A (IN)EFICÁCIA NORMATIVA DO CRIME DE INVASÃO DE DISPOSITIVO INFORMÁTICO

Guilherme Anderson Caneppele[1]

RESUMO: Este artigo tem como objetivo analisar a (in)eficácia do crime de invasão de dispositivo informático, introduzido no Brasil pela Lei 12.737/2012. Trata-se de pesquisa qualitativa, realizada por meio de método dedutivo e de procedimento técnico bibliográfico e documental. As reflexões acerca do tema iniciam pela abordagem dos crimes cibernéticos no Brasil através de relato histórico, identificando aspectos da legislação penal pertinentes. Ainda, examina, com base nos princípios, doutrina e decisões jurisprudenciais, a (in)eficácia desse tipo de crime. Nesse sentido, conclui que a tipificação do crime em questão é ineficaz, tendo em vista que não atingiu a finalidade de prevenir e reprimir a incidência desse tipo de delito, ante a deficiente tipicidade formal que impede a sua adequação típica.

PALAVRAS-CHAVE: Direito Penal. Crimes cibernéticos. Adequação típica. (In)eficácia. Invasão de dispositivo informático.

1 INTRODUÇÃO

A comunicação e a troca de informações sofreram inegáveis mudanças nos últimos tempos, tendo sido radicalmente transformadas para possibilitar a interação de pessoas ao redor do mundo quase que instantaneamente, para o compartilhamento de dados pessoais, profissionais ou de qualquer natureza.

[1] Bacharel em Direito pelo Centro Universitário UNIVATES, de Lajeado/RS. Advogado. gcaneppeleadv@gmail.com

O assunto em questão é de suma importância na sociedade contemporânea, considerando as diversas transformações que o mundo atravessa, especialmente com a evolução tecnológica do século XXI. Não se pode olvidar os inúmeros benefícios trazidos pela tecnologia, especialmente a internet, que conseguiu a façanha de encurtar espaços e dinamizar a comunicação no mundo todo.

Em contrapartida, abriu-se um novo espaço para o cometimento de delitos, chamados crimes cibernéticos, os quais ainda carecem de regulamentação no nosso país, conforme restará demonstrado ao decorrer do texto.

O Direito Penal, exercido sob o monopólio do Estado, regula as relações dos indivíduos em sociedade e as relações destes com a mesma sociedade através da *persecutio criminis*, que somente pode ser desempenhada de acordo com normas preestabelecidas. Com efeito, para acompanhar a evolução da sociedade, essas normas precisam ser atualizadas com o surgimento de novas condutas, sob pena de o controle social ficar desamparado.

A falta de regulamentação faz com que um fato seja atípico, tendo em vista que não existe crime sem prévia previsão legal, ficando o Estado impossibilitado de punir tal conduta. Por isso, diante da riqueza de dados e informações pessoais e profissionais, geralmente guardados em dispositivos informáticos, e da relevância desse bem jurídico, que se tornou alvo dos criminosos, justifica-se pertinente discutir a (in)eficácia normativa do crime de invasão de dispositivo informático, introduzido no Brasil pela Lei n. 12.737/2012, objetivo geral deste artigo. O estudo discute como problema: a tipificação do crime de invasão de dispositivo informático, introduzida no Código Penal pela Lei 12.737/2012, é eficaz? Como uma possível hipótese para tal questionamento, entende-se que o tipo penal crime de invasão de dispositivo informático não é eficaz, pois não atingiu a sua finalidade de prevenir e reprimir este tipo de delito, tendo em vista que a lei que introduziu o artigo em questão no Código Penal foi editada às pressas, em razão do clamor social pela divulgação das fotos íntimas da atriz Carolina Dieckmann, resultando na imperfeição técnica dos legisladores e, por conseguinte, na impossibilidade de adequação típica do fato à norma, restando ineficaz o crime em questão.

A investigação acadêmica, quanto à abordagem, será qualitativa, tendo como característica o aprofundamento no contexto estudado e a perspectiva interpretativa desses possíveis dados para a realidade, confor-

me esclarecem Mezzaroba e Monteiro (2009). Para obter a finalidade desejada pelo estudo, será empregado o método dedutivo, cuja operacionalização se dará por meio de procedimentos técnicos baseados na doutrina, legislação e jurisprudência, relacionados, inicialmente, pela abordagem dos crimes cibernéticos no Brasil através de relato histórico e pelo exame da legislação vigente, até chegar ao foco principal do trabalho, o exame da (in)eficácia do crime de invasão de dispositivo informático.

2 BREVE ABORDAGEM SOBRE OS CRIMES CIBERNÉTICOS NO BRASIL E A LEI N. 12.737/2012

A modernidade, especialmente após o século passado, trouxe consigo inúmeras transformações devido ao avanço da tecnologia. A internet, por exemplo, revolucionou o modo de comunicação das pessoas e a transmissão de dados e informações, encurtando espaços. Contudo, juntamente com os benefícios, sobrevieram novos meios e caminhos para o cometimento de delitos, notadamente os crimes cibernéticos. Esses crimes, por se constituírem em uma nova forma de execução, apresentam características peculiares e demandam adequações da legislação para que o Estado possa exercer legalmente o seu jus puniendi sem cometer abusos.

Dessa forma, faz-se necessário que o ordenamento jurídico acompanhe essas transformações que alteram significantemente o mundo, com o fim de regular as novas relações proporcionadas por estes meios, uma vez que esses inúmeros avanços trouxeram consigo novas práticas e novas organizações de infrações penais. Assim, é objetivo desta seção descrever relato histórico a respeito da internet e crimes cibernéticos e sua legislação.

2.1 RELATO HISTÓRICO DA INTERNET NO MUNDO E NO BRASIL

Com a internet sendo utilizada como novo meio de comunicação e interação, surgiu também um novo ambiente que mantém o sistema em funcionamento, o virtual. Contudo, juntamente com os benefícios, a internet trouxe malefícios, tendo se tornado um local para o cometimento de novos delitos, chamados crimes cibernéticos. A internet, como explica Ross *apud* Colli (2010, p. 32), "é uma rede mundial de computadores composta pela interligação de uma ou mais redes remotas ou locais ao redor do planeta".

O seu surgimento é fruto do investimento militar dos Estados Unidos em resposta ao programa *Sputnik* da extinta União Soviética. Assevera Col-

li (2010) que a corrida entre as duas nações fez com que a primeira criasse uma agência destinada ao desenvolvimento de pesquisas militares, denominada Arpa *(Advanced Research Projects Agency)*. Diante do interesse dessa agência no desenvolvimento de tecnologias da computação, surgiu a primeira rede de transmissão de dados entre computadores, chamada *Arpanet*. Inicialmente de domínio militar, no ano de 1969 passou a ingressar no campo acadêmico, para, após, por meio da intercomunicação entre computadores de diferentes universidades, a rede fosse expandida para os chamados *Personal Commputers* (PC).

Ainda, no ano de 1986, foi implementada a NSFNET, pela *National Science Foundation*, e a *Arpanet* passou a ser chamada de internet. Para que ocorresse o grande salto na utilização da internet, foi crucial a criação da *World Wide Web* pelos engenheiros Robert Caillaiu e Tim Berners-Lee, transformando a internet num sistema mundial público, de redes de computadores (DAVID *apud* WENDT; JORGE, 2013).

Com relação ao Brasil, a história da internet remonta ao ano de 1988 e tem como precursoras duas entidades ligadas às pesquisas acadêmicas: o Laboratório Nacional de Computação Científica do CNPq e a Fapesp. O Laboratório alugou, em 1988, uma linha da empresa Embratel e construiu um link com a rede americana de computadores *Bitnet*. Segundo Colli (2010), apesar de essa ter sido a atividade pioneira de conexão, a maior relevância científica deve ser atribuída à iniciativa da Fapesp em efetuar a primeira conexão TCP/IP – protocolo de comunicação utilizado para a troca de informações entre os computadores – com a internet, em fevereiro de 1991.

Foi dessa forma que a Internet chegou à residência da maioria da população brasileira e se tornou imprescindível para as pessoas, seja qual for a sua finalidade, social, laboral, científica etc.

2.2 CONCEITO E HISTÓRICO DOS CRIMES CIBERNÉTICOS NO BRASIL

Embora ainda não exista na doutrina um conceito pacificado sobre crimes cibernéticos, sendo, inclusive, tratados como sinônimo de crimes virtuais, informáticos, digitais etc., o presente trabalho abordará o conceito elaborado por alguns doutrinadores e, para melhor amoldar ao objeto da pesquisa, adotará uma posição.

Por um lado, entende Colli (2010) que o conceito de crimes informáticos pode ser dividido em duas categorias: a) quando o computador é uti-

lizado como meio-fim para a consecução de um crime; b) quando o computador, ou algo nele constante ou inerente, é o próprio objeto material da conduta criminalizada. Esse autor afirma que os crimes cibernéticos, dentro do gênero dos crimes informáticos, são aqueles em que um ou mais computadores, equipamentos telemáticos ou dispositivos eletrônicos, são utilizados, por um ou mais indivíduos, no cometimento de uma ou mais conduta(s) criminalizada(s), ou são alvo(s) desta(s).

Por outro lado, Wendt e Jorge (2013) apresentam uma classificação um pouco distinta e melhor aperfeiçoada de acordo com o ordenamento jurídico vigente, conceituando os crimes cibernéticos como sendo aqueles delitos praticados contra ou por intermédio de computadores (dispositivos informáticos em geral). Além dessa questão, apresentam uma classificação para as denominadas "condutas indevidas praticadas por computador", dividindo-as em crimes cibernéticos e ações prejudiciais atípicas. A espécie crimes cibernéticos, ainda, subdivide-se em crimes cibernéticos abertos e crimes exclusivamente cibernéticos.

Segundo os mesmos autores, as ações prejudiciais atípicas são aquelas condutas, praticadas na/através da rede mundial de computadores, que causam transtorno/prejuízo à vítima, mas que não existe uma previsão penal, sendo, portanto, impossível a sua punição no âmbito criminal. Pode-se citar, adiantando a exposição da próxima subseção, a hipótese em que o indivíduo que invade o computador de um conhecido sem o objetivo de obter, alterar ou excluir dados ou informações ou sem violar um mecanismo de segurança, em que ele não será indiciado nem preso, pois os fatos não se adequam ao tipo penal previsto no art. 154-A do Código Penal.

Quanto aos crimes cibernéticos, os exclusivamente cibernéticos são aqueles que somente podem ser praticados contra ou por intermédio de um computador, com a utilização de computadores ou de outros recursos tecnológicos que permitem o acesso à internet (WENDT; JORGE, 2013).

Existem inúmeras condutas que caracterizam crimes exclusivamente cibernéticos, como, por exemplo, o crime de aliciamento de crianças praticado por intermédio de salas de bate papo na internet, previsto no art. 241-D do Estatuto da Criança e do Adolescente da Lei n. 8.069/1990, e o próprio crime invasão de dispositivo informático previsto no art. 154-A do Código Penal.

Os abertos, segundo os autores supramencionados, são aqueles que podem ser praticados de forma tradicional ou por intermédio dos compu-

tadores, ou seja, o computador é apenas um meio para a prática do crime, como, por exemplo, um crime contra a honra cometido através da internet.

Diante do conceito de crimes cibernéticos, verifica-se que esses tipos de crimes pressupõem o envolvimento de mais de um computador ou dispositivo telemático ou eletrônico, além de estarem conectados por uma rede, seja material ou imaterial, como, por exemplo, o *wireless* (COLLI, 2010).

Adotar-se-á, para fins de melhor clareza para a pesquisa, o conceito de Wendt e Jorge, classificando as condutas indevidas praticadas por computador como gênero, e as espécies em ações prejudiciais atípicas e crimes cibernéticos, sendo estes subdivididos em abertos e exclusivamente cibernéticos.

Não há um marco temporal para a identificação dos primeiros delitos cibernéticos, pois, desde que a Internet foi criada, é possível que tenha sido utilizada como meio para o cometimento de delitos, tendo em vista que "a Internet é um paraíso de informações, e, pelo fato de estas serem riquezas, inevitavelmente atraem o crime" (CORRÊA, 2002, p. 42).

É interessante a forma como os criminosos se adaptam às novas tecnologias e conseguem meios para o cometimento de novos delitos. Sabe-se que, lamentavelmente os criminosos são mais rápidos que os legisladores, como destaca Inellas (2009, p. 35):

> Como Promotor de Justiça Criminal que sou, sei que, infelizmente, os criminosos são mais rápidos que os legisladores. Isso acontece em todo o mundo e o Brasil não é exceção. Ainda mais, em se tratando de Internet, que passou a ser largamente utilizada em nosso País há pouco tempo e que possui peculiaridades que outros meios de comunicação não têm. A facilidade com que a Internet oferece para a prática de crimes, deixou os juristas completamente assarapantados. Não possuímos legislação específica a respeito de crimes virtuais e o nosso Código Penal data de 1940.

Segundo Tonetto (2015), sem incluir o golpe do boleto, técnica virtual para fraudar usuários, dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil (Cert) apontam crescimento de 500% das fraudes virtuais de 2013 para 2014: foram 426.621 registros. Conforme o mesmo autor, os dados da Federação Brasileira de Bancos (Febraban) apontam que, somente em 2013, R$ 1,2 bilhão foram desviados de

todas as instituições financeiras do país em crimes cibernéticos – golpe do boleto, clonagem de cartões e *internet banking*.

Dessa forma, percebe-se que os crimes cibernéticos se tornaram um alvo interessante para os criminosos, seja pela alta movimentação financeira, seja pela dificuldade de investigação da polícia e do rastreamento das informações, aliada à falta de legislação penal.

Nesse sentido, diante da preocupação mundial com o perigo dos crimes cibernéticos, foi firmada em 23.11.2001, na cidade de Budapeste, a Convenção Europeia de Cibercrimes, em vigor desde 2004, após a ratificação de cinco países (EDERLY, 2008). Atualmente, segundo Dodge (2013), a Convenção conta com 22 signatários, sendo que o Brasil, até agora, não a ratificou.

Dando conta dessa fragilidade e com o objetivo de oferecer mais condições para a punição dos crimes cibernéticos no nosso país, uma vez que quando o Código Penal de 1940 entrou em vigor esses delitos não existiam, foi apresentado o Projeto de Lei 84/1999, pelo deputado Luiz Piauhylino. O referido projeto veio a ser aprovado no ano de 2008, porém com um substitutivo (Projeto de Lei 89/2003) que teve como relator o então senador Eduardo Azeredo. Em seguida, o Projeto de Lei retornou para a Câmara Federal e, no final de 2012, foi aprovado (WENDT; JORGE, 2013). A sanção ocorreu no dia 30 de novembro de 2012 (Lei 12.735/2012), porém a aprovação dessa lei tratou apenas de dois artigos, um sobre a estruturação da Polícia Civil e Federal no combate às ações delituosas em rede de computadores e, o outro, prevendo sobre os casos de racismo praticados por intermédio dos meios de comunicação social.

Em 2011, foi apresentado o Projeto de Lei n. 587/2011 pelo deputado Sandro Alex, com a finalidade de atualizar o projeto anterior sem as principais questões polêmicas que dificultaram a sua aprovação. Em seguida, após alguns meses, foi apresentado um Projeto de Lei alternativo pelos deputados Paulo Teixeira, Luiza Erundina, Manuela D'Ávila, João Arruda, Brizola Neto e Emiliano José, contendo apenas a tipificação de condutas criminosas, sem a previsão de guarda de *logs*.

No dia 16 de maio de 2012, em razão do clamor público causado pela divulgação das fotos íntimas da atriz Carolina Dieckmann, o plenário da Câmara dos Deputados aprovou o projeto do deputado Paulo Teixeira, que tipifica principalmente o crime de invasão de dispositivo informático. O

Projeto de Lei n. 2793/2011 foi encaminhado para análise do Senado e no dia 30 de novembro de 2012 foi sancionada a Lei n. 12.737, sendo denominada socialmente e pela mídia de Lei Carolina Dieckmann. Cumpre destacar, por oportuno, que a lei traz consigo ainda a regulamentação penal no art. 154-B, o acréscimo do §1º do art. 266 do CP e ainda acrescenta ao artigo 298 o § único.

No entanto, a referida lei tem sido alvo de discussão na doutrina. Especificamente, o tipo penal previsto no art. 154-A do Código Penal, introduzido pela Lei 12.737/2012, atualmente em foco por virtude da numerosa troca de dados e informações por meio da Internet.

2.3 PROJETOS DE LEI EM ANDAMENTO E DIREITO COMPARADO

Ainda, para corroborar a insuficiência de leis relacionadas ao tema, sabe-se que existem diversos projetos de leis em tramitação no Brasil com relação a esses delitos, propostos justamente para suprir as lacunas existentes.

Alguns deles estão tendo um andamento razoável e aos poucos estão sendo colocados em vigor, haja vista a clara necessidade de regulamentação. No dia 23.04.2014 foi sancionada a Lei n. 12.965, conhecida como Marco Civil da Internet. Ela estabelece alguns princípios, garantias, direitos e deveres para o uso da internet no Brasil, inclusive a necessidade da guarda de *logs* de acesso, que podem facilitar a identificação dos autores dos delitos cibernéticos.

Embora não prescreva nenhum tipo penal, a lei do Marco Civil da Internet deve embasar futuros diplomas sobre cibercrimes, pois traz para o direito positivo o resguardo da disponibilidade da informação, através da proteção da estabilidade, segurança e funcionalidade da rede, garantindo, por exemplo, que a informação estará disponível a serviço do usuário quando acessada. É o entendimento de Cecilio (2014, texto digital):

> O marco civil da internet contempla a proteção da estabilidade, segurança e a funcionalidade da rede (art 3º, V), trazendo para o direito positivo o resguardo da disponibilidade da informação – garantia de que estará a serviço do usuário quando acessada, e que é ameaçada, por exemplo, nos ataques de negação de serviço (DDoS), que suspendem *websites* pela sobrecarga do servidor. Outro exemplo é a proteção dos dados pessoais (art. 3º, III), que corresponde à confiden-

> cialidade, à autenticidade à integridade da informação – garantidoras de que ela será acessada somente por usuários autorizados e legítimos, e de que não serão corrompidas. São violadas, dentre variadas possibilidades, quando há o acesso indevido – seja remoto ou local – a um terminal.

Há ainda a lei 13.185/15 que estabelece o Programa de Combate à Intimidação Sistemática (*Bullying*), publicada no dia 09.11.2015 e em vigor, com o objetivo de prevenir e combater este tipo de violência, inclusive aquela praticada pela rede mundial de computadores, conhecida como *Cyberbullying*.

Quanto à divulgação de fotos ou vídeos com cena de nudez ou ato sexual sem autorização da vítima maior de idade, como nos casos das comunidades de relacionamentos e do aplicativo WhatsApp, conduta que atualmente é atípica, está em tramitação no Senado Federal o Projeto de lei n. 63/2015, de autoria do Senador Romário Faria, pretendendo acrescentar ao Código Penal o artigo que tipifica essa conduta. Atualmente, encontra-se na Comissão de Constituição, Justiça e Cidadania, aguardando designação do relator.

Por oportuno, cumpre ressaltar que a conduta acima descrita, embora atípica, costuma ser enquadrada em outro tipo penal, qual seja o da difamação, previsto no art. 139, caput, do Código Penal, tendo em vista que a reputação da vítima é atingida. Conforme relatado anteriormente, algumas ações permitem o enquadramento do delito em um tipo penal diverso, para que o autor não fique impune pela inexistência de um tipo penal específico.

Entrementes, a regulamentação dos crimes cibernéticos de forma geral pode estar próxima, tendo em vista que está em tramitação o Projeto de Lei n. 236/2012, de autoria do senador José Sarney, intitulado Novo Código Penal. No projeto, há a previsão de um capítulo na parte especial destinado aos crimes cibernéticos.

Segundo Cecilio e Caldeira (2014), além de reproduzir o sumário conceitual da Convenção de Budapeste de 2001, o projeto traz, em título exclusivo, um rol de "crimes cibernéticos", atribuindo tipicidade a uma série de condutas vinculadas ao uso de sistemas informatizados, para as quais comina, sem exceção, pena privativa de liberdade. Atualmente, o projeto está aguardando designação do relator, depois de ter passado pela Comissão de Constituição, Justiça e Cidadania.

Uma breve comparação com a legislação de outros países é importante para, além de complementar a pesquisa, confirmar o atraso legislativo do nosso país quanto aos crimes cibernéticos.

Com relação aos Estados Unidos, considerando que se trata do país no qual primeiramente despontaram as revoluções cibernéticas e *ciberculturais*, e, consequentemente, as primeiras conturbações, não se estranha que as inovações da legislação digital desse país acabem influenciando os demais (RIBEIRO, 2013). Segundo o autor, em 1990, o primeiro estado norte-americano, a Califórnia, passou a tipificar o crime de *stalking* (perseguição), sendo seguido por outros e passando a ser formuladas normas para regularem as condutas praticadas nos sistemas eletrônicos. Hoje, praticamente todos os estados de lá criminalizam o *bullying* e o *cyberbullying*.

Já na Espanha, por exemplo, o Parlamento aprovou uma lei que visa a regulamentar o comércio eletrônico, tornando as Provedoras de acesso responsáveis pelo conteúdo de suas páginas e exigindo que os dados cadastrais do usuário fiquem armazenados, por, no mínimo, um ano (INELLAS, 2009).

Ainda, Portugal inovou ao estabelecer a responsabilidade penal da pessoa jurídica nos casos de criminalidade informática, através da Lei n. 109, de 17 de agosto de 1991. No art. 7º da mesma lei, tipificou o crime de furto como sendo o acesso não autorizado a sistemas informáticos, com a intenção de alcançar benefício ou vantagem indevidos (INELLAS, 2009).

3 A (IN)EFICÁCIA DO CRIME DE INVASÃO DE DISPOSITIVO INFORMÁTICO (ART. 154-A DO CÓDIGO PENAL)

Ainda que o propósito das revoluções tecnológicas e da internet especialmente, tenha sido de criar meio para facilitar a comunicação e a vida das pessoas, infelizmente esse fim foi desvirtuado por alguns para proveitos próprios, com o cometimento de delitos. Para tentar controlar essas ações e exercer regularmente o seu *jus puniendi*, o Estado elabora normas com o objetivo de punir e reprimir essas condutas através do Direito Penal.

A criação do tipo penal previsto no art. 154-A do Código Penal, de criminalizar a invasão de dispositivo informático, teve como objetivo reprimir esse tipo de conduta que se tornou recorrente nos dias atuais, e proteger a intimidade e a privacidade das pessoas, oferecendo sanções. Contudo, o tipo penal referido é alvo de críticas e discussões doutrinárias, que questionam a sua eficácia.

3.1 ELEMENTOS DO TIPO PENAL

Inserido de forma tímida pela Lei 12.737/2012, o delito de invasão de dispositivo informático "tem por tutela a liberdade individual, particularmente a privacidade no tocante a dados e informações, de cunho pessoal ou profissional, contidas em dispositivo informático, cuja segurança deve ser de alguma forma quebrada sem a autorização do titular" (PRADO; CARVALHO; CARVALHO, 2014, p. 863).

Nessa linha, Nucci (2013) entende que este seria o bem mediato a ser tutelado, enquanto o bem imediato seria a proteção à intimidade, à vida privada, à honra, à inviolabilidade de comunicação e correspondência, uma vez que o tipo penal ingressou no campo dos crimes contra a inviolabilidade de segredos, previstos na seção IV do Capítulo VI do Título I do Código Penal.

O sujeito ativo pode ser qualquer pessoa, eis que o tipo penal não exigiu condição especial. Há uma terminologia utilizada na informática para definir aquele que invade dispositivos informáticos, bem definida por Prado, Carvalho e Carvalho (2014, p. 863):

> Segundo a terminologia utilizada na informática, aquele que invade tais dispositivos com finalidade ilegal, de obtenção de vantagem indevida ou de prejuízo alheio, é denominado cracker. Cracker é, portanto, o sujeito que 'invade sistema de computadores de outra pessoa, frequentemente em uma rede, supera senhas ou licenças em programas de computadores ou de outras formas, intencionalmente, quebra a segurança de computadores.' [...] Não se pode confundir cracker com hacker, termo utilizado para designar o sujeito que é um 'aficionado por informática, profundo conhecedor de linguagens de programação, que se dedica à compreensão mais íntima do funcionamento de sistemas operacionais e a desvendar códigos de acesso a outros computadores. O *hacker* não gosta de ser confundido com um *cracker*, pois ao contrário deste, não invade sistemas com fins criminosos, mas para ampliar seus conhecimentos ou pela satisfação de detectar suas possíveis falhas de segurança'.

Assim, resumidamente, o sujeito ativo do delito de invasão de dispositivo de informática é o *cracker*, ao contrário do senso comum que intitula o agente que invade sistemas como *hacker*.

Já o sujeito passivo, segundo o autor supracitado, é o titular do dispositivo informático, tanto o proprietário como o detentor.

Dispõe o artigo 154-A do Código Penal:

> Art. 154-A: Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput*.
>
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I – Presidente da República, governadores e prefeitos;
>
> II – Presidente do Supremo Tribunal Federal;
>
> III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

> IV – dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Como se sabe, o tipo penal é composto por uma parte objetiva e outra subjetiva, doravante denominados tipo objetivo e subjetivo, respectivamente. No caso específico dos crimes de invasão de dispositivo informático, o tipo objetivo é dividido em duas partes, e reside aqui a grande problemática do tipo penal, conforme restará demonstrado a seguir.

A primeira parte do tipo objetivo (*invadir, adulterar, destruir*) encerra um tipo misto alternativo e, na segunda, há um tipo misto cumulativo (representado pela conduta de *instalar*), sendo possível invadir um dispositivo e realizar algo sem instalar nenhuma vulnerabilidade. Por outro lado, a segunda parte refere um tipo misto cumulativo, consistente em *instalar* (*alojar, colocar*) vulnerabilidades, que dependem da ação de invadir (PRADO; CARVALHO; CARVALHO, 2014).

De acordo com Greco (2014), o tipo penal exige a presença dos seguintes elementos: a) o núcleo *invadir*; b) dispositivo informático alheio; c) conectado ou não à rede de computadores; d) 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; f) ou instalar vulnerabilidades para obter vantagem ilícita.

Invadir, segundo o mesmo autor, tem o sentido de violar, penetrar, acessar, sendo *dispositivo informático alheio* todo aquele aparelho capaz de receber e transmitir dados, como, por exemplo, computadores, tablets, smartphones, etc., pertencente a outra pessoa. Aqui, acrescenta-se a lição de Mirabete e Fabbrini (2013), no sentido de que a invasão pode ocorrer tanto na hipótese por acesso *online* como também mediante acesso físico direto do agente ao dispositivo informático.

Mediante violação indevida de mecanismo de segurança é a forma através da qual ocorre a invasão, podendo ser físico, como as portas, travas para teclados com chaves, ou lógico, tais como o uso de nome de usuário e senhas, criptografar dados etc. (PRADO; CARVALHO; CARVALHO, 2014).

Com o fim de obter (alcançar, adquirir), *adulterar* (alterar, modificar) ou *destruir* (inutilizar, extinguir) *dados ou informações*, tem-se o elemento subjetivo do injusto (PRADO; CARVALHO; CARVALHO, 2014).

Sem autorização expressa ou tácita do titular do dispositivo, no entendimento dos doutrinadores supracitados, é elemento normativo do tipo com referência a uma causa de justificação, cuja ausência torna a conduta não apenas típica, como lícita, não havendo que se falar em cometimento de delito.

Instalar vulnerabilidades para obter vantagem ilícita, consistente na segunda parte do dispositivo legal, de acordo com Prado, Carvalho e Carvalho (2014), são itens físicos ou lógicos que alteram a segurança do dispositivo, são brechas no sistema computacional que permitem a obtenção de vantagem contrária ao direito, de natureza patrimonial ou não. São exemplos disso os vírus, *worms*, *trojans* e outras ferramentas utilizadas pelos criminosos para obter informações e dados.

Nucci (2013) preleciona que o legislador optou por equiparar a preparação e a execução em igual quilate, para fins de criminalização. Assim, o autor pode apenas instalar vulnerabilidades para que, no futuro, outrem dele se valha, como também pode utilizar mecanismo de espionagem para violação de dados. Complementando, o estudioso aduz que, se o mesmo agente instalar a vulnerabilidade e, depois, invadir o dispositivo informático, ele cometerá um crime. Caso ele instale, mas outro invada, cada qual cometerá o seu delito distinto. Por outro lado, se duas pessoas, mancomunadas, dividem tarefas (um instala; outro invade), trata-se de crime único, em concurso de agentes (art. 29 CP).

O tipo subjetivo do crime de invasão de dispositivo informático é representado pelo dolo, não havendo previsão para a modalidade de natureza culposa (GRECO, 2014).

De acordo com Prado, Carvalho e Carvalho (2014), consuma-se o delito com a mera invasão do dispositivo informático ou instalação de vulnerabilidades, sendo desnecessário que haja efetivamente destruição de dados ou obtenção de vantagem ilícita. Dessa forma, infere-se que se está diante de um delito formal ou de mera conduta/atividade, sendo o seu resultado (obtenção ou destruição de dados e instalação de vulnerabilidades) mero exaurimento do crime.

A tentativa é possível tendo em vista a sua natureza plurissubsistente, onde se pode fracionar o *iter criminis*. Nesse sentido, Greco (2014) exemplifica a hipótese na qual o agente é descoberto quando procurava invadir dispositivo informático alheio, durante suas tentativas de violar indevidamente o mecanismo de segurança, para os fins previstos no tipo penal.

Há ainda a figura equiparada prevista no § 1º do referido artigo, que criminaliza a conduta de quem *produz* (fabrica), *oferece* (oferta, expõe, sugere), *distribui* (dá, reparte) *vende* (comercializa) ou *difunde* (divulga) *dispositivo de computador com o intuito de permitir a prática da conduta definida no caput*. É também crime formal, não havendo, portanto, a necessidade que o invasor efetivamente utilize ou pratique alguma outra forma do núcleo do tipo penal, bastando somente a simples prática dos comportamentos (GRECO, 2014).

Outrossim, está previsto no §3º a modalidade qualificada do delito, dependendo do tipo de dados e informações obtidos pelo agente. Já no § 2º, § 4º e § 5º, estão previstas causas especiais de aumento de pena, conforme o dano praticado ou a pessoa vitimada.

Com relação à pena e à ação penal, será possível a proposta de suspensão condicional do processo, eis que a pena mínima não é superior a 01 ano. A competência é do Juizado Especial Criminal, tendo em vista que a pena máxima não ultrapassa dois anos, e a ação penal, conforme determinação contida no art. 154-B, será em regra de iniciativa pública condicionada à representação, salvo se o crime for cometido contra a administração pública direta ou indireta ou contra empresas ou concessionárias de serviços públicos, caso em que será incondicionada, tendo em vista o interesse coletivo atingido (GRECO, 2014).

3.2 VISÃO DOUTRINÁRIA E JURISPRUDENCIAL

Como se percebe após a análise do tipo penal objetivo em questão, reside na tipicidade o grande problema da caracterização da infração penal nos crimes cibernéticos.

A Lei n. 12.737/2012, no entendimento de Wendt e Jorge (2013), representou um avanço para o ordenamento jurídico, porém alguns de seus aspectos têm gerado polêmica e preocupação, como, por exemplo, em relação às suas penas, consideradas brandas. Segundo o autor, é necessário o aprimoramento da legislação que trate dos referidos delitos, o que, preventivamente, ajudaria a diminuir a sua incidência por favorecer a punição dos seus autores. No entanto, a criação de novos tipos penais pouco poderá colaborar se não existe, por exemplo, um prazo mínimo para a guarda de log, proteção da privacidade, ações integradas etc.

Destaca-se, nesse ponto, que com a edição da Lei n. 12.965/2014, conhecida como Marco Civil da Internet, houve um avanço da legislação, de

forma a regulamentar o prazo mínimo para a guarda de log e proteger a informação, permanecendo, contudo, carente de ações integradas para que a efetiva tutela desses bens jurídicos seja garantida no meio eletrônico.

Apesar de os crimes cibernéticos carecerem de regulamentação em nosso ordenamento jurídico, existem tipos penais que podem enquadrar as condutas praticadas, ainda que não propriamente adequados, chamado de crimes cibernéticos abertos, na classificação de Wendt e Jorge (2013), de acordo com a classificação feita na subseção anterior. Há, nesse sentido, o exemplo dos crimes contra a honra, de estelionato e os de furto mediante fraude, previstos no Código Penal e praticados por intermédio da internet, já tipificados em nosso ordenamento e que podem enquadrar algumas condutas praticadas por intermédio de dispositivos informáticos.

Cabette (2013, texto digital) corrobora o entendimento de que há a necessidade de criação de novos tipos penais para o combate dos delitos cibernéticos, uma vez que são revestidos de características peculiares e necessitam de regulamentação, assim como ocorre nos demais ramos do direito, como, por exemplo, civil e comercial:

> Há muito que se discute sobre a necessidade ou não de erigir normas penais especiais relativas aos delitos informáticos. Seria isso mesmo necessário ou o recurso aos tipos penais tradicionais seria suficiente? Entende-se que o fenômeno informático está a exigir regulamentação especial devido às suas características que divergem de tudo quanto sempre foi usual. Isso se faz sentir claramente em outros ramos do direito como na área civil, processual, comercial, consumerista, trabalhista, cartorial etc. Por que seria diferente na seara penal? Agiu, portanto, com correção o legislador ao criar o tipo penal ora em estudo, especialmente considerando o fato de que há tutela de bem jurídico constitucionalmente previsto, como já se explicitou acima.

De outra banda, há doutrinadores que veem com pessimismo a Lei 12.737/2012, especialmente com relação à sua eficácia, entendendo, inclusive, que a tutela civil teria condições de ser mais eficiente com relação aos crimes cibernéticos que invadem a privacidade das pessoas. É o entendimento de Gomes (2013, texto digital):

> [...] Eu, particularmente, confio mais em medidas civis (determinadas por juiz civil, como remoção de uma notícia ofensiva). Confio mais em indenizações. Quem conhece mi-

> nimamente o funcionamento da justiça criminal no Brasil não pode se iludir: ela está, em geral, sucateada. Porque sucateada está a polícia civil (investigativa), que conta com incontáveis cadáveres nas suas portas, o que já é suficiente para sugar todos os seus recursos materiais e pessoais. Medidas civis urgentes são mais eficazes nessa área. De qualquer modo, houve intenção de se suprir uma lacuna no Brasil. O relator do projeto, deputado Paulo Teixeira, procurou fazer o melhor texto, mas todo conjunto de palavras permitem mil interpretações. Numa rápida olhada assinalei 104 conceitos dados pela lei, todos dependentes de interpretação. As penas são baixas (em regra, até dois anos), logo, a chance de prescrição é muito grande. Por todos esses motivos, não confio na eficácia preventiva dessa lei. A tutela civil teria condições de ser mais eficiente.

É justamente com base nesse possível enquadramento das condutas aos delitos já existentes em nosso ordenamento que o doutrinador defende a desnecessidade de criação de novos tipos penais, além da posição de que a área civil tem mais condições de tutelar a privacidade das pessoas com base em medidas cautelares e indenizações.

Entrementes, nem todas as condutas praticadas poderão ser passíveis de enquadramento nos tipos penais existentes, mormente a limitação do poder punitivo estatal e o conceito analítico de crime, sendo necessário que, além de o crime imputado ser típico, previsto em lei, em obediência ao princípio da legalidade, ele precisa ser antijurídico e culpável para que se possa iniciar a persecução penal. Em recente decisão, o Tribunal de Justiça do Estado do Rio Grande do Sul assentou que a cópia de arquivos digitais sem autorização não é furto e tampouco invasão de dispositivo informático, sendo, portanto, tal conduta atípica. A ementa é a seguinte:

> APELAÇÃO CRIME. CRIMES CONTRA O PATRIMÔNIO. FURTO QUALIFICADO PELO ABUSO DE CONFIANÇA. CÓPIA DE ARQUIVOS E DOCUMENTOS INFORMÁTICOS. ATIPICIDADE DA CONDUTA. ABSOLVIÇÃO. Tanto a narrativa contida na denúncia como os substratos probatórios colacionados aos autos revelam que a ré copiou, para si, possivelmente infringindo contrato firmado perante sua empregadora, arquivos e documentos informáticos gravados em disco rígido de computador - conduta atípica e que não se subsume àquela abstratamente prevista no artigo 155 do CP. Precedentes doutrinários de que o verbo nuclear previsto no tipo - subtrair - pressupõe o apoderamento da coisa móvel alheia mediante apreensão e ulterior remoção do local onde se encon-

> trava, exigindo-se, para a consumação do ilícito, que a res seja inclusive transportada para lugar onde a vítima não mais possa, ainda que precariamente, realizar vigilância sobre a mesma. Inviabilidade de se considerar que a acusada, copiando, para si, dados e arquivos informáticos, tenha tirado os mesmos da esfera de disponibilidade ou custódia da empresa ofendida, visto que simplesmente duplicou e gravou os mesmos em dispositivo do tipo USB, permanecendo a informação originária acessível à respectiva detentora de seus direitos autorais. Ausência de *animus furandi* ou *rem sibi habendi* que impõe, nesse contexto, considerar atípica a conduta noticiada, razão do acolhimento do pleito absolutório nos termos do artigo 386, inciso III, do Estatuto Penal Adjetivo. APELAÇÃO DEFENSIVA PROVIDA. APELO MINISTERIAL DESACOLHIDO. (Apelação Crime Nº 70049844483, Sétima Câmara Criminal, Tribunal de Justiça do RS, Relator: Naele Ochoa Piazzeta, Julgado em 29/04/2014).

No acórdão, a Relatora entendeu que a conduta de copiar dados cibernéticos para si não se amolda ao verbo nuclear previsto no tipo penal do crime de furto, tendo em vista que não há o apoderamento de coisa móvel alheia e nem mesmo o transporte da coisa para outro lugar, saindo da esfera de vigilância da vítima. Ao final, destaca que em atenção ao princípio da anterioridade (o fato é anterior à edição da Lei 12.737/12), e porque o caso concreto não englobaria "violação indevida de mecanismos de segurança", sequer cogita a desclassificação da conduta descrita na incoativa para o crime de invasão de dispositivo informático, previsto no art. 154-A do Código Penal, tendo, desta forma, provido o apelo defensivo e absolvido a ré.

Ressalta-se, por oportuno, que explorando o caso em tela não se pretende discutir se a cópia de dados eletrônicos caracteriza ou não o crime de furto, mas analisar a adequação típica, ou seja, a incidência do fato praticado com relação à norma penal e a (im)possibilidade de incriminação da ré com base nos tipos penais existentes. Igualmente, o delito de invasão de dispositivo informático, por ser crime-meio de algum outro mais grave, é utilizado para pedir a desclassificação da imputação e consequentemente uma pena menor para o autor, como, por exemplo, nos crimes de furto de valores bancários pela internet.

Quanto aos casos em que houve tão somente o crime de invasão de dispositivo informático, não foram encontradas decisões jurisprudenciais nesse sentido. Uma das razões é que o delito é recente, tendo entrado em vigor com a edição da Lei 12.737/12, que foi publicada no Diário Oficial em

03 de dezembro de 2012, com *vacatio legis* de 120 dias. A outra é que, conforme visto, ainda que o crime seja qualificado, a pena máxima será de 02 anos e a competência para julgamento é do Juizado Especial Criminal. Assim, como a possibilidade de ocorrer a transação penal é bastante grande, não foram encontradas decisões de mérito sobre o caso.

3.3 A (IN)EFICÁCIA DO CRIME DE INVASÃO DE DISPOSITIVO INFORMÁTICO

O estudo do tipo penal em questão leva a crer que, quanto ao seu tipo penal objetivo, é desnecessária a inserção da expressão *mediante violação indevida de mecanismo de segurança* no tipo penal, pois está se alijando da tutela penal todos os dispositivos informáticos que não possuem tal mecanismo (NUCCI, 2013). Segundo o doutrinador, caso o ofendido esqueça de ativar a senha de proteção ou mesmo não haja programa nesse prisma, está desguarnecido da proteção penal, querendo, pois, o legislador que a vítima se proteja de algum modo; se não o fizer, a tutela penal não a alcança.

De fato, a inserção da expressão "mediante violação indevida de mecanismo de segurança" acabou por restringir a incidência do tipo penal apenas nos casos em que existe uma proteção por algum mecanismo de segurança, ou, em caso contrário, estaríamos diante de um fato atípico, não considerado crime. Ocorre que desta forma o legislador acabou deixando de fora da tutela penal os dispositivos informáticos que não possuem ou estão com o mecanismo de segurança inabilitado, deixando desprotegidas justamente as pessoas que mereciam a sua tutela.

Esses casos são muito comuns, ocorrendo, por exemplo, a obtenção de fotos íntimas de vítima maior de idade e a posterior divulgação por meio eletrônico, por exemplo, pelo aplicativo *WhatsApp*, sendo a conduta, portanto, atípica na área penal por inexistir violação do mecanismo de segurança e nem mesmo a tipificação penal da divulgação de fotos íntimas de pessoas maiores de idade sem autorização. Contudo, conforme destacado anteriormente, existem casos passíveis de enquadramento como crime contra a honra, por exemplo, de difamação, com o objetivo de punir os autores do delito ainda que não haja tipo penal específico.

Seguindo essa linha, no entendimento de Cabette (2013, texto digital), o ideal seria "que o legislador incriminasse diretamente somente a invasão ou instalação de vulnerabilidades, independentemente da violação de mecanismo de segurança". Complementando, o estudioso mencionado

preleciona que poderia inclusive o legislador criar uma qualificadora ou uma causa especial de aumento pena para o caso de a invasão se dar com a violação de mecanismo de segurança.

Para ilustrar a aberração criada pelos legisladores, Cabette (2013, texto digital) faz uma inteligente comparação entre o mecanismo de segurança de um computador com as portas e janelas das casas:

> Observe-se ainda que ao exigir a 'violação indevida de mecanismo de segurança', não bastará a existência de instalação desses mecanismos no dispositivo informático invadido, mas também será necessário que esses mecanismos estejam atuantes no momento da invasão, caso contrário não terá havido sua violação e o fato também será atípico, o que é ainda mais estranho. Explica-se: imagine-se que um computador pessoal é dotado de antivírus, mas por algum motivo esse antivírus foi momentaneamente desativado pelo próprio dono do aparelho. Se há uma invasão nesse momento, o fato é atípico! Note-se que neste caso o exemplo da porta aberta e da invasão de domicílio é realmente muito elucidativo. A casa tem portas, mas estas estão abertas, então as pessoas podem entrar sem a autorização do morador? É claro que não! Mas, parece que com os sistemas informáticos o raciocínio legislativo foi diverso e, diga-se, equivocadíssimo.

O exemplo acima retratado reflete perfeitamente o problema criado pelos legisladores ao inserirem a expressão "violação indevida de mecanismo de segurança", tendo em vista que, obedecendo-se ao conceito analítico de crime, para que se possa iniciar a persecução penal o delito precisar ser típico, ou seja, estar previsto em lei. A aberração criada, em analogia às portas e janelas que protegem uma casa, não consideraria crime de violação de domicílio, previsto no art. 150, *caput*, do Código Penal, caso alguém invadisse uma residência com as portas e janelas abertas.

Com relação aos dispositivos informáticos, são atualmente ferramentas de trabalho e possuem as mais diversas utilidades, guardando a privacidade e a intimidade das pessoas, valores íntimos que, se violados e divulgados, podem causar enormes prejuízos morais e psicológicos às vítimas. Não são poucos os casos vistos diariamente nos meios de informação em que houve prévia divulgação de uma foto íntima da pessoa.

Esse tipo de conduta, segundo Dip e Afiune (2013), trouxe à tona o conceito de "*revenge porn*" ou "pornô da vingança", que se refere à prática cada vez mais comum de divulgar fotos e vídeos íntimos sem o consentimento da outra pessoa, geralmente por parte de um homem, para se vingar. Tanto a conduta de divulgação quanto a de invasão de dispositivo informático para obtenção deste tipo de dado deve ser severamente reprimido tanto pelas normas quanto pela sociedade, uma vez que o dano causado pode ser irreparável. Para retratar o abalo que este tipo de conduta pode causar nas pessoas, especialmente nos jovens e adolescentes, as autoras mencionadas, após os suicídios de uma garota no Estado do Rio Grande do Sul e uma da Paraíba por causa da divulgação de fotos/vídeos íntimos na internet, fizeram um estudo em que falam com adolescentes do país sobre o suicídio dessas meninas e revelam como é amadurecer em um mundo em que o virtual é real.

4 CONCLUSÃO

As pessoas, em um mundo cada vez mais globalizado e competitivo, precisam cuidar de sua privacidade e intimidade, não sendo dado a ninguém o direito de invadir, deturpar ou divulgar informações e dados que não lhe pertencem. Diante desta premissa, a liberdade individual merece especial atenção e a devida proteção penal, eis que constitucionalmente garantida, através da inviolabilidade das comunicações e o sigilo profissional, expressas no art. 5º, XII, da Constituição Federal.

São inegáveis os benefícios proporcionados pela revolução tecnológica proporcionada no século XXI, principalmente através da internet, ferramenta que revolucionou os meios de comunicação e a transmissão de informações. Ocorre que, infelizmente, algumas pessoas desvirtuaram esse objetivo e transformaram o meio eletrônico em um local para o cometimento de delitos, uma vez que a sua riqueza é imensurável e, lamentavelmente, sabemos que o crime volta suas atenções para onde há riqueza.

Nesse sentido, a regulamentação desses delitos oriundos dos avanços tecnológicos, ainda que revestidos somente de um novo meio de execução, como é o caso dos crimes cibernéticos, se faz justa a fim de propiciar a segurança jurídica necessária; assim como os demais ramos do direito fizeram com o direito civil e comercial, por exemplo, se adequando para regular as relações de consumo virtuais.

Contudo, essa regulamentação deve ser precedida de muito estudo por parte dos legisladores, sempre respeitando os princípios constitucionais e beirando a perfeição técnica, a fim de que a nova norma não se torne ineficaz. Infelizmente, motivado pelo clamor social proporcionado pela divulgação de fotos íntimas da atriz Carolina Dieckmann na época, essas regras não foram observadas na edição do tipo penal de invasão de dispositivo informático, que não conseguiu proteger a liberdade individual das pessoas, punir e reprimir este tipo de conduta.

A inserção da expressão "violação indevida de mecanismo de segurança" acabou por alijar da tutela penal a pessoa que, por um descuido ou desconhecimento, não está provida do mecanismo de segurança, deixando, com a utilização do termo "indevidamente", uma excludente de ilicitude implícita no tipo penal, o que deixou deficiente a tipicidade formal e, por conseguinte, a sua adequação típica. Frisa-se que nem sempre o enquadramento de condutas às normas já existentes é possível, devendo, sobretudo, ser respeitado o princípio da legalidade.

Dessa forma, diante da análise do problema proposto para este estudo – A criminalização da invasão de dispositivo informático, introduzido no Código Penal pela lei 12.737/12, é eficaz? –, pode-se concluir que a hipótese inicial levantada para tal questionamento é verdadeira, na medida em que o crime em questão não atingiu a sua finalidade.

Apesar de a área cível ser um caminho para ressarcir o abalo sofrido pela vítima, sabe-se que muitos dos criminosos são pobres e não possuem condições financeiras de cumprir com a condenação e o pagamento da indenização, ficando a vítima sem a devida compensação. Em que pese não ter sido possível a localização de decisões jurisprudenciais de mérito sobre esse tipo de crime, é crível que os tribunais tendem a decidir e encontrar os problemas já apontados pela doutrina, no sentido de que o artigo em questão possui deficiências técnicas que o tornam tipicamente inadequado e, portanto, ineficaz.

Nessa linha, denota-se que se a proteção do bem jurídico tutelado pelo crime em questão ficar alienada à necessidade de violação de algum mecanismo de segurança para configuração do delito, as pessoas que mais necessitam da proteção do direito penal por estarem vulneráveis aos criminosos, ficarão desamparadas. Se, conforme visto no texto, essa continuar sendo a ideia do legislador e o crime continuar sendo utilizado como crime-meio para outro mais grave, como, por exemplo, o furto mediante fraude

de valores bancários, o tipo penal mencionado continuará sem utilidade alguma, restando totalmente ineficaz.

Não obstante, o aumento da pena cominada aos infratores, tese defendida por alguns doutrinadores, seria interessante para não tornar tão precária a proteção a um bem jurídico tão importante como o da liberdade individual, tendo em vista que com a pena máxima superior a dois anos se afasta a competência do Juizado Especial Criminal e, consequentemente, a possibilidade de aplicação dos seus institutos despenalizadores previstos.

Dessa forma, impõe-se a incidência da tutela penal sobre um bem jurídico tão valioso como esse. Cabe aos legisladores a elaboração de normas penais eficazes que possam efetivamente coibir e punir a prática do delito de invasão de dispositivo informático, atendendo à função do direito penal em um Estado Democrático de Direito clamada por Roxin: prover a segurança jurídica através da proteção dos bens jurídicos e direitos.

5 REFERÊNCIAS

BRASIL. Decreto-Lei nº. 2.848, de 07 de dezembro de 1940. **Código Penal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm>. Acesso em: 24 ago. 2015.

BRASIL. Lei nº. 8.069, de 13 de julho de 1990. **Estatuto da Criança e do Adolescente**. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/l8069.htm>. Acesso em: 24 ago. 2015.

BRASIL. Tribunal de Justiça do Estado do Rio Grande do Sul. **Apelação Criminal nº 70049844483**, 7ª Câmara Criminal. Apelante/Apelado: Nara Elisa Follmer. Apelante/Apelado: Ministério Público. Apelado/Assistente de Acusação: Medabil Sistemas Construtivos S.A. Relatora: Des.ª Naele Ochoa Piazzeta. Porto Alegre, 29 abr. 2014. Disponível em: <http://www.tjrs.jus.br/busca/search>. Acesso em: 24 set. 2015.

CABETTE, Eduardo Luís Santos. O novo crime de invasão de dispositivo informático. **ConJur**, São Paulo, 04 fev. 2013. Disponível em: <http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico>. Acesso em: 02 set. 2015.

CECILIO, Leonardo Rezende. Marco civil da internet deve embasar futuros diplomas sobre cibercrimes. **ConJur**, São Paulo, 27 jun. 2014. Disponível

em: <http://www.conjur.com.br/2014-jun-27/leonardo-cecilio-marco-civil-embasar-futuros-diplomas-cibercrimes>. Acesso em: 02 set. 2015.

CECILIO, Leonardo Rezende; CALDEIRA, Felipe Machado. Cibercrimes em projeto do Senado carecem de precisão. **ConJur**, São Paulo, 05 mar. 2014. Disponível em: <http://www.conjur.com.br/2014-mar-05/previsao-cibercrimes-projeto-senado-carece-precisao-tecnica>. Acesso em: 02 set. 2015

COLLI, Maciel. **Cibercrimes**: Limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá, 2010.

DIP, Andrea; AFIUNE, Giulia. Como um sonho ruim. **Pública**: Agência de Reportagem e Jornalismo Investigativo, São Paulo, 19 dez. 2013. Disponível em: <http://apublica.org/2013/12/6191/>. Acesso em: 28 set. 2015.

DODGE, Raquel E. F. **Roteiro de atuação sobre crimes cibernéticos**. Ministério Público Federal. Câmara de Coordenação e Revisão. 2. ed. Brasília: Ministério Público Federal, 2013.

GOMES, Luiz F. Lei Carolina Dieckmann e sua (in)eficácia. **Revista JusNavigandi**, Teresina, ano 18, n. 3536, 7 mar. 2013. Disponível em: <http://jus.com.br/artigos/23897>. Acesso em: 17 ago. 2015.

GRECO, Rogério. **Curso de Direito Penal**. 11. ed. Rio de Janeiro: Impetus, 2014. v. 2.

INELLAS, Gabriel C. Z de. **Crimes na internet**. 2. ed. São Paulo: Juarez de Oliveira, 2009.

MEZZAROBA, Orides; MONTEIRO, Cláudia S. **Manual de metodologia da pesquisa no Direito**. 5. ed. São Paulo: Saraiva, 2009.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. **Manual de Direito Penal**. 30. ed. São Paulo: Atlas, 2013. v. 2.

NUCCI, Guilherme de S. **Manual de Processo Penal e Execução Penal**. 11. ed. Rio de Janeiro: Forense, 2014.

_____. **Código Penal Comentado**. 13. ed. São Paulo: Revista dos Tribunais, 2013.

PRADO, Luiz R.; CARVALHO, Érika M. de; CARVALHO, Gisele M. de. **Curso de Direito Penal Brasileiro**. 13. ed. São Paulo: Revista dos Tribunais, 2014.

RIBEIRO, Thiago de L. **O direito aplicado ao cyberbulling**: honra e imagem nas redes sociais. Curitiba: InterSaberes, 2013. E-book. Disponível em: <http://univates.bv3.digitalpages.com.br/users/publications/9788582127995/pages/-2 >. Acesso em: 10 ago. 2015.

TONETTO, Maurício. Defenda-se das fraudes virtuais. **Zero Hora**, Porto Alegre, p.32, 03 jul. 2015.

WENDT, Emerson; JORGE, Higor V. N. **Crimes Cibernéticos**: Ameaças e procedimentos de investigação. 2. ed. Rio de Janeiro: Brasport, 2013.