito de poder ter acesso aos dados e informações do dispositivo informático invadido.

É inegável que a Lei 12.737/12 trouxe inúmeros termos e expressões novas, sendo que a ausência de definição dos mesmos pode gerar problemas no ato de aplicação da legislação, tanto persecutória quanto processual. Problemas tais como a disponibilidade ou não do bem jurídico tutelado (em obediência ao artigo 5º da Constituição Federal), a pretensão punitiva na forma condicionada a representação, a taxatividade e a tipificação em relação à materialização do crime, uma vez que este adstringe a aspectos formais (não obstante o elemento subjetivo de dolo), a disseminação da informação e os crimes em massa.

Greco (2013) afirma que os delitos praticados através da informática podem ser de difícil apuração, principalmente, devido à dificuldade de identificação do autor do crime, que é condição para a instauração de inquérito policial, se for o caso.

Ramos Júnior (2013, p. 116) também faz uma crítica em relação ao conceito de “vulnerabilidades”:

> É o que ocorre, por exemplo, em relação ao conceito de “vulnerabilidades”. Uma vez que a norma penal prevê como crime a conduta de instalar vulnerabilidades em dispositivo informático alheio com o fim de obter vantagem ilícita, não seria correto afirmar, exclusivamente sob o ponto de vista computacional, que o delito em questão seria crime impossível, porque as vulnerabilidades seriam bugs (erros ou falhas no sistema) que não foram instaladas pelo invasor e que seriam preexistentes à invasão. Para efeitos de aplicação da norma penal, as vulnerabilidades devem ser entendidas como qualquer código malicioso capaz de expor a risco a segurança dos dados e das informações armazenadas ou o próprio funcionamento do dispositivo informático, pois a lei penal deve ser interpretada teleologicamente, conforme os princípios jurídicos que lhe são próprios, buscando extrair o seu exato alcance e real significado através da busca da vontade da lei, atendendo à sua finalidade que está expressa no art. 1º da Lei 12.737/12, isto é, a tipificação criminal de delitos informáticos.

Assim, para o autor, poderão ser considerados como "vulnerabilidades", para fins de aplicação da lei penal, os vírus de computador. No entanto, não haverá crime no caso de instalação de *cookies* no computador do usuário, pois estes geralmente são "instalados" automaticamente pelo computador quando se acessa a página na internet.

Ramos Júnior (2013, p. 117) lembra que, superando a questão da ausência de falta de definição de conceitos para os novos termos e expressões trazidos pela Lei 12.737/12, observa-se que, em se tratando de delitos informáticos, pode haver o problema da identificação do autor do crime.

> A navegação da internet costuma deixar um rastro por meio do qual é possível fazer uma investigação a fim de identificar o criminoso. Assim, é possível descobrir qual é o endereço de IP (Internet Protocol) utilizado pelo agente, para identificar a hora e o local de onde o hacker invasor acessou a internet para praticar o delito.

Importante frisar que foi publicada recentemente, no Diário Oficial da União, a Lei 12.965, de 23 de abril 2014, conhecida como “Marco Civil da Internet”. Mencionada lei estabelece, além dos princípios, as garantias, direitos e deveres, no que tange ao uso da internet no Brasil.

O “Marco Civil da Internet” traz clareza e solução a determinados temas e lacunas, sobretudo, adverte sobre o período de guarda de registros e dados de usuários. Assim sendo, será facilitada a identificação do autor do crime, bem como a elucidação do horário e do local utilizados pelos criminosos para invadir os dados.

12 CONCLUSÃO

A Lei nº 12.737/2012 trouxe para o ordenamento jurídico-penal brasileiro o novo crime de “Invasão de Dispositivo Informático”, previsto no art. 154-A, do Código Penal. Foi chamada pela imprensa de “Lei Carolina Dieckmann”, devido ao fato de a atriz ter sido vítima de invasão de seu computador, com a consequente divulgação de suas fotos íntimas pela internet. Até então, tal conduta delituosa não era prevista, de forma específica, como infração penal.

A pressão social causada em decorrência de a atriz global ter sido vítima dessa invasão fez com que houvesse um clamor exacerbado para a criminalização dos delitos informáticos. No entanto, em função da urgência para a publicação e sanção da lei em comento, a mesma pode ser considerada imperfeita, o que é corriqueiro nos textos legais brasileiros. Por se tratar de uma legislação recente, as primeiras impressões ainda não são suficientes para legitimar a eficácia (ou não) do dispositivo legal. Certamente, vários obstáculos serão superados pela jurisprudência.

A tipificação dos “delitos informáticos” é uma inovação bem recepcionada, tendo em vista os acelerados processos informáticos e constantes avanços tecnológicos. No entanto, além de este sintetizado estudo não esgotar a análise do tipo e nem tampouco exaurir os conceitos e argumentos sobre o tema em comento, existe o grande desafio de transpor o mero juridicismo, aplicando-se os dispositivos legais de maneira efetiva.

Para tanto, é necessária uma estruturação da Polícia Judiciária, visando a que a apuração das infrações penais e autoria sejam realizadas com emprego de diligência e zelo. As apurações devem ser realizadas com extremo rigor e eficácia. Por fim, tal instituto é um estímulo ao próprio Poder Legislativo, para que faça uma análise contínua dos temas correlatos aos crimes de informática, pois trata-se de uma matéria que exige uma constante discussão.

Os intuitos da lei penal, juntamente com a pretensão punitiva do Estado, constituem-se em prevenção de danos ao bem tutelado. Logo, as vias administrativas, judiciárias e legislativas devem permanecer atentas às possíveis sanções e coações nos crimes de informática, reiterando o tema, sequencialmente, a fim de que se atinja a completude da norma, alcançando a eficácia para a qual existe.

Neste contexto, a inserção do dispositivo legal no Código Penal Brasileiro só terá efetividade quando os direitos das vítimas dos crimes informáticos, as quais sofreram

violação criminosa e dolosa de seus dados ou arquivos pessoais, forem assegurados e os autores dos delitos devidamente identificados e punidos.

REFERÊNCIAS

BRASIL, Constituição (1988) **Constituição da República Federativa do Brasil**. Brasília: Senado, 1988. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 26 abr. 2014.

_____. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Diário Oficial da União, Brasília, 1 de janeiro de 1942. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 26 abr. 2014.

_____. **Lei nº 9.099, de 26 de setembro de 1995**. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Diário Oficial da União, Brasília, 26 de setembro de 1995. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9099.htm>. Acesso em: 20 abr. 2014.

_____. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União, Brasília, 30 nov. 2012. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 25 abr. 2014.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, 23 abr. 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 30 abr. 2014.

CABETTE, E. L. S. **O novo crime de invasão de dispositivo informático**. Disponível em: < http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico>. Acesso em: 18 abr. 2014.

CAVALCANTE, M. A. L. **Primeiros comentários à Lei n.° 12.737/2012, que tipifica a invasão de dispositivo informático**. Disponível em: <http://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html>. Acesso em: 20 abr. 2014.

GRECO, R. **Comentários sobre o crime de invasão de dispositivo informático – Art. 154-A do Código Penal**. Disponível em: <http://www.rogeriogreco.com.br/?p=2183>. Acesso em: 21 abr. 2014.

MAGGIO, V. de P. R. **Novo crime: invasão de dispositivo informático – CP, art. 154-A**. Disponível em: <http://atualidadesdodireito.com.br/vicentemaggio/2012/12/16/invasao-de-dispositivo-informatico-cp-art-154-a/>. Acesso em: 23 abr. 2014.

MENDES, G. F.; COELHO, I. M.; BRANCO, P. G. G. **Curso de direito constitucional**. São Paulo: Saraiva, 2007.

RAMOS JÚNIOR, H. S. **Invasão de dispositivo informático e a Lei 12.737/12: comentários ao art. 154-A do Código Penal Brasileiro**. Disponível em: < http://www.42jaiio.org.ar/proceedings/simposios/Trabajos/SID/09.pdf>. Acesso em: 24 abr. 2014.