Invasão de Dispositivo Informático e a Lei 12.737/12: Comentários ao art. 154-A do Código Penal Brasileiro

Hélio Santiago Ramos Júnior[1]

[1] Assistente de Procuradoria de Justiça (MPSC). Especialista em Direito Processual Civil (UNISUL). Mestre em Engenharia e Gestão do Conhecimento (UFSC), Brasil.

hsrjunior@mpsc.mp.br

Abstract. This paper research presents the violation of the data privacy on the internet by invasion of informatics device in Brazil. First, it explains how the native doctrine and jurisprudence used to deal with this illegal behavior before the existence of Federal Law number 12.737/12, known as "Carolina Dickmann Law", which included the article 154-A at the Brazilian Criminal Code to punish this invasion of informatics device as a crime. Then, it shows the most important legal and criminal aspects related to this new crime, bringing out some concepts of legal terms and expressions which were not defined by the law but are very important and discusses about some hypothetical situations that may happen in the application and practice of new criminal law. It also makes comments related to the criminal behavior of producing, offering, distribution, sale or dissemination of device or computer program in order to allow the practice the crime of invasion of informatics device, after that, it shows the hypothesis of increased punishments for these crimes, and, finally it concludes this review by pointing to some legal alternatives of interpretation to solve the difficulties of applying the new law.

Keywords: invasion of informatics device, data privacy, cybercrime, criminal law.

1 Introdução

Há uma década atrás já se dizia que a preocupação com a privacidade na *internet* tenderia cada vez mais a se ampliar justamente em decorrência do desenvolvimento de processos acelerados e mais complexos de trocas de inforações no ciberespaço.[1]

Com efeito, é nesse contexto que se insere a Lei 12.737/12, conhecida como Lei Carolina Dickmann, em referência à atriz de televisão que teve sua privacidade devassada, com a invasão de seu computador e divulgação de suas fotos íntimas na *internet*, sendo vítima da conduta que se pretende reprimir criminalmente por meio dessa nova lei, com a inserção do artigo 154-A no Código Penal Brasileiro (CP).

O novo tipo penal consiste em 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. Também configura esse delito a conduta de quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta acima descrita.

Diante deste novo cenário no qual os delitos informáticos começam a incorporar o sistema jurídico-penal, sendo expressamente referidos no art. 1º da Lei 12.737/12, torna-se interessante a análise jurídica do crime de invasão de dispositivo informático.

Assim, inicia-se o presente estudo, apresentando uma retrospectiva de como a doutrina e a jurisprudência pátria se esforçavam para encontrar algumas alternativas nas leis penais vigentes que permitissem a repressão criminal à invasão de dispositivo informático, ou seja, por meio de teses de equiparação do crime informático a outros delitos previsto no CP, como a subtração de dados ao crime de furto, a inutilização de dados do computador ao crime de dano, e, até mesmo, a tentativa de aplicação de leis penais especiais à invasão de dispositivo informático alheio, como, por exemplo, a lei da interceptação de comunicação telefônica (Lei 9.629/96) e a legislação eleitoral no tocante à invasão aos sistemas informáticos eleitorais (Leis nº 9.100/95 e 9.504/97).

Na sequência, aborda-se o crime de invasão de dispositivo informático, previsto no *caput* do art. 154-A do CP, apresentando conceitos e classificações para esse delito, assim como alguns dos principais aspectos jurídicos e criminais envolvendo esse novo crime, discutindo alguns casos hipotéticos que poderiam ocorrer e a análise sobre a possiblidade de aplicação ou não da Lei 12.737/12 às situações apresentadas.

Esse artigo também fará comentários sobre o crime de produção, oferecimento, distribuição, venda e difusão de dispositivo ou programa de computador praticado com o intuito de permitir a prática do crime do *caput* do art. 154-A do CP, ocasião em que igualmente serão apresentadas algumas problemáticas, como, por exemplo, a situação das empresas de *software* que comercializem programas de análise forense.

Após estas explanações, são apresentadas as causas de aumento de pena do crime de invasão de dispositivo informático, previstas nos §§2º a 5º do art. 154-A do CP, examinando alguns casos para averiguar se ocorrerá ou não a sua incidência.

Para finalizar esse trabalho, são apresentadas algumas alternativas jurídicas para contornar as possíveis dificuldades na aplicação da lei, especialmente no que se refere à ausência de definição legal para muitos dos novos conceitos trazidos pela Lei 12.737/12, assim como a dificuldade de se identificar o autor do delito informático no caso concreto, trazendo perspectivas de possibilidade para solução desses problemas.

2 A Invasão de Dispositivo Informático antes da Lei 12.737/12

Antes do advento da Lei 12.737/12, muito se discutiu, do ponto de vista doutrinário, sobre a possibilidade de se considerar a invasão de dispositivo informático uma conduta típica com base na legislação penal então vigente.

As teses de equiparação foram: a) da subtração de dados de um computador ao crime de furto [2] e b) da inutilização de dados do computador ao crime de dano [3], porém nenhuma delas obteve êxito quanto à sua aplicação nos tribunais.

É oportuno salientar que, a despeito de se caracterizar o crime de furto quando "o agente utiliza o acesso indevido, invadindo computadores de instituições bancárias e desviando dinheiro para outra conta" [4], nesse caso, o agente responderia pelo furto de dinheiro, e não pelo "furto" de dados do computador, que seria conduta atípica.

Assim é que surge a diferença entre delitos informáticos puros ou próprios, que são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados); e os delitos informáticos impuros ou impróprios que "já se encontram devidamente tipificados no ordenamento jurídico pátrio, uma vez que o manuseio do computador e da *Internet* é mero meio, simples codificação no *modus operandi* do delito, não implicando no delito" [5].

Também surgiu, na doutrina, uma discussão acerca da possibilidade de equiparação da invasão e obtenção de conteúdo das comunicações eletrônicas (*e-mails*) ao crime de violação de correspondência, entretanto predominou o entendimento de que o *e-mail* não pode ser considerado uma correspondência fechada, por ser vedado o uso de analogia no direito penal, inviabilizando, assim, a aplicação dessa norma penal. [4]

Em relação à jurisprudência, equiparou-se a invasão de dispositivo informático ao crime de interceptação de comunicação, previsto no art. 10 da Lei 9.629/96.

Dispõe o art. 10 da Lei 9.629/96 que: "Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei".

Com base nesse dispositivo de lei, o Tribunal de Justiça de Santa Catarina (TJSC) considerou, em um de seus julgados, como sendo penalmente típica "a conduta de quem 'invade' provedor de *internet*, apropriando-se dos *logins* e senhas de seus usuários e, assim, 'invadindo' seus computadores, os quais tinha livre e desimpedido acesso, podendo, inclusive apagar arquivos do sistema, como, de fato, o fez" [6].

Entretanto, era nítida a fragilidade dessa tese jurídica, uma vez que o conceito de interceptação pressupõe que sejam captados dados e informações de comunicação que esteja em curso, o que não é um requisito para a invasão de dispositivo informático, porque esta pode ocorrer de diversas formas, inclusive sem que haja interceptação.

A mídia já veiculou a informação de que seria possível a equiparação da invasão e modificação de páginas de órgãos públicos na *internet* aos crimes de inserção de dados falsos em sistemas de informações (artigo 313-A do CP) e de modificação ou alteração não autorizada de sistemas de informações (artigo 313-B do CP).

Entretanto, tratou-se de informação errônea, porque ambos os tipos penais citados (arts. 313-A e 313-B do CP) consistem em crimes próprios, ou seja, delitos que somente podem ser praticados por funcionário público ou, no último caso, por terceiro

em coautoria ou participação com aquele; pois, além de o terceiro invasor não ser equiparado a funcionário público, dificilmente o praticará em coautoria com este [7].

Uma vez que as eleições no país são realizadas por meio da urna eletrônica, no que se refere à invasão de sistema informático eleitoral, houve a preocupação em se tipificar condutas que porventura pudessem prejudicar a sua realização, como foi o caso da Lei nº 9.100/95 que, em seu art. 67, VII, passou a dispor sobre o crime de acesso indevido ao sistema informático eleitoral para alterar o resultado das eleições, nos seguintes termos: "obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos". A Lei nº 9.504/97 revogou, em parte, tacitamente, esse artigo, em seu art. 72, I, ao tipificar a conduta de "obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos", sendo o art. 67, inc. VII da Lei nº 9.100/95 aplicável somente aos casos de tentativa previstos nesta lei.

Acrescenta-se, ainda, no tocante à invasão e à instalação de vulnerabilidades no sistema eleitoral, a possibilidade de aplicação do art. 72, II, da Lei nº 9.504/97, que pune a conduta de "desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral".

Desta forma, pode-se dizer que em relação à invasão de dispositivo informático, apenas os sistemas eleitorais contavam com alguma tutela penal capaz de reprimir tais ilícitos informáticos, mesmo assim se desconhece a existência de algum caso concreto e prático em que houvesse a aplicação dessas normas a tais modalidades de crimes.

3 Invasão de dispositivo informático (art. 154-A, *caput*, do CP)

Conforme acima demonstrado, mesmo antes do advento da tipificação do crime de invasão de dispositivo informático, a doutrina e a jurisprudência já consideravam reprovável e merecedora de reprimenda penal a conduta antiética do agente que invade computador alheio, sem autorização, para fins ilícitos.

A justificativa do projeto que deu origem a essa lei esclarece que o seu objetivo é "oferecer à sociedade uma alternativa equilibrada de repressão a condutas socialmente consideradas como indesejáveis, sem no entanto operar a criminalização excessiva e demasiado aberta que permitiria considerar todo e qualquer cidadão como um potencial criminoso em seu uso cotidiano da rede mundial de computadores".

A Lei 12.737/12 já se encontra em pleno vigor, desde o início do mês de abril do ano corrente (2013), porém não definiu o que se entende por "dispositivo informático" para efeitos penais, o que não deverá ser óbice algum à sua aplicação.

Pode-se, no entanto, conceituar dispositivo informático, para fins de aplicação da lei penal, como qualquer dispositivo capaz de armazenar dados, informações e documentos em meio digital, independentemente do modo de seu funcionamento, que pode ser utilizado para se conectar a um computador ou a uma rede, tais como: computadores, *notebooks*, *netbooks*, *laptops*, *tablets*, *smartphones*, *iphones*, *ipads* etc.

O crime previsto no *caput* do art. 154-A do CP 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. A pena cominada para esse delito é de detenção, de 3 (três) meses a 1 (um) ano, e multa.

Embora possa ser considerado como um delito de alta tecnologia, é crime de menor potencial ofensivo, pois, como se vê, a sua pena máxima é inferior a dois anos.

Trata-se de crime comum, que pode ser praticado por qualquer pessoa, pois a lei não exige nenhuma qualidade ou condição especial do agente. Assim, não é preciso provar que o autor do delito seja um *hacker* invasor, detentor de habilidades especiais.

Um *hacker* pode ser definido como o indivíduo que detém certos conhecimentos como a prática de invadir e acessar sistemas não autorizados, independentemente da finalidade ou não de causar um dano ou obter vantagem indevida. O fato de ter esses conhecimentos, não significa necessariamente que irá utilizá-los para cometer delitos. Assim, é possível fazer a distinção entre o *hacker* ético e o invasor. [8]

Hacker ético, como o próprio nome sugere, é aquele que utiliza tais conhecimentos para fins lícitos, podendo auxiliar no trabalho da perícia forense ou na segurança dos sistemas de informações de empresas, fazendo testes de segurança, desde que devidamente autorizados. Ao contrário, o *hacker* invasor é aquele que emprega as suas habilidades para fins ilícitos, como, por exemplo, para a prática do crime de invasão de dispositivo informático.

O delito em questão é crime formal, isso implica dizer que, mesmo que o agente não consiga obter, adulterar ou destruir dados ou informações com a invasão, ou obter vantagem ilícita com a instalação de vulnerabilidades, ainda assim há consumação do delito, o qual independe de se alcançar ou não o resultado previsto no tipo penal.

Uma vez que se trata de crime doloso, somente é punível quando o agente quis o resultado ou assumiu o risco de produzi-lo, pois não se admite a modalidade culposa. Entretanto, para caracterizar o delito, necessária é a presença do dolo específico, ou seja, no caso da invasão de dispositivo informático alheio, a intenção do agente deve ser a obtenção, a adulteração ou a destruição de dados ou informações; e, em relação à instalação de vulnerabilidades, seu intuito deve ser a obtenção de vantagem ilícita.

A invasão de dispositivo informático é um crime instantâneo, tendo em vista que o delito se configura no exato momento em que o agente consegue invadir o sistema, sendo irrelevante que o dispositivo esteja ou não conectado à *internet*.

A consumação do delito pode ocorrer nos casos de dispositivos que funcionem por computação em nuvem (*cloud computing*) quando, por exemplo, a intenção for a de obter acesso a dados e informações, pois o tipo penal não exige que os dados que se pretende obter se encontrem armazenados no disco rígido do computador do próprio usuário, sendo irrelevante que estejam em um computador remoto ou no *hardware* de terceiros.

Idêntico raciocínio pode ser aplicado em relação aos provedores de serviços de armazenamento *online* de dados, que também funcionam por computação em nuvem.

Assim, o que importa é que a invasão seja feita em um dispositivo informático alheio, sem autorização, mediante violação indevida de mecanismo de segurança e com o fim de se obter dados e informações, sendo suficiente o seu acesso, pois não é necessário fazer cópia ou *download* do arquivo para obter esses dados e informações.

Interessante questão é saber se seria típica ou não a conduta do *hacker* que invade dispositivo informático alheio, com violação indevida de mecanismo de segurança, sem autorização expressa ou tácita do titular do dispositivo, com o único propósito de alertar o seu proprietário quanto às falhas de segurança.

Nesse caso, não seria possível qualificar o *hacker* como ético, pois, ainda que a sua intenção não seja causar dano ou prejuízo a outrem, ele não estará utilizando os seus conhecimentos para fins lícitos, caso não possua autorização para invadir sistema ou dispositivo informático alheio, pois se o invasão é ilegal, a sua conduta é ilícita. Ao invadir o sistema sem autorização, o invasor assumiu o risco de produzir o resultado.

O simples fato de se invadir dispositivo informático alheio, com violação indevida de mecanismo de segurança e sem autorização já revela que o invasor tem a intenção de obter acesso não autorizado, o que, em tese, é suficiente para a consumação desse delito, mesmo porque é irrelevante que haja a obtenção, adulteração ou destruição de dados ou informações, justamente por se trata de um crime formal.

Portanto, na hipótese acima apresentada, entende-se que o *hacker* é considerado um invasor e a sua conduta é penalmente típica, podendo ser responsabilizado pelo crime de invasão de dispositivo informático previsto no art. 154-A, *caput*, do CP.

Do ponto de vista jurídico, entende-se que a única forma de não responsabilizar o *hacker* invasor por esse delito informático, seria demonstrar que ele tinha autorização do titular do dispositivo para realizá-la, ou, então, provar que não houve invasão, mas sim acesso indevido ao dispositivo que não tinha nenhum mecanismo de segurança.

Por mecanismo de segurança, pode-se entender qualquer mecanismo, solução ou alternativa computacional destinada a proteger o dispositivo informático contra qualquer espécie de ameaça à segurança de dados e informações nele armazenadas.

Observa-se que nem sempre o acesso não autorizado a sistemas computacionais irá caracterizar o crime de invasão de dispositivo informático. Isso porque, para que haja a consumação desse delito, torna-se imprescindível que ocorra invasão ao dispositivo informático, com a violação indevida do mecanismo de segurança e sem autorização.

O crime de invasão do dispositivo informático pressupõe a violação indevida do seu mecanismo de segurança. Esse mecanismo de segurança pode ser perfeitamente uma senha, pois a lei não faz distinção entre os diferentes tipos de mecanismos de segurança e nem especifica qual o grau de proteção que o dispositivo deve ter.

A admissibilidade da senha como mecanismo de segurança não implica reconhecer que o dispositivo esteja totalmente protegido, basta que tenha proteção e que esta seja justamente violável, pois se o dispositivo informático estivesse protegido a ponto de o seu mecanismo de segurança ser inviolável, seria impossível a consumação do delito.

O mecanismo de segurança do dispositivo informático também pode ser um anti-vírus, que detecta, bloqueia as ameaças e impede a instalação de códigos maliciosos. Nota-se que o tipo penal não exige, como condição elementar para a sua consumação, que o mecanismo de segurança (no caso, o anti-vírus) seja atualizado e muito menos que a vítima utilize o mecanismo de segurança mais moderno e eficiente que existe.

Caso a vítima não mantenha o seu mecanismo de segurança atualizado, ela estará desprotegida do ponto de vista técnico, porém isso não significa dizer que o usuário se encontra desprovido da proteção jurídico-penal prevista no art. 154-A, *caput*, do CP.

Assim, em tese, é possível que haja a consumação do delito ainda que o anti-vírus esteja desatualizado e não consiga detectar ou bloquear a invasão ao computador, pois

a norma penal se refere apenas à violação indevida de mecanismo de segurança e não dispõe sobre a obrigatoriedade da vítima manter o seu sistema de proteção atualizado.

Em relação ao anti-vírus como mecanismo de segurança, é importante dizer que, mesmo que ele esteja atualizado, não consegue detectar todas as ameaças. Assim, o fato de não ter bloqueado uma invasão não significa dizer que ele não funcionou ou que não esteja funcionando, mas, simplesmente, não foi eficaz em bloquear o ataque.

Portanto, se durante uma invasão a dispositivo informático alheio, sem autorização, o mecanismo de segurança "não funcionar" no momento da invasão, isso só será relevante se o não funcionamento ocorreu porque o sistema de proteção não estava ativado, caso contrário haverá invasão, porque o *hacker* conseguiu invadir o sistema, mesmo com o mecanismo de segurança estando ativado, portanto, deve-se concluir que houve violação a esse sistema de proteção, caracterizando, assim, o delito.

Não se deve confundir de forma alguma a proteção jurídica com a proteção técnica, pois aquela pressupõe exatamente a falibilidade da técnica para a sua aplicação, já que os crimes informáticos ocorrem por erros humanos ou falhas na proteção do sistema, pois o *hacker* obtém êxito na invasão porque explora as suas vulnerabilidades. Caso assim não fosse, se esses fatores não existissem, a tecnologia certamente resolveria sozinha essse problema e não haveria necessidade de leis para punir delitos dessa natureza, os quais seriam considerados crimes informáticos impossíveis.

Reconhece-se que "a tecnologia pode contribuir para proporcionar uma maior eficácia da lei, na medida em que cria mecanismos técnicos que podem auxiliar na tarefa de coibir a prática de comportamentos proibidos pela legislação vigente" [9].

Com a tipificação do crime de invasão de dispositivo informático, a criação de mecanismos de segurança é um exemplo desse tipo de contribuição da tecnologia para uma maior eficácia da lei, porém não ela supre a necessidade da proteção jurídica, de modo que se pode dizer que ambas as "espécies" de proteção se complementam.

É importante mencionar que, especialmente em se tratando de crimes informáticos, toda análise da aplicação da lei penal deve ser feita com base no caso concreto, pois, na maioria das vezes, dependerá de um laudo pericial para constatar se houve invasão, portanto as suas peculiaridades é que irão definir a tipicidade ou não do delito.

4 Produção, oferecimento, distribuição, venda ou difusão de dispositivo ou programa de computador (art. 154-A, §1, do CP)

Conforme dispõe o art. 154-A, §1º, do CP, o agente que produz, oferece, distribui, vende ou dinfude dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput* desse artigo, incorre na mesma pena prevista para esse delito, ou seja, detenção, de 3 (três) meses a 1 (um) ano, e multa.

Se o alcance do conceito de "dispositivo informático" para fins penais é algo que ainda não está perfeitamente delimitado, o memo não ocorre em relação ao "programa de computador", cuja definição jurídica está expressamente prevista na lei.

Nos termos do art. 1º da Lei 9.609/98, tem-se o conceito legal de programa de computador: "é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos,

instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados".

A tipificação penal da conduta de quem produz, oferece, distribui e vende ou difunde dispositivo ou programa de computador com o intuito de permitir a invasão de dispositivo informático não se trata aqui de hipótese de responsabilidade objetiva.

Em outras palavras, o produtor do dispositivo ou do programa de computador não será responsável pelo simples fato de produzi-lo, a não ser que o tenha feito com a intenção de permitir a prática do crime de invasão de dispositivo informático.

Somente haverá consumação desse delito quando estiver provado que a intenção daquele que produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador é permitir a prática do delito previsto no *caput* do art. 154-A do CP.

Assim, para a consumação desse crime, não basta a simples comprovação de que o dispositivo ou programa de computador permite a prática da conduta criminosa vedada, devendo demonstrar, por exemplo, que ao produzi-lo, a sua intenção era que ele fosse utilizado para permitir a invasão de dispositivo alheio, mediante violação indevida de mecanismo de segurança, sem autorização expressa ou tácita do titular do dispositivo, ou instalar vulnerabilidades, caso contrário não haverá crime.

O objetivo do tipo penal não é criminalizar a conduta das empresas de *software* que desenvolvem programas de computador para auxiliar no trabalho da perícia forense ou na segurança dos sistemas de informações de empresas, mas, ao contrário, é coibir a conduta daqueles que produzem, oferecem, distribuem, vendem ou difundem tais programas com o objetivo de permitir a prática da conduta criminosa ora combatida.

Ainda que o verbo "disponibilizar" não esteja previsto no §1º do art. 154-A do CP, um *hacker* que disponibiliza em sua página na *internet* esses programas que permitem a realização de testes de segurança por meio de invasão de computadores, poderá, em tese, estar cometendo o crime, na modalidade de "oferecer", caso ali exponha e oferte o uso dessas ferramentas e se possa concluir, pelo teor do próprio *site*, que a sua intenção seja a de permitir a prática do crime de invasão de dispositivo informático.

Se esse programa for um vírus de computador que seja hábil a invadir dispositivo informático alheio ou instalar vulnerabilidades, deverá haver inversão do ônus da prova, ou seja, haverá presunção de que a intenção do agente é realmente a prática da conduta criminosa, admitindo-se, porém, a produção de prova em sentido contrário.

Registra-se que, embora já tipificada a conduta de "distribuir" dispositivo ou programa de computador com o fim de permitir a prática do crime de invasão de dispositivo informático, inseriu-se ainda o verbo "difundir" no tipo penal do §1º do art. 154-A do CP. Logo, não há dúvidas quanto à tipicidade da conduta do agente que distribui ou difunde vírus de computador, *trojans* (cavalo de tróia) ou qualquer outro código malicioso capaz de permitir a prática do crime previsto no *caput* desse artigo.

4 Causas de aumento de pena

As causas de aumento de pena estão previstas nos §§2 a 5º do art. 154-A do CP e serão, a seguir, comentadas.

4.1 Invasão que resulta em prejuízo econômico (art. 154-A, §2º do CP)

Caso a invasão resulte em prejuízo econômico, a pena será aumentada de um sexto a um terço, conforme prevê o §2º do art. 154-A do CP. Assim, para que haja o crime, não é necessário que ocorra dano patrimonial, mas se esse ocorrer, a pena é majorada.

Não há dúvidas quanto aos prejuízos econômicos que a invasão de dispositivo informático poderá causar às vítimas. Em relação às empresas, estas, em geral, não divulgam a informação de que seus sistemas foram invadidos, porque sabem que isso repercute negativamente, pois prejudicará não só a sua imagem no mercado, como também afastará a sua clientela, gerando-lhe prováveis problemas financeiros.

No caso acima mencionado, poder-se-ia argumentar que não teria sido a invasão que resultou no prejuízo econômico da empresa, mas sim a sua publicidade. Nesse aspecto, a causa de aumento incidiria ao se constatar que o invasor, com a simples prática do delito, deu publicidade a essa invasão, seja com a obtenção, adulteração ou destruição dos dados da empresa. Para que isso ocorra, deve haver prova do prejuízo econômico e do nexo de causalidade entre este e a invasão e a publicidade desta.

Essa causa de aumento de pena só tem aplicação quando o prejuízo econômico é consequência direta da invasão de dispositivo informático e não quando a invasão for o meio utilizado pelo agente para praticar um crime contra o patrimônio por meio da *internet*, hipótese em que poderá haver concurso material.

Assim, o prejuízo econômico decore da própria invasão ao dispositivo informático, como, por exemplo, no caso de terem sido adulterados ou destruídos dados ou informações armazenadas no computador da vítima, causando-lhe dano patrimonial.

Na hipótese do §2º, o *hacker* invasor não age com a intenção de obter vantagem econômica indevida em prejuízo da vítima – embora, na prática, acabe causando lesão ao patrimônio desta – mas, sim, atua com a finalidade de obter, adulterar ou destruir dados ou informações armazenadas no dispositivo informático alheio no caso de sua invasão, ou, então, para obter vantagem ilícita no caso de instalação de vulnerabilidades, desde que esta vantagem não seja de natureza patrimonial.

Desta forma, cumpre frisar que a lei penal não teve a finalidade de punir de forma mais branda os crimes patrimoniais de furto e de estelionado cometidos por meio informático, ao contrário, eles continuarão, em tese, a ser punidos da mesma forma, pois o crime do art. 154-A do CP é crime contra a pessoa, e não contra o patrimônio.

Esse delito está inserido na Seção IV "Dos crimes contra a inviolabilidade dos segredos", do Capítulo VI "Dos Crimes contra a liberdade individual", do Título I "Dos crimes contra a pessoa". Assim, a despeito de o art. 154-A do CP ser um delito informático, o bem jurídico tutelado não é o dispositivo informático, mas sim a inviolabilidade dos dados e informações pessoais armazenadas em meio informático.

Portanto, a única diferença agora é que o *hacker* que invadir computador alheio para obter dados e, em seguida, subtrair dinheiro de contas bancárias da vítima, poderá responder por dois delitos autônomos em concurso material, por atingir bens jurídicos diversos, não havendo de se falar em subsidiariedade, porque se faz presente o dolo de ambos os delitos, os quais, inclusive, são realizados em momentos distintos.

4.2 Invasão que resulta na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas ou controle remoto não autorizado (art. 154-A, §3º, CP)

Prevê o §3º do art. 154-A do CP que, se a invasão resulta na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas ou controle remoto não autorizado, a pena é de reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

Observa-se que, mesmo com a aplicação do dobro da pena para a hipótese do §3º desse artigo, o crime continua sendo de menor potencial ofensivo, uma vez que a pena máxima do delito não é superior a dois anos, nos termos do art. 61 da Lei 9.099/95.

Para que haja a obtenção de dados e informações, especialmente no que se refere ao conteúdo de comunicações eletrônicas privadas, não é necessário que esse dados sejam transferidos em meio digital para o computador do *hacker* invasor e nem que sejam impressos em papel para materializá-los, desde que existam provas que revelem que o invasor leu o conteúdo dos *logs* ou que conseguiu acessar arquivos nos quais estavam armazenados os históricos das comunicações eletrônicas privadas da vítima.

No que se refere à obtenção de segredos comerciais ou industriais, aplica-se, em regra, o mesmo entendimento, basta acessar os dados, não sendo necessário copiá-los. Isso porque o simples acesso permite a obtenção do seu conteúdo com a sua leitura. De qualquer forma, para aplicação desta causa de aumento deverão haver provas de que o invasor obteve o conteúdo dos segredos comerciais ou industriais, por meio da invasão de dispositivo informático, com o acesso aos respectivos documentos.

O crime de invasão de dispostivo informático também terá a sua pena aumentada caso o *hacker* invasor obtenha o controle remoto não autorizado do dispositivo informático invadido. Sobre esta forma de invasão, esclarece-se que "o acesso remoto é o método mais comum de invasão de sistemas computacionais. Não há qualquer contato físico do pirata com o computador invadido e o computador no qual o agente emite os comandos de acesso é diferente daquele em que os dados estão armazenados. O acesso se dá através de uma rede que, na maioria absoluta das vezes, é a *Internet*" [10].

O tipo penal previsto no *caput* estabelece que há crime quando a invasão ocorre sem autorização expressa ou tácita do titular do dispositivo, assim cumpre analisar se estaria caracterizado o delito na hipótese em que é o próprio usuário quem acessa, por inadvertência, um *malware* (código malicioso) que libera o acesso ao seu dispositivo.

A despeito de já configurar o delito previsto no §1º do art. 154-A do CP a simples conduta de distribuir e difundir dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput* desse artigo, nas hipóteses em que o usuário é induzido em erro a acessar determinado código malicioso que permita o controle remoto do seu dispositivo, incide essa causa de aumento prevista no seu §3º.

Em regra, o crime de invasão de dispositivo informático é um delito comissivo, que pressupõe que haja uma ação por parte do agente. Entretanto, em tese, poderá ocorrer situações em que haja responsabilização penal do agente nos casos de omissão penalmente relevante do titular do dispositivo invadido que tem ciência dessa invasão e que, com o seu comportamento anterior, criou o risco da ocorrência do resultado.

Entende-se que, se o *hacker* invasor, após a invasão, utilizar o controle remoto não autorizado de dispositivo informático para praticar novos delitos do art. 154-A, *caput*,

do CP, o invasor responderá pelo crime, inclusive, em continuidade delitiva, dependendo do caso concreto. Quanto ao titular do dispositivo informático invadido, ele não será responsabilizado criminalmente, exceto se for demonstrado que ele estava ciente da invasão e do controle remoto do seu computador e não tomou nenhuma providência, aderindo à prática criminosa e assumindo o risco do resultado, por permitir ou tolerar que o seu dispositivo informático fizesse parte de uma *botnet* [11], comumente utilizada por esses invasores para praticar delitos informáticos.

4.3 Divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos (art. 154-A, §4º, CP)

A preocupação com a comercialização ilegal de dados e informações pessoais armazenadas em dispositivos informáticos não é algo recente, ela já existia há mais dez anos atrás. Alertava-se que seria "um fator de preocupação a possibilidade de se comercializar informações particulares do usuário que é obtida pela empresa que as solicita de modo que deve se ter o cuidado com o armazenamento dos dados como as informações pessoais dos clientes, seus perfis e endereços eletrônicos" [1].

Caso o criminoso, após invadir o dispositivo informático alheio e obter o conteúdo de comunicações eletrônicas privadas, de segredos comerciais ou industriais ou de informações sigilosas, realize a divulgação, a comercialização ou a transmissão a terceiros, a qualquer título, dos dados e informações obtidos, incidirá a causa de aumento de pena de um a dois terços, conforme previsto no §4º do art. 154-A do CP.

A Lei 12.737/12 não revogou o §1º-A do art. 153 do CP, inserido pela Lei 9.983/00, de modo que continua em vigor esse delito, o qual consiste em "divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública", hipótese em que a pena é de detenção, de 1 (um) a 4 (quatro) anos, e multa.

A diferença é que, na hipótese do tipo penal previsto no art. 153, §1º-A do CP, tutela-se apenas as informações sigilosas e reservadas da Administração Pública, que devem assim estar expressamente definidas em lei, enquanto que o art. 154-A, §4º do CP se aplica aos dados e informações armazenados em dispositivo, seja de órgãos públicos ou privados, aplicando-se a pessoas físicas ou jurídicas, e, além de prever a sua divulgação, também considera crime a comercialização e a transmissão desses dados e informações, desde que a sua obtenção tenha ocorrido por meio do crime do *caput* do art. 154-A do CP*,* funcionando como causa de aumento de pena desse delito.

4.4 Invasão praticada contra pessoas específicas (art. 154-A, §5º, CP)

Estabelece o §5º do art. 154-A do CP que a pena será aumentada de um terço à metade se crime for praticado contra o Presidente da República, os governadores eos prefeitos (inciso I); contra o Presidente do Supremo Tribunal Federal (inciso II); o Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal (inciso III); ou contra o dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal (inciso IV).

5 Dificuldades e perspectivas com a aplicação da nova lei penal

Pretende-se aqui comentar possíveis dificuldades na aplicação da nova lei que inseriu a invasão de dispositivo informático alheio como crime no Código Penal Brasileiro, assim como apontar soluções jurídicas para estas questões advindas com a tipificação do crime de invasão de dispositivo informático.

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.

Também é importante afastar a ideia de que haveria autorização tácita no caso de o titular do dispositivo informático, induzido a erro por engenharia social, acessar dispositivo ou programa de computador que permita o acesso e controle remoto do seu computador, pois a manifestação de vontade nesse caso estará totalmente viciada e comprometida, uma vez que o usuário não pode autorizar algo do qual nem sequer tem conhecimento.

A autorização tácita ocorre na hipótese em que o silêncio importa em anuência, quando as circunstâncias ou os usos o autorizarem, e não for necessária a declaração de vontade expressa, nos termos do art. 111 do Código Civil. Pode ocorrer, por exemplo, quando há contratação de profissional da segurança da informação para realizar "testes de segurança" na rede de computadores da empresa do titular do dispositivo e, embora não conste no contrato autorização expressa para "invadir" tais computadores, tal anuência seja presumida pela natureza do próprio contrato.

Outro aspecto importante diz respeito ao conceito de invasão, o qual não pode ficar adstrito às hipóteses em que ocorram um "ataque" ao dispositivo informático alheio. Assim, para efeitos penais, deve-se entender que há invasão sempre que alguém tenta violar indevidamente e burlar o mecanismo de segurança do dispositivo informático.

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.

Assim, o perito forense, ao ser nomeado para verificar a ocorrência da invasão ao dispositivo informático, deverá verificar não só se houve um "ataque" ao computador, mas também se houve violação indevida ou burla a algum mecanismo de segurança, pois o fato de conseguir ultrapassar o mecanismo de segurança mediante o uso de algum artifício fraudulento implica inegavelmente a sua violação, ainda que para isso tenha colaborado a ocorrência de erros humanos ou de falhas de segurança.

Nesse aspecto, enfatiza-se que o tipo penal, embora exija violação indevida ao mecanismo de segurança, não condiciona a tutela penal ao fato de se considerar o titular do dispositivo informático "protegido" ou "desprotegido", basta apenas que tenha proteção (mecanismo de segurança) e que esta seja violada no caso concreto.

Isso porque ninguém está totalmente protegido na *internet*, e a lei não estabeleceu nenhum grau de proteção que o mecanismo de segurança deve ter como condição para consumação do delito, mas, cumpre reforçar, exige, a lei, apenas que o dispositivo informático tenha algum mecanismo de segurança e que este seja violado.

Desta forma, entende-se que, se o mecanismo de proteção for um anti-vírus, embora seja recomendável que este se mantenha atualizado, não faz sentido algum afastar a tipicidade do delito apenas porque a vítima não estava com o seu anti-vírus atualizado, pois em direito penal não existe compensação de culpas, assim, a culpa concorrente vítima não afasta a tipicidade do crime do art. 154-A, *caput*, do CP.

Enfatiza-se que o crime ocorre justamente porque o invasor explora as fragilidades do sistema, mesmo porque, conforme já mencionado, se o mecanismo de segurança do dispositivo informático fosse inviolável, o crime seria impossível.

Nem sempre o conceito jurídico coincidirá com o conceito computacional, porém, em se tratando de aplicação do direito ao caso concreto, deve prevalecer o conceito jurídico, como é o caso do programa de computador que é definido pela própria lei, não sendo necessário que tal conceito seja o mesmo dado pela ciência da computação.

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, infere-se que poderão ser consideradas como "vulnerabilidades" para fins de aplicação da lei penal, os vírus de computador, *trojans*, *keyloggers* dentre outros, pois, por questão de lógica, depreende-se ser esta a finalidade do legislador penal.

Em regra, não haverá crime nos casos de instalação de *cookies* no computador do usuário, pois estes geralmente são "instalados" automaticamente pelo computador quando se acessa a página na *internet* e embora possam conter dados da navegação e outros fornecidos pelo usuário, os *browsers* (programas de navegação na *internet*)

costumam fornecer ao internauta a opção de exclusão desses arquivos do computador. Caso houvesse delito, poder-se-ia aplicar, nesse caso, o princípio da insignificância.

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, costuma-se 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.

No Brasil, com a pretensão de se regulamentar o uso da *internet*, há uma tendência em se exigir dos estabelecimentos comerciais que forneçam serviços de acesso à *internet*, como as *lan houses*, que realizam o cadastro dos dados de seus usuários, registrando a data e o horário da navegação, como alternativa para tornar viável a responsabilização penal de quem praticar o delito nesses estabelecimentos.

Em Santa Catarina, a Lei Estadual 14.890/09 disciplina o controle de usuários em estabelecimentos voltados à comercialização do acesso a *internet* no âmbito estadual, inclusive determinando que os referidos estabelecimentos deverão adotar sistema de monitoramento por câmeras de vigilância, em especial nos acessos aos computadores. O mesmo também já vem ocorrendo em diversos outros estados da federação.

Essa lei estadual prevê, em seu art. 2º, que os estabelecimentos deverão manter o cadastro de usuários pelo prazo de dois anos, contendo informações como o tipo e o número do documento de identidade com foto apresentado, o endereço e o telefone, o equipamento usado, bem como os horários do início e do término de sua utilização e o Protocolo Internet - IP - do equipamento usado.

Finalmente, com, a obtenção desses dados, torna-se possível a identificação da autoria do crime, que, associada à constatação da materialidade do delito, com o apoio da perícia forense, faz com que estejam presentes as condições para a instauração de inquérito policial destinado a apurar a responsabilidade criminal do autor do delito de invasão de dispositivo informático, previsto no art. 154-A do CP,

Referências

1. Ramos Júnior, H. S. Considerações sobre a privacidade no espaço cibernético. In: II Ciberética. Simpósio Internacional de Propriedade Intelectual. Florianópolis, 2003.
2. Brandão, E. A. A Invasão de Computadores no Brasil – Crime de Furto. In: Opice Blum, R. M. S.; Bruno, M. G. S.; Abrusio, J. C. Manual de Direito Eletrônico e Internet.São Paulo: Lex Editora, 2006. p. 79-83.
3. Vianna, T. L. Do delito de dano e de sua aplicação ao Direito Penal informático. In: Revista dos Tribunais, São Paulo, a. 92, n. 807, janeiro de 2003. p. 486-492.
4. Ramos Junior, H. S.: Estudo sobre a Aplicabilidade das Leis Penais aos Crimes Informáticos no Brasil. In: The Third International Conference of Forensic Computer Science. ISSN 1980-1114. v. 3. n.1. 2008. p. 41.
5. Meira, J. C. J. A tutela penal dos cybercrimes e o projeto de lei contra os crimes de informática. In: Revista da Fundação Escola Superior do Ministério Público do Distrito Federal e Territórios. Brasília, v.15, p. 117-159, dez/2007.

6. Brasil. Tribunal de Justiça de Santa Catarina. Apelação Criminal n. 2007.006842-9, Rel. Des. Irineu João da Silva, julgado em 22/05/2007. Disponível em: <http://www.tjsc.jus.br>.
7. Ramos Junior, H. S.: Crimes contra a Segurança dos Sistemas de Informações da Administração Pública. In: Proceeding of the International Conference of Forensic Computer Science. Guarujá: ABEAT, 2007. v. 2. p. 64-69.
8. Foina, A. G. Uma sociologia dos hackers: aspectos relevantes para o combate aos delitos informáticos no contexto brasileiro. In: Anais da I Conferência Internacional de Perícias em Crimes Cibernéticos. Brasília: Departamento de Polícia Federal, 2004.
9. Ramos Junior, H. S. Questões legais do uso da certificação digital na proteção dos direitos de autor de programa de computador. In: Proceeding of the International Conference of Forensic Computer Science. Brasília: Departamento de Polícia Federal, 2006. v. 1. p. 43-50.
10. Vianna, T. L. Fundamentos do Direito Penal Informático: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003. p. 76.
11. Ianelli, N; Hackworth, A. Botnet as a Vehicle for Online Crimes. In: Proceeding of the International Conference of Forensic Computer Science. Brasília: Departamento de Polícia Federal, 2006.