CENTRO UNIVERSITÁRIO UNIVATES
CURSO DE DIREITO

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

Guilherme Anderson Caneppele

Lajeado, dezembro de 2015.

Guilherme Anderson Caneppele

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

Monografia apresentada na disciplina de Trabalho de Curso II – Monografia do Curso de Direito, do Centro Universitário Univates, como parte da exigência para obtenção do título de Bacharel em Direito.

Orientadora: Profa. Ma. Elisabete Cristina Barreto Muller

Lajeado, dezembro de 2015.

Guilherme Anderson Caneppele

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

A Banca examinadora abaixo aprova a Monografia apresentada na disciplina de Trabalho de Curso II – Monografia, do curso de graduação em Direito, do Centro Universitário Univates, como parte da exigência para a obtenção do grau de Bacharel em Direito:

Profa. Ma. Elisabete Cristina Barreto Muller – orientadora
Centro Universitário Univates

Dr. Ederson Luciano Maia Vieira
Promotor de Justiça

Dr. Alex Edmundo Assmann
Delegado de Polícia Civil

Lajeado, 1º de dezembro de 2015.

AGRADECIMENTOS

Primeiramente, agradeço aos meus pais, Marco e Salete, por todo o afeto e amor a mim proporcionados. Pela constante preocupação e incentivo àquilo que, infelizmente, não tiveram oportunidade: os estudos. Vocês são meus exemplos de honestidade, determinação e persistência, a base que, sem dúvidas, contribuiu para me tornar uma pessoa digna.

Ao meu irmão, Julierme, pelo seu companheirismo, carinho e respeito, e por sempre acreditar em mim.

À minha namorada, Daniele, pela compreensão, carinho e amor. Por ter te conhecido e ter a honra estar ao seu lado nesta etapa tão importante da minha vida, compartilhando essa vitória. Agradeço pelo apoio e por sempre torcer para que alcance meus ideais.

Aos meus amigos, professores, companheiros e supervisores de estágio que de alguma forma prestaram ensinamentos, conselhos e apoio.

Agradeço, por fim, à minha orientadora Elisabete Cristina Barreto Muller, pelos seus inestimáveis conselhos, ensinamentos e esforços despendidos ao decorrer deste trabalho.

“Quereis prevenir delitos? Fazei com que
as leis sejam claras e simples”.
(Cesare Beccaria)

RESUMO

A tipificação penal do crime de invasão de dispositivo informático, previsto no art. 154-A do Código Penal e inserido no título dos crimes contra a liberdade individual, visa tutelar a privacidade concernente a dados e informações pessoais e profissionais. A presente tem como objetivo geral analisar a (in)eficácia desse recente crime, introduzido no Brasil pela Lei 12.737/12. 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 descrição de conceitos preliminares e princípios relativos aos crimes cibernéticos, trazendo seus elementos fundamentais. Em seguida, aborda os crimes cibernéticos no Brasil através de uma análise histórica, identificando os aspectos da legislação penal do nosso ordenamento jurídico que tratam sobre esse delito, observando as suas carências. Por fim, examina, com base nos princípios, doutrina e decisões jurisprudenciais, a (in)eficácia do crime de invasão de dispositivo informático. Nesse sentido, conclui que o crime em questão é ineficaz, tendo em vista que não atingiu a finalidade de prevenir e reprimir a incidência deste tipo de delito, ante a existência de expressões no tipo penal que impedem a adequação típica do fato à norma.

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

LISTA DE ABREVIATURAS

Arpa	Advanced Research Projects Agency
Cert	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CNPq	Conselho Nacional de Desenvolvimento Científico e Tecnológico
CF	Constituição Federal
CP	Código Penal
CPP	Código de Processo Penal
Febraban	Federação Brasileira de Bancos
HTML	HyperText Markup Language
IP	Internet Protocol
ISPs	Internet Service Providers
Ibase	Instituto Brasileiro de Análises Sociais e Econômicas
MCI	Marco Civil da Internet
ONU	Organização das Nações Unidas
PL	Projeto de Lei
PC	Personal Computers
RNP	Rede Nacional de Pesquisas
WWW	World Wide Web

SUMÁRIO

1 INTRODUÇÃO 9

2 CONCEITOS PRELIMINARES E PRINCÍPIOS RELATIVOS AOS CRIMES CIBERNÉTICOS 12

2.1 Conceito e função dos princípios 13

2.2 Princípio da legalidade e da reserva legal 14

2.3 Princípio da humanidade 15

2.4 Princípio da inocência, contraditório e das provas irrepetíveis em cibercrimes 17

2.5 Princípio da territorialidade 18

2.6 Conceito de crime 20

2.6.1 Conceito material e formal de crime 21

2.6.2 Conceito analítico de crime 22

2.6.2.1 Tipo e tipicidade penal 23

2.6.2.2 Antijuricidade ou ilicitude 26

2.6.2.3 Culpabilidade 27

3 ABORDAGEM SOBRE OS CRIMES CIBERNÉTICOS NO BRASIL E A LEI N. 12.737/12 30

3.1 Breve histórico da internet 31

3.1.1 A internet no Brasil 32

3.2 Conceito de crime cibernético 34

3.3 Contexto histórico dos crimes cibernéticos no Brasil 36

3.3.1 A edição da Lei n. 12.737/12: Lei Carolina Dieckmann 37

3.4 Projetos de lei em andamento no Brasil 39

3.5 Características e peculiaridades da persecução penal dos crimes ciberneticos 40

3.6 Breves considerações acerca do direito comparado 44

4 A (IN)EFICÁCIA DO CRIME DE INVASÃO DE DISPOSITIVO INFORMÁTICO (ART. 154-A DO CÓDIGO PENAL)....46
4.1 Bem jurídico e sujeitos do delito....47
4.2 Elementos do tipo....48
4.2.1 Tipo objetivo....49
4.2.2 Tipo subjetivo....50
4.3 Consumação e tentativa....51
4.4 Ação penal....52
4.5 Visão doutrinária e jurisprudencial....52
4.6 A (in)eficácia do artigo 154-A do Código Penal....58

5 CONCLUSÃO....63

REFERÊNCIAS....67

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 de todo mundo quase que instantaneamente, seja para o compartilhamento de dados pessoais, profissionais, ou de qualquer natureza que for.

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, chamado crimes cibernéticos, que ainda carecem de regulamentação no nosso país, conforme restará demonstrado ao decorrer do trabalho.

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 totalmente desamparado.

A falta de regulamentação de normas específicas 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 do crime de invasão de dispositivo informático.

Não é tarefa fácil o Estado acompanhar simultaneamente os avanços da sociedade e conseguir, ao mesmo tempo, regular todas as relações, ainda mais quando se trata de um crime complexo como o cibernético, que pode envolver vários países, justamente por ser virtual e não encontrar fronteiras.

No entanto, cabe ao Estado organizar-se da melhor forma possível e regulamentar o tema, seja através da criação de normas ou tratados internacionais que possibilitem o exercício regular do poder punitivo.

Nesse sentido, o presente trabalho pretende, como objetivo geral, estudar a (in)eficácia do crime de invasão de dispositivo informático, recém introduzido no Brasil pela Lei n. 12.737/12. O estudo discute como problema: O crime de invasão de dispositivo informático, introduzido no Código Penal pela lei 12.737/12, é eficaz?

Como uma possível hipótese para tal questionamento, entende-se que o 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 pesquisa, quanto à abordagem, será qualitativa, que tem como característica o aprofundamento no contexto estudado e a perspectiva interpretativa desses possíveis dados para a realidade, conforme 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 descrição de conceitos preliminares e princípios relativos aos crimes cibernéticos, passando pela abordagem dos crimes cibernéticos no Brasil através de uma análise histórica 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.

Dessa forma, no primeiro capítulo de desenvolvimento deste estudo serão descritos conceitos preliminares e princípios relativos aos crimes cibernéticos. Primeiramente, serão apontados o conceito e a função dos princípios, notadamente os constitucionais que atuam como limitadores do poder punitivo. Em seguida, far-se-á a compreensão de alguns conceitos de crime, destacando-se, principalmente, o conceito analítico de crime.

Na sequência, no segundo capítulo, far-se-á uma abordagem sobre os crimes cibernéticos no Brasil e sobre a legislação penal vigente. Em um primeiro momento serão tecidas considerações históricas sobre a internet, e pelo conceito de crime cibernético. Após, passar-se-á ao estudo da evolução histórica deste tipo de delito no Brasil. Além disso, fará uma análise da legislação brasileira específica vigente sobre esses crimes.

Adiante, no terceiro capítulo, far-se-á a análise, com base nos princípios constitucionais, bem como na doutrina e em decisões jurisprudenciais, da (in)eficácia do crime de invasão de dispositivo informático, introduzido no Código Penal pela Lei n. 12.737/12.

2 CONCEITOS PRELIMINARES E PRINCÍPIOS RELATIVOS AOS CRIMES CIBERNÉTICOS

O Direito Penal, ramo do Direito Público Interno, regula as relações dos indivíduos com a sociedade através da *persecutio criminis*, que é exercida sob o monopólio do Estado e somente pode ser desempenhada de acordo com normas preestabelecidas, garantindo-se, assim, uma punição a quem não tem um comportamento adequado para viver em sociedade.

A *persecutio criminis* pode ser entendida como o caminho para que o Estado exerça o seu direito e atinja o seu objetivo de punir o autor de ações violadoras de bens jurídicos, ou seja, havendo uma conduta contrária às normas existentes nasce o *jus puniendi* do Estado.

No entanto, há a necessidade de que o poder punitivo estatal seja limitado, a fim de que não se torne abusivo. Nesse sentido, para se ter uma melhor compreensão do seu papel e dos princípios constitucionais limitadores do poder punitivo estatal, faz-se necessária uma análise de alguns conceitos sobre essa importante matéria.

Assim, será objetivo deste capítulo descrever noções sobre o Direito Penal e Processual Penal, trazendo alguns elementos fundamentais, como princípios penais e processuais penais atinentes aos crimes cibernéticos, conceito de crime, tipicidade, ilicitude e culpabilidade.

2.1 Conceito e função dos princípios

Os princípios, do latim *principium*, denotam uma ideia de começo, origem, ou seja, onde tudo começou. Possuem uma força normativa constitucional, eis que são basilares dos atuais Estados Democráticos de Direito, dando sustentação e ao mesmo tempo limites ao ordenamento jurídico.

Nessa linha, o presente estudo abordará alguns princípios limitadores constitucionais do *jus puniendi* do Estado, especialmente os da legalidade, humanidade e territorialidade, que impossibilitam, por exemplo, considerar crime algo não previsto em lei ou a invasão da competência de um território estrangeiro no caso do cometimento de um crime cibernético oriundo de outro país.

Em seguida, será analisado o conceito de crime, indispensável para complementar o trabalho. Conforme se verá, o fato típico, elemento integrante do conceito analítico de crime, exige a descrição do tipo penal em lei para que se inicie a *persecutio criminis*, obedecendo-se, assim, ao princípio da legalidade.

Neste singelo exemplo, percebe-se a força dos princípios e a explicitação de ser a origem e a base das normas do ordenamento jurídico.

Nesse sentido, para Barroso (2005) os princípios indicam valores a serem preservados ou fins a serem alcançados, trazendo em si um conteúdo axiológico ou uma decisão política.

Na mesma linha, Bonavides (2006, p. 289) ressalta que os princípios servem de base para sustentar o ordenamento jurídico e são de grande relevância, especialmente pela função exercida nas Constituições:

> A importância vital que os princípios assumem para os ordenamentos jurídicos se torna cada vez mais evidente, sobretudo se lhes examinarmos a função e presença no corpo das Constituições contemporâneas, onde aparecem como os pontos axiológicos de mais alto destaque e prestígio com que fundamentar na Hermenêutica dos tribunais a legitimidade dos preceitos da ordem constitucional.

É sabido que essa força dos princípios inerentes aos textos constitucionais, atuando como limitadores, veio se aprimorando ao longo do tempo e é fruto de muitas batalhas da sociedade, em busca da concretização do direito.

Dessa forma, resumidamente, pode-se afirmar que os princípios possuem funções, dentre outras, informativa e fundamentadora, realizando a congruência, o equilíbrio e a essencialidade de um sistema jurídico legítimo (BONAVIDES 2006).

2.2 Princípio da legalidade e da reserva legal

Segundo Bitencourt (2012, p. 48), "o princípio da legalidade constitui uma efetiva limitação ao poder punitivo estatal". Por este princípio, a elaboração das normas incriminadoras é função exclusiva da lei, isto, é nenhum fato pode ser considerado crime sem que antes da sua ocorrência exista uma lei definindo-o como crime e cominando-lhe a sanção correspondente.

Esse entendimento deu origem à conhecida fórmula latina *nullum crimen, nulla poena sine praevia lege*, há tempos idealizada por Beccaria e disposta no sentido de que não existe crime sem lei anterior que o defina.

Tal garantia vem igualmente prevista no art. 5º, XXXIX, da Constituição Federal de 1988, sendo assegurado que "não haverá crime sem lei anterior que o defina, nem pena sem prévia cominação legal".

Ferrajoli (2014, p. 344) ensina que "somente as leis (e não também a moral ou outras fontes externas) dizem o que é delito e que as leis somente dizem o que é delito (e não também o que é pecado)".

Menciona Prado, De Carvalho e De Carvalho (2014), que o fundamento político do princípio da legalidade radica principalmente na função de garantia da liberdade do cidadão ante a intervenção estatal arbitrária, por meio da realização da certeza do direito. Respeitando-se tal princípio, assegura-se a existência de segurança jurídica e de garantia individual.

Por outro lado, quanto ao princípio da reserva legal, Bitencourt (2012, p. 49) afirma que “significa que a regulação de determinadas matérias deve ser feita, necessariamente, por meio de lei formal, de acordo com as previsões constitucionais a respeito. Nesse sentido, a Constituição brasileira, no seu art. 22, I, prevê que compete privativamente à União legislar sobre Direito Penal.

Segundo o mesmo autor, garante-se, assim, que nenhuma pessoa seja submetida ao poder punitivo estatal, se não com base em leis formais que sejam fruto do consenso democrático. Ou seja, ninguém será punido por um crime cibernético se, por exemplo, ele não estiver estritamente tipificado em lei, como por exemplo a invasão em sites e portais, conduta atualmente atípica no ordenamento jurídico brasileiro.

Deste modo, “somente as leis podem decretar as penas dos delitos, e esta autoridade só pode residir no legislador, que representa toda a sociedade unida por um contrato social” (BECCARIA, 1996, p. 44).

Na mesma linha, Prado, De Carvalho e De Carvalho (2014) dizem que o motivo que justifica a escolha do Legislativo como o único detentor do poder normativo em sede penal reside em sua legitimação democrática, fazendo com que justamente não seja arbitrário.

No entanto, sabe-se que a maioria das condutas danosas são passíveis de enquadramento, ainda que não exista o tipo penal adequado, como por exemplo o furto mediante fraude por meio eletrônico, em que há uma fraude para conseguir os dados bancários da vítima e posteriormente o furto de valores bancários.

Estas e outras possibilidades de enquadramento serão analisadas detalhadamente nos próximos capítulos, cotejando-se a legislação penal existente e as condutas ilícitas praticadas, especialmente no meio cibernético.

2.3 Princípio da humanidade

O princípio da humanidade, conforme preleciona Bitencourt (2012), é o maior entrave para a adoção da pena capital e da prisão perpétua. Esse princípio sustenta que o

poder punitivo não pode aplicar sanções que atinjam a dignidade da pessoa humana ou que lesionem a constituição físico-psíquica dos condenados.

Sustenta Ferrajoli (2014) que o cerne da questão é *como punir*, articulando-se em dois subproblemas: o da *qualidade* e o da *quantidade* da pena, afastando-se a antiga ideia de igualdade entre delito e pena, que vigorava desde o Código de Hamurabi com o princípio do talião (olho por olho, dente por dente).

Além de ser reconhecido pela Declaração Universal da ONU de 1948[1], o ordenamento jurídico brasileiro, mais especificamente a Constituição Federal de 1988, recepcionou tal princípio no art. 5º, conforme se vê:

> Art. 5º, XLIX. É assegurado aos presos respeito à integridade física e moral.
> Art. 5º, XLVII. Não haverá penas:
> a) De morte, salvo em caso de guerra declarada, nos termos do art. 84, XIX;
> b) De caráter perpétuo;
> c) De trabalhos forçados;
> d) De banimento;
> e) Cruéis.

Ainda, vista a sua importância, a dignidade da pessoa humana foi estabelecida pela Constituição Federal como fundamento do Estado Democrático de Direito, no seu art. 1º, III, sendo, portanto, vedada qualquer criação ou aplicação de pena que atente contra esse princípio.

Ramíres apud Prado, De Carvalho e De Carvalho (2014), ensina que é justamente na dignidade humana que radica o fundamento material do princípio da humanidade, visto que constitui o último e fundamental limite material à atividade punitiva do Estado.

Em desfavor das penas de morte, Beccaria (2002, p. 100) já demonstrava a sua indignação quanto a ofensa à dignidade humana:

> Parece-me absurdo que as leis, que são a expressão da vontade pública, que abominam e punem o homicídio, o cometam elas mesmas e que, para dissuadir o cidadão do assassínio, ordenem um assassínio público. Quais são as leis verdadeiras e mais úteis? São aqueles pactos e aquelas condições que todos desejariam propor e observar, enquanto se cala ou se funde com a do interesse público a voz sempre presente do interesse privado. Qual é o sentimento geral sobre a pena de morte? Ele se manifesta nos atos de indignação e de desprezo de cada um ao avistar o verdugo, que é, no entanto, um inocente executor da vontade pública, um bom cidadão que contribui para

[1] "Art. 1º: Todas as pessoas nascem livres e iguais em dignidade e direitos. São dotadas de razão e consciência e devem agir em relação umas às outras com espírito de fraternidade."

> o bem coletivo, o instrumento necessário à segurança pública interna, como os bravos soldados são para a externa.

Dessa forma, pactuando do mesmo raciocínio de Ferrajoli, Beccaria entende que a pena deve ser proporcional ao dano, e não à gravidade do delito, sob risco de se perder a finalidade de punir.

2.4 Princípio da inocência, contraditório e provas irrepetíveis em cibercrimes

O princípio da inocência, previsto no art. 5º, LVII, da Constituição Federal, proíbe expressamente que alguém seja considerado culpado até o trânsito em julgado de sentença penal condenatória. Portanto, segundo Colli (2010), a acusação deverá exercer uma mínima atividade probatória, objetivamente incriminadora, a fim de oportunizar um juízo condenatório.

Nas palavras de Nucci (2014, p. 34), "as pessoas nascem inocentes, sendo esse o seu estado natural, razão pela qual, para quebrar tal regra, torna-se indispensável que o Estado-acusação evidencie, com provas suficientes, ao Estado-juiz, a culpa do réu.

Nesse sentido, Tourinho Filho (2013, p. 73), preleciona:

> Aí está o princípio: enquanto não definitivamente condenado, presume-se o réu inocente. Claro que a expressão "presunção de inocência" não pode ser interpretada ao pé da letra, literalmente, do contrário os inquéritos e os processos não seriam toleráveis, visto não ser possível inquérito ou processo em relação a uma pessoa inocente. Sendo o homem presumidamente inocente, sua prisão antes do trânsito em julgado da sentença condenatória implicaria antecipação da pena, e ninguém pode ser punido antecipadamente, antes de ser definitivamente condenado, a menos que a prisão seja indispensável a título de cautela.

Esse princípio está intimamente ligado ao do contraditório e das provas irrepetíveis, particularmente nos cibercrimes, tendo em vista que a busca e apreensão de computadores e periféricos supostamente utilizados em um delito constitui verdadeiro meio de prova em fase pré-processual de investigação, sendo, como medida cautelar, irrepetível na fase judicial (COLLI, 2010).

Por isso, o mesmo autor aduz que o contraditório assume papel fundamental diante das provas periciais e das medidas de busca e apreensão que venham a ser realizadas nos casos de cibercrimes.

Em caso contrário, a análise de conteúdo de arquivos, por exemplo, estará sob o risco de esta atividade de obtenção dar origem a uma prova ilícita, vedada pelo art. 157, *caput*, do Código de Processo Penal[2].

Por sua vez, o contraditório, igualmente previsto no art. 5º, LV, da Carta Magna, garante o direito de defesa e a todos recursos a ela inerentes, inclusive na fase investigativa, pré-processual. No entendimento de Nucci (2014, p. 37), "quer dizer que a toda alegação fática ou apresentação de prova, feita no processo por uma das partes, tem o adversário o direito de se manifestar, havendo um perfeito equilíbrio na relação".

2.5 Princípio da territorialidade

Preconiza Bitencourt (2012) que em alguns casos, para um combate eficaz da criminalidade, pode ocorrer necessidade de que os efeitos da lei penal ultrapassem os limites territoriais para regular fatos ocorridos além de sua soberania, surgindo, assim, a necessidade de limitar a eficácia espacial da lei penal, justamente o que ocorre com os crimes cibernéticos, tema do presente trabalho.

Os delitos cibernéticos ocorrem em um ambiente peculiar com relação aos crimes normais, possibilitando que ultrapassem fronteiras. No entendimento de Colli (2010, p.30), esse local se chama ciberespaço e seria o ambiente constituído pela troca de informações transmitidas por cabos óticos:

> O ciberespaço seria o ambiente constituído pela troca de informações transmitidas por cabos óticos e por consequência por meio da luz, permite àqueles inseridos nesse ambiente o tráfego internacional e o acesso a dados remotos, restando usuários e máquinas em locais diferentes, possibilitando o cometimento de delitos que ultrapassam fronteiras.

[2] "Art 157, *caput*: São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais".

A lei penal brasileira adota como regra geral, pelo princípio da territorialidade, a sua aplicação aos fatos puníveis praticados no território nacional, independentemente da nacionalidade do agente, da vítima, ou do bem jurídico lesado, conforme dispõe o art. 5º, *caput*, do Código Penal:

> *Art. 5º, caput: Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.*

Segundo Nucci (2014), é a regra que assegura a soberania nacional, tendo em vista que não teria sentido aplicar normas procedimentais estrangeiras para apurar e punir um delito ocorrido dentro do território brasileiro.

No entanto, como toda regra tem sua exceção, um dos fatores de afastamento da aplicação da lei processual penal é a ressalva feita aos tratados, convenções e regras de direito internacional, prevista no art. 1º, I, do Código de Processo Penal[3], além da submissão do Brasil à jurisdição do Tribunal Penal Internacional a cuja criação tenha manifestado adesão, conforme dispõe o art. 5º, §4º, da Constituição Federal.

Um exemplo de exceção ao princípio da territorialidade é a passagem inocente, entendida por Gomes e Molina (2009) como aquela em que um navio estrangeiro está passando pelas águas brasileiras quando ocorre, dentro dele, um delito. É certo que o crime ocorreu em território nacional, mas se não existe nenhum brasileiro no caso, aplica-se o princípio da passagem inocente e vale o direito penal do país em que está registrado o navio.

Salienta-se que os navios e os aviões possuem regras peculiares para aplicação do direito penal, sujeitando-se ao princípio da extraterritorialidade, previsto no art. 7º do Código Penal, que não merecerá maior destaque por não ser objeto da pesquisa.

Outrossim, destaca-se que os crimes cibernéticos também possuem regras especiais para aplicação da legislação penal, pois, assim como os crimes cometidos nos navios e aeronaves, são delitos que ocorrem no espaço. Quanto a estes, a competência para processar e julgar receberá atenção especial mais adiante, em momento oportuno.

---

[3] "Art. 1º: O processo penal reger-se-á em todo o território brasileiro, por este Código, ressalvados: I – os tratados, as convenções e regras de direito internacional".

2.6 Conceito de crime

Após devidamente analisados o conceito e a função dos princípios, passar-se-á descrição do conceito de crime, que, invariavelmente, obedece aos princípios e decorre dos seus desdobramentos.

Como se verá, o conceito de crime, genérico a qualquer tipo de delito, inclusive aos crimes cibernéticos, merece atenção no presente trabalho para que se possa precisar a verdadeira caracterização do crime cometido, perpassando, dessa forma, pelos seus elementos integrantes.

Aqui, destaca-se principalmente o elemento da tipicidade, integrante do conceito analítico de crime, uma vez que é o principal obstáculo na persecução dos crimes cibernéticos, dada a evolução dos meios tecnológicos e o cometimento de novos delitos, exigindo-se, para a devida atuação do Estado como órgão repressivo e punitivo, a adequação típica.

O ordenamento jurídico brasileiro, por meio da Lei de Introdução ao Código Penal brasileiro (Decreto-lei n. 3.914/41), define crime da seguinte forma:

> Art. 1º. Considera-se crime a infração penal a que a lei comina pena de reclusão ou detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração a que a lei comina isoladamente pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente.

No entanto, Bitencourt (2012) entende que não existe ontologicamente diferença entre crime e contravenção, afirmando que a diferenciação é puramente político-criminal e o critério é simplesmente quantitativo, com base na sanção assumindo caráter formal. Dessa forma, o critério distintivo entre crime e contravenção seria dado pela natureza da pena privativa de liberdade cominada.

Como se percebe, a diferenciação de crime e contravenção se deu pela natureza da prisão aplicável, sem se preocupar com um conceito doutrinário. O atual Código Penal não traz a definição de crime, deixando a sua elaboração para a doutrina (BITENCOURT, 2012).

O conceito de crime, segundo Toledo (2000) é, substancialmente, um fato humano que lesa ou expõe a perigo bens jurídicos protegidos. No entanto, para ele, essa definição, que

por sinal se confunde com o conceito material de crime que será visto mais adiante, é insuficiente para a dogmática penal, que necessita de outra mais analítica, apta a pôr à mostra os aspectos essenciais ou os elementos estruturais do conceito de crime.

O significado de bem jurídico, no entendimento de Prado, de Carvalho e de Carvalho (2014, p. 219), "vem a ser um ente (dado ou valor social) material ou imaterial extraído do contexto social, de titularidade individual ou metaindividual, considerado como essencial para a coexistência e o desenvolvimento do homem".

Ainda, sabe-se que existem as definições de crime material e crime formal, que, juntamente com o conceito analítico de crime, serão analisadas a seguir.

2.6.1. Conceito material e formal de crime

O conceito material de crime está ligado, no entendimento de Bitencourt (2012), à ação ou omissão que contraria os valores ou interesses do corpo social, exigindo uma proibição com a ameaça de pena.

Na mesma linha, Prado, de Carvalho e de Carvalho (2014) entendem que o conceito material está ligado ao conteúdo do ilícito penal – caráter danoso da ação ou seu desvalor social -, quer dizer, o que determinada sociedade, em dado momento histórico, considera que deve ser proibido pela lei. Nesse sentido, com a identificação da sociedade acerca dos bens jurídicos a serem protegidos e da gravidade da sua violação, serão elaboradas as políticas criminais.

Por outro lado, o conceito formal define crime como toda ação ou omissão proibida por lei, sob a ameaça de pena (BITENCOURT, 2012).

Corroborando este entendimento, Prado, de Carvalho e de Carvalho (2014) prelecionam que o conceito formal é a simples definição do delito sob o ponto de visto do Direito positivo, isto é, o que a lei incrimina, consistindo, portanto, na relação de contrariedade entre o fato e a lei penal. Temos como simples exemplo o art. 121 do Código Penal: "Matar alguém", em que o legislador descreve o delito de homicídio.

Contudo, é cediço que os conceitos formal e material são insuficientes para permitir à dogmática penal a realização de uma análise de elementos estruturais do conceito de crime (BITENCOURT, 2012). Assim, na sequência, passará a ser feita a análise do conceito analítico de crime, aquele entendido como o mais completo.

2.6.2 Conceito analítico de crime

Prado, de Carvalho e de Carvalho (2014) fazem uma análise histórica-evolutiva, mencionando que a ação, como primeiro requisito do delito, só apareceu com Berner (1857), sendo que a ideia de ilicitude, desenvolvida por Ihering (1867) para a área civil, foi introduzida no Direito Penal por obra de Von Lizst e Beling (1881), e a de culpabilidade, com origem em Merkel, desenvolveu-se pelos estudos de Binding (1877).

Segundo o mesmo autor, posteriormente, no início do século XX, graças a Beling (1906), surgiu a ideia de tipicidade. Todo esse desenvolvimento culminou com a formulação atualmente adotada: conduta típica, ilícita e culpável (concepção tripartida).

Diante da concepção tripartida, surgiu a moderna teoria finalista criada por Hans Welzel na década de 1930, consistindo que a ação penal consiste na proposição do fim, na escolha dos meios necessários e na realização da ação no mundo real (ZAFFARONI; PIERANGELI, 2004).

Por oportuno, cumpre ressaltar que existem teorias que acrescentam o elemento da punibilidade (Nelson Hungria) e outras que excluem a culpabilidade, chamadas quadripartidas e bipartidas, respectivamente. Contudo, a maior discussão doutrinária se dá nas teorias bipartida e tripartida, sendo a culpabilidade o foco da problemática.

Somente a título de argumentação, eis que o conceito de crime não é o foco da pesquisa, em relação à primeira hipótese cabe dizer que a punibilidade é consequência do crime, sendo, portanto, possibilidade de aplicação da pena e não elemento constitutivo, isto é, agregado ao conceito de crime. Ao contrário, pressupõe a existência de um crime já aperfeiçoado (TOLEDO, 2000).

No tocante à segunda possibilidade, de exclusão do elemento culpabilidade, a teoria bipartida defende o delito como sendo uma conduta típica e ilícita, afirmando ser a culpabilidade pressuposto da pena, e não elemento constitutivo daquele. No entanto, ao ver de Prado, de Carvalho e de Carvalho (2014), além de ser falto em relação ao encadeamento regular (em contradição do pensamento discursivo), carece esse posicionamento de fundamentação sólida em termos metodológicos.

Assim, superadas as considerações iniciais sobre os conceitos de crime, o presente trabalho adotará o sistema tripartido de crime, passando em seguida a fazer a análise individual dos elementos do conceito analítico de crime, quais sejam: a tipicidade, a ilicitude e a culpabilidade.

2.6.2.1 Tipo e Tipicidade penal

Tipo, segundo o entendimento de Greco (2014, p. 38), "como a própria denominação nos está a induzir, é o modelo, o padrão de conduta que o Estado, por meio de seu único instrumento, a lei, visa impedir que seja praticada ou determina que seja levada a efeito".

Podemos citar, como exemplo, a proteção do patrimônio por parte do Estado, com a criação do tipo existente no art. 155, *caput*, do Código Penal, conforme se vê:

> Art. 155. Subtrair, para si ou para outrem, coisa alheia móvel:
> Pena – reclusão, de 1(um) a 4(quatro) anos, e multa.

Com essa redação, Greco (2014) entende que o Estado descreve, precisamente, o modelo de conduta que quer proibir, sob pena de quem lhe desobedecer ser punido de acordo com as sanções previstas em seu preceito secundário. Quando isso acontecer, surgirá outro fenômeno, chamado tipicidade.

A tipicidade, conforme preleciona Bitencourt (2012), é uma decorrência natural do princípio da reserva legal: *nullum crimen nulla poena signe praevia lege*, abordado anteriormente juntamente com os demais princípios limitadores do poder punitivo estatal. É a conformidade do fato praticado pelo agente com a moldura abstratamente descrita na lei penal, isto é, a conduta praticada pelo agente deve subsumir-se na moldura descrita na lei.

Além disso, há doutrinadores que entendem que a tipicidade penal é composta da fusão entre a tipicidade formal e a tipicidade conglobante. No entendimento de Greco (2014), esta última surgiria quando comprovado que a conduta praticada pelo agente é considerada antinormativa, ou seja, contrária à norma penal, bem como ofensiva a bens de relevo para o direito penal. Dessa forma, a tipicidade conglobante seria conjugada pela antinormatividade (conduta contrária à norma penal) e pela tipicidade material (lesão ao bem jurídico).

Na mesma linha, Zafaroni e Pierangeli (2004), prelecionam que o juízo de tipicidade não é um mero juízo de tipicidade legal, mas, antes, de tipicidade penal, que somente se verifica depois de comprovada a tipicidade conglobante, como corretivo da tipicidade legal.

Assim, conceituada a tipicidade penal, passa-se a descrever apenas as formas do tipo doloso, com o objetivo de delimitar a estrutura típica dos crimes cibernéticos.

Nesse sentido, a doutrina divide o tipo do injusto punível doloso em objetivo e subjetivo, sendo, na ótica de Bitencourt (2012), objetivo o tipo aquele que descreve todos os elementos objetivos que identificam e limitam o teor da proibição penal: o sujeito ativo, a conduta proibida, o objeto da conduta, as formas e meios da ação, o resultado, a relação de causalidade, etc.

Segundo o mesmo autor, o tipo subjetivo tem relação com todos os aspectos subjetivos do tipo de conduta proibida que, concretamente, produzem o tipo objetivo. É constituído de um elemento geral, o *dolo*, que nada mais é do que a intenção do agente, tipificado no art. 18, I, do Código Penal[4].

Com efeito, todo crime é a descrição de uma conduta, que pode ser realizada mediante ação ou omissão. Há uma classificação em crimes formais (ou de mera conduta) como sendo aqueles em que não é exigido resultado da ação e os crimes materiais, aqueles em que é exigido um resultado ou dano (BITENCOURT, 2012).

O Código Penal adotado por nós utiliza a teoria chamada da equivalência dos antecedentes ou da *conditio sine qua non*, não distinguindo entre causa e condição. É o que dispõe o art. 13 do Código Penal, *in verbis*:

[4] "Art. 18: Diz-se o crime: I - doloso, quando o agente quis o resultado ou assumiu o risco de produzi-lo".

> Art. 13: O resultado, de que depende a existência do crime, somente é imputável a quem lhe deu causa. Considera-se causa a ação ou omissão sem a qual o resultado não teria ocorrido.

Dessa forma, conforme explica Toledo (2000), depreende-se que somente no caso em que se verifique uma interrupção de causalidade, ou seja, quando sobrevém uma causa que, sem cooperar propriamente com a ação ou omissão produz por si só o evento, que não poderá ser atribuído ao agente.

Nesse sentido, Bitencourt (2012) reforça a ideia de que, além da relação de causalidade nos crimes materiais, é necessário demonstrar que o resultado constitui precisamente a realização do risco proibido criado pelo autor através de sua conduta.

Segundo o autor supracitado quanto ao tipo subjetivo, o dolo constitui a consciência e a vontade de realização da conduta descrita em um tipo penal, sendo composto por dois elementos: o cognitivo (consciência daquilo que pretende praticar) e o volitivo (vontade de abranger a ação ou omissão).

De outra banda, o tipo injusto doloso ainda pode ser classificado em omissivo, aqueles em que os tipos penais incriminadores que se expressam em proibições e mandamentos ou ordens (PRADO; DE CARVALHO; DE CARVALHO, 2014).

Esse tipo de delito, nas palavras de Bitencourt (2012), pode ser omissivo quando o agente não faz o que pode e deve fazer, que lhe é juridicamente ordenado. Ainda, há uma divisão entre crimes omissivos próprios e impróprios (ou comissivos por omissão). Um exemplo clássico do crime omissivo próprio é aquele previsto no caput do art. 135 do Código Penal[5], bastando a mera conduta para que o delito se consume, sendo o resultado mero exaurimento e majorante da pena.

Por outro lado, os crimes omissivos impróprios são, segundo o mesmo autor, aqueles em que o agente tem o dever de agir para evitar um resultado concreto, e não o simples dever de agir, sendo, portanto, um crime de resultado (material). O nosso Código Penal, no art. 13, § 2º, definiu os casos em que a omissão é penalmente relevante nos casos omissivos impróprios, como por exemplo, do policial que tem obrigação legal de proteção:

[5] "Art. 135: Deixar de prestar assistência, quando possível fazê-lo sem risco pessoal, à criança abandonada ou extraviada, ou à pessoa inválida ou ferida, ao desamparo ou em grave e iminente perigo; ou não pedir, nesses casos, o socorro da autoridade pública".

> Art. 13, § 2º: A omissão é penalmente relevante quando o omitente devia e podia agir para evitar o resultado. O dever de agir incumbe a quem:
> a) tenha por lei obrigação de cuidado, proteção ou vigilância;
> b) de outra forma, assumiu a responsabilidade de impedir o resultado;
> c) com seu comportamento anterior, criou o risco da ocorrência do resultado.

Assim, analisado o tipo e a tipicidade penal, passa-se a descrever a ilicitude e a culpabilidade, eis que elementos integrantes do conceito analítico de crime.

2.6.2.2 Antijuricidade ou ilicitude

Quanto a este elemento, Bitencourt (2012) anota que alguns autores utilizam equivocadamente a expressão "antijuricidade" para definir o próprio injusto, que é a ação qualificada de antijurídica, levando essa ambiguidade de sentidos a equívocos, pois trata-se de conceitos absolutamente distintos.

Para o mesmo autor, o injusto é a forma de conduta antijurídica propriamente, como por exemplo, a perturbação arbitrária da posse, o furto etc. Por outro lado, a antijuridicidade é uma qualidade dessa forma de conduta, mais precisamente a contradição em que se encontra com o ordenamento jurídico.

A reforma penal de 1984, seguindo a orientação de Assis Toledo, adotou a terminologia ilicitude, abandonando a tradicional, antijuridicidade, que o Código Penal de 1940 utilizava.

Assim, com base na lição de Toledo (2000, p. 161), entende-se por ilicitude o fato humano que se apresente em oposição à ordem jurídica:

> Nesse sentido, um fato humano – qualquer que seja – será ilícito sempre que se apresente em oposição à ordem jurídica, estabelecendo com esta uma relação de contraposição. E isso ocorre tanto com o fazer o proibido pelo ordenamento jurídico quanto com o não fazer o que está determinado por esse mesmo ordenamento. A ilicitude penal, é, assim, a propriedade de certos comportamentos humanos, seja sob a forma de ação, seja sob a forma de omissão, de se oporem à ordem jurídica.

Passada a divergência de conceitos, podemos entender, conforme Bitencourt (2012), que a antijuridicidade pode ser dividida em formal e material. Aquela, seria a contradição da ação com o mandamento ou proibição da norma, enquanto essa, seria mais precisamente a

ofensa produzida pelo comportamento humano ao interesse jurídico protegido, ou seja, a lesão ao bem jurídico.

Complementando, o autor supramencionado ainda aduz que o ordenamento jurídico valora dois aspectos: de um lado, o desvalor da ação, digamos, com uma função seletiva, destacando certas condutas como intoleráveis para o direito penal, e, de outro lado, o desvalor do resultado que torna relevante para o direito penal aquelas ações que representam uma ofensa aos bens jurídicos tutelados.

Por outro lado, é mister fazer uma distinção entre antijuricidade e antinormatividade. No entendimento de Zaffaroni e Pierangeli (2004, p. 437):

> A antijuricidade pressupõe antinormatividade, mas não é suficiente a antinormatividade para configurar a antijuricidade, pois a antinormatividade pode ser neutralizada por um preceito permissivo. Dito em outras palavras, posto que a tipicidade penal implica a antinormatividade, a antijuricidade com relevância penal pressupõe a tipicidade. Neste sentido, a tipicidade atua como um indício da antijuricidade, como um desvalor provisório, que deve ser configurado ou desvirtuado mediante a comprovação das causas de jusitificação.

As causas de justificação ou excludentes de ilicitude estão previstas no nosso ordenamento jurídico especificamente no art. 23 e incisos do Código Penal, *in verbis*:

> Art. 23 – Não há crime quando o agente pratica o fato:
> I – em estado de necessidade;
> II – em legítima defesa;
> III – em estrito cumprimento de dever legal ou no exercício regular de direito.

Entretanto, essas causas de justificação não serão objeto de análise neste trabalho. Assim, após a análise do fato típico e da ilicitude, passamos ao último elemento integrante do conceito analítico de crime, qual seja, a culpabilidade.

2.6.2.3 Culpabilidade

O último elemento integrante do conceito analítico de crime, a culpabilidade, pode ser entendido, na visão de Bitencourt (2012), como um juízo individualizado de atribuição de responsabilidade penal, e representa uma garantia para o infrator frente aos possíveis excessos do poder punitivo estatal.

Pode se entender que essa compreensão provém do princípio de que não há pena sem culpabilidade: *nulla poena sine culpa*. Nesse sentido, a culpabilidade apresenta-se como fundamento e limite para a imposição de uma pena justa.

Por outro lado, a culpabilidade também é entendida como um instrumento para a prevenção de crimes e, sob essa ótica, o juízo de atribuição de responsabilidade penal cumpre com a função de aportar estabilidade ao sistema normativo, confirmando a obrigatoriedade do cumprimento das normas (BITENCOURT, 2012).

Outrossim, Prado, de Carvalho e de Carvalho (2014) ensinam que a culpabilidade tem na liberdade do homem de poder atuar de modo diverso seu fundamento ontológico, como dado real e inerente à sua própria condição de pessoa humana livre e responsável. Sendo, pois, a reprovabilidade da vontade final.

Ainda, segundo o autor supracitado, a teoria finalista do direito penal redefiniu a culpabilidade com base nos seus elementos, quais sejam: a imputabilidade (capacidade de motivação); consciência da ilicitude (requisito da motivação) e exigibilidade de outra conduta (necessidade de motivação).

A imputabilidade, nas palavras de Bitencourt (2012, p. 448) é "a capacidade ou aptidão para ser culpável, embora, convém destacar, não se confunda com responsabilidade, que é o princípio segundo o qual o imputável deve responder". Assim, seguindo a teoria de Welzel, pressupõe-se que a capacidade de culpabilidade apresenta dois momentos específicos: um intelectual e outro de vontade, isto é, a capacidade de compreensão do injusto e a determinação da vontade conforme essa compreensão. Sem a presença desses dois elementos a capacidade de culpabilidade fica descaracterizada, afastando-se, portanto, a imputabilidade penal.

Algumas causas de exclusão de imputabilidade são descritas no nosso ordenamento jurídico, mais precisamente no art. 26 do Código Penal[6], como por exemplo a menoridade, a

[6] "Art. 26: É isento de pena o agente que, por doença mental ou desenvolvimento mental incompleto ou retardado, era, ao tempo da ação ou omissão, inteiramente incapaz de entender o caráter ilícito do fato ou de determinar-se de acordo com esse entendimento. Art. 27: Os menores de 19 (dezoito) anos são penalmente inimputáveis, ficando sujeitos às normas estabelecidas na legislação especial. Art. 28, §1º: É isento de pena o agente que, por embriaguez completa, proveniente de caso fortuito ou força maior, era, ao tempo da ação ou da omissão, inteiramente incapaz de entender o caráter ilícito do fato ou de determinar-se de acordo com esse entendimento."

doença mental, o desenvolvimento mental incompleto ou retardado e a embriaguez acidental incompleta.

O outro elemento da culpabilidade, a potencial consciência da ilicitude, é entendida como a consciência ou o conhecimento atual ou possível da conduta, ou seja, da possibilidade de o agente poder conhecer o caráter ilícito de sua ação (PRADO; DE CARVALHO; DE CARVALHO, 2014).

Portanto, basta que o agente tenha conhecimento potencial que o seu comportamento contraria ao ordenamento jurídico. Entrementes, está previsto, quando inevitável, uma causa de excludente de culpabilidade chamada erro de proibição, prevista no art. 21 do Código Penal, *in verbis*:

> Art. 21 O desconhecimento da lei é inescusável. O erro sobre a ilicitude do fato, se inevitável, isenta de pena; se evitável, poderá diminuí-la de um sexto a um terço.

Por fim, o último elemento da culpabilidade, a exigibilidade da conduta diversa, tem relação com a possibilidade de se exigir comportamento diverso do que teve. Há casos em que se acha fortemente atenuada a possibilidade de agir conforme a norma (PRADO; DE CARVALHO; DE CARVALHO, 2014).

Esses casos, conhecidos como causas de exclusão de exigibilidade de conduta diversa ou causas de inexigibilidade de conduta diversa, estão previstos no art. 22 do Código Penal[7] e excluem a culpabilidade do agente. São elas a coação moral irresistível, que exclui a ação por inexistência de vontade, e a obediência hierárquica ou devida.

Destarte, analisados os conceitos preliminares e princípios relativos aos crimes cibernéticos que interessam à pesquisa, descrever-se á, no próximo capítulo, uma análise histórica dos crimes cibernéticos no Brasil, conceito de crime cibernético, com especial análise e atenção à legislação vigente.

[7] "Art. 22: Se o fato é cometido sob coação irresistível ou em estrita obediência a ordem, não manifestamente ilegal, de superior hierárquico, só é punível o autor da coação ou da ordem".

3 ABORDAGEM SOBRE OS CRIMES CIBERNÉTICOS NO BRASIL E A LEI N. 12.737/12

A modernidade, especialmente após o século XXI, trouxe consigo inúmeras transformações devido ao avanço da tecnologia. A internet, por exemplo, revolucionou o modo e comunicação das pessoas e a transmissão de dados e informações, encurtando espaços. Contudo, juntamente com os benefícios, sobrevieram novos meios e novos 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, este capítulo terá o objetivo de estudar legislação vigente sobre crimes cibernéticos no Brasil, perpassando por uma análise histórica da internet, pelo conceito de crime cibernético, pela evolução histórica dos crimes cibernéticos no Brasil e finalmente pela análise da legislação brasileira específica sobre esses crimes.

3.1 Breve análise histórica da internet

A grande revolução tecnológica promovida durante o século XXI culminou principalmente em uma nova forma de comunicação através de um novo meio, a internet. Com isso, os espaços foram encurtados e a comunicação entre pessoas de lados opostos do globo foi possível. Contudo, juntamente com os benefícios, infelizmente a internet trouxe consigo malefícios, tendo se tornado em um local para o cometimento de novos delitos, chamados crimes cibernéticos.

Nesse sentido, faz-se necessária uma análise histórica do surgimento dessa nova ferramenta, a fim de que seja possível entender a sua evolução e como se tornou alvo dos criminosos.

A internet, como ensina 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 Colli (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, posteriormente, por meio da intercomunicação entre computadores de diferentes universidades, a rede fosse expandida para os chamados *Personal Commputers* (PC) (COLLI, 2010).

Ainda, no ano de 1986, foi implementado a NSFNET, pela National Science Foundation, e 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:

> Foi crucial a criação da WWW – World Wide Web -, pelos engenheiros Robert Caillaiu e Tim Berners-Lee. Criadores também do HTML – HyperText Markup

> Language – e também dos browsers. A internet transforma-se num sistema mundial público, de redes de computadores (DAVID apud WENDT; JORGE, 2013, p.8).

Acrescenta Guizzo (2002, p. 22) que "esse emaranhado de redes acadêmicas, comerciais e militares, tendo como espinha dorsal a NFSNET e como padrão o TCP/IP, acabou evoluindo para o que hoje conhecemos como Internet".

A partir disso, segundo o autor acima mencionado, foi que estudantes, professores, pesquisadores e pessoas de todas as profissões começaram a se ligar na rede, sendo assim, que a Internet acabou se transformando no maior sistema de comunicação do mundo.

3.1.1 A internet no Brasil

No 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 (COLLI, 2010).

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.

Complementa Guizzo (2002) que em 1989 a comunidade acadêmica, com o apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), criou a Rede Nacional de Pesquisas (RNP), que por sua vez, implantou uma rede de abrangência nacional que interligava diversas capitais brasileiras.

Segundo o mesmo autor, foi em meados de 1994, com grande contribuição da RNP e do Ibase (Instituto Brasileiro de Análises Sociais e Econômicas), que a Internet ultrapassou as fronteiras acadêmicas e começou a chegar aos ouvidos de muitos brasileiros, passando a desenvolver-se até se tornar a grande ferramenta de hoje.

Fundamental para a coordenação e incentivo da implantação da Internet no nosso país foi a criação do Comitê Gestor da Internet/BR, que foi instituído em 1995, no governo

Fernando Henrique Cardoso. A atribuição deste órgão era (e ainda é) coordenar e incentivar a implantação da internet no Brasil, tratando-se de uma espécie de espinha dorsal desta rede no país (COLLI, 2010).

A consolidação da Internet em nosso país veio no ano de 1997, com a propagação da novidade através de revistas, difusão de novos provedores e a adesão em massa das instituições, conforme Guizzo (2002, p. 27):

> O ano de 1997 veio consolidar a Internet tupiniquim. Novas revistas sobre o assunto foram lançadas. Os provedores chegaram a diversas centenas. O conteúdo em língua portuguesa na rede tornou-se significativo. Empresas, bancos, universidades e até o governo fizeram questão de marcar presença na Internet. Algumas estimativas mais otimistas diziam que o número de usuários no Brasil passou de um milhão naquele ano. Mas não há certeza.

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 e etc.

Por oportuno, com relação ao *IP* (Internet Protocol), cumpre destacar que ele atribui a cada computador conectado um endereço exclusivo (endereço IP). Assim, é possível localizar qualquer computador conectado à rede e trocar dados com ele, sendo, portanto, possível a sua localização (SAWAYA, 1999).

A distribuição desses IPs, segundo Wendt e Jorge (2013), é feita internacionalmente pela IANA, que é a autoridade responsável. Aos usuários são atribuídos endereços de Ips por provedores de serviço Internet (Internet Service Providers – ISPs), que são divididos em autoridades regionais para distribuição dos blocos de endereços de Ips, sendo a LACNIC a responsável na América Latina e no Caribe.

Como veremos mais adiante, o IP é um grande aliado e, muitas vezes, o único, dos investigadores de crimes cibernéticos, por possibilitar, em algumas situações, a localização do usuário e possível autor do delito praticado. Aliás, este é um dos grandes desafios da persecução penal dos crimes cibernéticos, tendo em vista que o anonimato da rede virtual é um dos fomentos desse tipo de crime.

3.2 Conceito de crime cibernético

Devidamente analisado o contexto histórico do surgimento da internet, faz-se necessária a descrição do que são e de qual é o conceito dos crimes cibernéticos, bem como da sua positivação no ordenamento jurídico do nosso país.

Embora ainda não exista na doutrina um conceito pacificado sobre crimes cibernéticos, sendo, inclusive, tratados como sinônimo de crimes virtuais, informáticos, digitais e 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 utilizado 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.

O mesmo autor afirma que os crimes cibernéticos, dentro do gênero dos crimes informáticos, são aqueles 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. Podemos citar, adiantando a exposição do próximo capítulo, 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 indicado 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. 8.069/90, e o próprio crime invasão de dispositivo informático previsto no art. 154-A do Código Penal, que será detidamente analisado no próximo capítulo.

Os abertos, segundo o autor supramencionado, são aqueles que podem ser praticados de forma tradicional ou por intermédio dos computadores, 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.

Existem, ainda, aqueles crimes praticados por funcionário público contra a administração em geral, previstos nos arts. 313-A e 313-B do Código Penal, que tipificam a conduta de inserção de dados falsos em sistema de informação e de modificação ou alteração não autorizada de sistema de informação, respectivamente. Ou seja, há diversos tipos penais em nosso ordenamento que preveem o cometimento de delitos exclusivamente cibernéticos, não sendo o objeto da pesquisa esgotar a análise de todas as possibilidades, somente exemplifica-las, tendo em vista que o foco principal está no art. 154-A do Código Penal.

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).

Adotaremos, para fins de melhor didática 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.

3.3 Contexto histórico dos crimes cibernéticos no Brasil

Devidamente conceituados os crimes cibernéticos, é pertinente abordar como esse tipo de delito surgiu no nosso país, como se deu a sua evolução e como o Estado reagiu para tentar se contrapor e exercer o seu *jus puniendi*.

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, nova 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, pela alta movimentação financeira, 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 vinte e dois signatários, sendo que o Brasil, até agora, não a ratificou.

Essa convenção, segundo Colli (2010), teve entre os seus principais objetivos a harmonização de elementos relativos a infrações penais na área da cibercriminalidade, a definição de poderes necessários para investigar e intentar ações penais em cada Estado e a implantação de um regime de cooperação internacional rápido e eficaz.

Os debates acerca da adesão do nosso país à Convenção são controvertidos, pois, conforme Dodge (2013), de maneira geral, recebe apoio de autoridades brasileiras (Polícia Federal, por exemplo) e de outro não conta com o mesmo entusiasmo, como do Ministério das Relações Exteriores.

Várias questões tratadas nessa Convenção poderiam ser discutidas e aperfeiçoadas para a criação de uma legislação eficaz contra os crimes cibernéticos no nosso país, cabendo aos legisladores tal questão, uma vez que, conforme veremos a seguir, a nossa legislação de crimes cibernéticos vigente é demasiadamente frágil.

3.3.1 A edição da Lei n. 12.737/12: Lei Carolina Dieckmann

Com o objetivo de oferecer mais condições para a punição dos crimes cibernéticos, 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 obteve aprovação na Câmara Federal no ano de 2003, passou a tramitar no Senado e, 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 12.735/12), 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. Convém lembrar que os logs guardam informações sobre a utilização de determinado serviço na internet pelo usuário, contendo data, horário e número do IP, sendo, portanto, bastante úteis na identificação do autor do delito (WENDT; JORGE, 2013).

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, que prevê a interrupção de sistema telemático ou de informações de utilidade pública, e ainda acrescenta ao artigo 298 o § único, que faz a equiparação dos cartões de crédito ou de débito a documento particular, para efeitos de incriminação do *caput*.

No entanto, a referida lei tem sido alvo de bastante discussão na doutrina. Especificamente, o tipo penal previsto no art. 154-A do Código Penal, introduzido pela Lei 12.737/12, atualmente em foco por virtude da numerosa troca de dados e informações por

meio da Internet, será objeto de estudo do próximo capítulo, que versará sobre a sua (in)eficácia.

3.4 Projetos de Lei em andamento no Brasil

Perpassada a análise do conceito de crime cibernético e da sua positivação em nosso ordenamento jurídico, passar-se-á, para fins de complementação do estudo, à abordagem dos projetos de leis em tramitação no Brasil com relação a esses delitos, propostos justamente para suprir as lacunas existentes.

Recentemente, no dia 23.04.l4 foi sancionada a Lei n. 12.965/14, conhecida como Marco civil da internet. Ela estabelece alguns princípios, garantias, direitos e deveres para o uso da internet no Brasil, estabelecendo, 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 confidencialidade, 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.

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 de 2015, de autoria do Senador Romario Faria, que pretende 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[8], 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.

Há ainda em tramitação, o projeto de lei n. 5369 de 2009, de autoria do Deputado Federal Vieira da Cunha, que pretende tornar crime a prática de *bullying*, inclusive o praticado virtualmente, pela internet. O projeto está atualmente aguardando designação do relator, após parecer da Comissão de Segurança Pública e Combate ao Crime Organizado.

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 de 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.

Dessa forma, analisados os projetos de lei existentes, passar-se-á, no próximo subcapítulo, a descrever-se, ainda que brevemente, algumas características e peculiaridades da persecução penal dos crimes cibernéticos, eis que indissociável a vinculação do direito material com o processual, dada a peculiaridade dos crimes cibernéticos.

3.5 Características e peculiaridades da persecução penal dos crimes cibernéticos

Tendo em vista que os crimes cibernéticos são delitos *sui generis* pois existe uma limitação do tema relacionada ao uso da rede mundial de computadores, a sua investigação difere um pouco daquelas dos crimes comuns.

[8] “Art. 139: Difamar alguém, imputando-lhe fato ofensivo à sua reputação”.

A persecução penal, nas palavras de Tourinho Filho (2013), apresenta dois momentos distintos: o da investigação policial e o da ação penal, sendo que esta consiste no pedido de julgamento da pretensão punitiva, enquanto aquele é atividade preparatória da ação penal, de caráter preliminar e informativo.

Na etapa policial, Wendt e Jorge (2013) sustenta que o processo investigativo de crimes cibernéticos contém diferentes fases: a inicial (técnica) e a consequencial (campo), de investigação policial propriamente dita.

Segundo o mesmo autor, durante o período da fase técnica da investigação, são executadas e analisadas algumas tarefas e/ou informações, cujo objetivo único é localizar o computador que foi utilizado para a ação criminosa. Ao analisar as informações recebidas, inclusive através da quebra de dados autorizada pelo Poder Judiciário, pode ser necessária, ainda, representações perante o provedor de conexão ou conteúdo de dados, com a finalidade de complementar o conjunto probatório.

Jordão apud Wendt e Jorge (2013) destaca que, quando ocorre a conexão de um computador ou dispositivo similar à internet (celular, tablet, etc.), o endereço de IP (Internet Protocol) é atribuído exclusivamente para aquele internauta, permitindo, assim, a identificação e localização do computador que permitiu a conexão e o acesso criminoso na internet.

A partir desse momento, segundo Wendt e Jorge (2013), surge a denominada fase de campo, quando há necessidade de deslocamento de agentes policiais para realização de diligências com o intuito de promover o reconhecimento operacional no local, sempre de maneira discreta, pois poderá haver a necessidade de solicitar uma medida processual penal cautelar.

Superados todos os desafios supramencionados da investigação policial, a persecução criminal continua com a ação penal, que, segundo Nucci (2014), é o direito do Estado- acusação ou do ofendido de ingressar em juízo, solicitando a prestação jurisdicional, representada pela aplicação das normas de direito penal ao caso concreto.

Neste momento, temos outros desafios a serem enfrentados, principalmente os conflitos de competências. Colli (2010) diz que isto se deve ao fato de que em uma infração

penal desta natureza podem existir diversos critérios a orientar o local onde, de fato, houve a consumação.

Segundo o mesmo autor, podemos citar: a) local onde se encontrava o sujeito ativo do crime (quem, por exemplo publica um vídeo de pornografia infantil na rede); b) local onde se encontrava o sujeito passivo do crime (quem visualiza o vídeo); c) o local do servidor que armazena o vídeo (tendo em vista que é ali que estão os dados acessados); d) ou ainda, não há como se estabelecer onde ocorreu a infração, pois ocorrida em ambiente que não possui *locus* definido (intangibilidade online).

Neste sentido, ao analisar o Conflito de Competência n. 66.981/RJ, o Superior Tribunal de Justiça definiu, de acordo com o art. 70 do Código de Processo Penal, que a infração de pornografia infantil se consumou no momento da publicação das imagens na internet, sendo, portanto, competente para processar e julgar o delito o local da publicação ilícita, que, no caso, ocorreu em São Paulo. A sua ementa é a seguinte:

> CONFLITO NEGATIVO DE COMPETÊNCIA. PROCESSO PENAL. VEICULAÇÃO NA INTERNET DE IMAGENS PORNOGRÁFICAS ENVOLVENDO CRIANÇAS E ADOLESCENTES. COMPETÊNCIA QUE SE FIRMA PELO LOCAL DA PUBLICAÇÃO ILÍCITA. 1. Conforme entendimento desta Corte, o delito previsto no art. 241 da Lei 8.069/90 consuma-se no momento da publicação das imagens, ou seja, aquele em que ocorre o lançamento na Internet das fotografias de conteúdo pornográfico. É irrelevante, para fins de fixação da competência, o local em que se encontra sediado o responsável pelo provedor de acesso ao ambiente virtual. 2. Conflito conhecido para determinar competente o suscitado, Juízo Federal da 1ª Vara Criminal, do Júri e das Execuções Penais da Seção Judiciária do Estado de São Paulo. (CC 66.981/RJ, Rel. Ministro OG FERNANDES, TERCEIRA SEÇÃO, julgado em 16/02/2009, DJe 05/03/2009)

Cumpre destacar, por oportuno, que o nosso ordenamento jurídico adotou a teoria da ubiquidade, prevista no art. 6º do Código Penal[9], que adota o lugar do crime como sendo aquele em que se realizou qualquer dos momentos do *iter criminis*, seja da prática dos atos executórios, seja da consumação (INELLAS, 2009).

Acontece que, conforme exposto acima, nos crimes cibernéticos o *iter criminis* se desenrola em lugares diferentes, inclusive em outros países. Surge aí o grande problema da competência para processar e julgar esse tipo de delito, tendo em vista que devem ser obedecidos os princípios da territorialidade e da soberania nacional, explicitados no primeiro capítulo do trabalho.

[9] "Art. 6 º: Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado".

A dúvida sobre a competência para processar e julgar também está entre a atuação da Justiça Estadual ou da Justiça Federal. Dodge (2013), explica que nas modalidades publicar ou divulgar fotografias, vídeos ou outros registros por meio da Internet, com utilização de comunidades de relacionamento por exemplo (Facebook, etc), a competência será da Justiça Federal. A previsão da tutela encontra-se em tratado ou convenção internacional e há a internacionalidade do fato, nos termos do art. 109, V, da Constituição Federal[10].

Com relação aos diretos da criança, destaca-se, por oportuno, que o Brasil é signatário da Convenção sobre os Direitos da Assembleia das Nações Unidas, de 20 de novembro de 1989, com a ratificação em 24 de setembro de 1990, e entrada em vigor no país em 23 de outubro de 1990, através do Decreto n. 99.710/90.

Outrossim, é sabido que os delitos de divulgação ou publicação de fotos através de comunidades de relacionamentos são acessíveis em qualquer local do planeta, desde que se esteja conectado à rede mundial de computadores, caracterizando-se, portanto, a internacionalização do delito e consequentemente a competência da Justiça Federal para processar e julgar, independentemente da comprovação de que o resultado se deu no exterior.

Contudo, caso a troca de fotografias se dê através de e-mail, por exemplo, entre pessoas residentes no Brasil, a competência será da Justiça Estadual, tendo em vista que não há internacionalidade pela divulgação nos limites do território nacional e a sua competência é residual.

Este é o entendimento do Superior Tribunal de Justiça, que através do julgamento do Conflito de Competência n. 111.338/TO, definiu que os casos em matéria de divulgação de imagens pornográficas afetos à Justiça Federal são aqueles em que as comunidades de relacionamentos são utilizadas, ao passo que a troca de e-mails entre pessoas residentes no Brasil é de competência da Justiça Estadual:

> CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSO PENAL. DIVULGAÇÃO DE IMAGENS PORNOGRÁFICAS DE CRIANÇAS E ADOLESCENTES POR MEIO DA INTERNET. CONDUTA QUE SE AJUSTA ÀS HIPÓTESES PREVISTAS NO ROL TAXATIVO DO ART. 109 DA CF. COMPETÊNCIA DA JUSTIÇA FEDERAL. 1. Este Superior Tribunal de Justiça tem entendido que só o fato de o crime ser praticado pela rede mundial de computadores não atrai a competência da Justiça Federal. 2. A competência da Justiça Federal é

[10] "Art. 109: Aos juízes federais compete processar e julgar: [...] V- os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente".

> fixada quando o cometimento do delito por meio eletrônico se refere à infrações previstas em tratados ou convenções internacionais, constatada a internacionalidade do fato praticado (art. 109, V, da CF), ou quando a prática de crime via internet venha a atingir bem, interesse ou serviço da União ou de suas entidades autárquicas ou empresas públicas (art. 109, IV, da CF). 3. No presente caso, há hipótese de atração da competência da Justiça Federal, uma vez que o fato de haver um usuário do Orkut, supostamente praticando delitos de divulgação de imagens pornográficas de crianças e adolescentes, configura uma das situações previstas pelo art. 109 da Constituição Federal. 4. Além do mais, é importante ressaltar que a divulgação de imagens pornográficas, envolvendo crianças e adolescentes por meio do Orkut, provavelmente não se restringiu a uma comunicação eletrônica entre pessoas residentes no Brasil, uma vez que qualquer pessoa, em qualquer lugar do mundo, desde que conectada à internet e pertencente ao dito sítio de relacionamento, poderá acessar a página publicada com tais conteúdos pedófilos-pornográficos, verificando-se, portanto, cumprido o requisito da transnacionalidade exigido para atrair a competência da Justiça Federal. 5. Conflito conhecido para declarar competente o Juízo da Vara Federal e Juizado Especial Federal de Pato Branco – SJ/PR, ora suscitado. (STJ, Relator: Ministro OG FERNANDES, Data de Julgamento: 23/06/2010, S3 - TERCEIRA SEÇÃO)

3.6 Breves considerações acerca do direito comparado

Por fim, após a análise da legislação brasileira sobre os crimes cibernéticos, é pertinente, ainda que a título complementar, uma breve comparação com a legislação de outros países, uma vez que os crimes cibernéticos se alastraram para todos os lugares do mundo.

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 mesmo autor, em 1990 o primeiro estado norte-americano passou a tipificar o crime de *stalking* (perseguição), sendo seguidos por outros e passando a serem formuladas normas para regularem as condutas praticadas nos sistemas eletrônicos. Hoje, praticamente todos os estados de lá criminalizam o *bullying* e o *cyberbullying*, o que no Brasil ainda não é considerado crime, embora tenha projeto de lei tramitando, conforme comentado anteriormente.

Já na Espanha, por exemplo, o Parlamento aprovou uma lei que visa 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).

Por outro lado, na Inglaterra, Inellas (2009) aduz que foi promulgada a Lei Terrorismo n. 2000, que classifica como ciberterroristas, as pessoas que “põem vidas em riscoatravés da manipulação de sistemas de computadores públicos”, ampliando o conceito de terrorista anteriormente previsto em lei.

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).

Diante do exposto, devidamente analisados os crimes cibernéticos a legislação brasileira vigente, no capítulo final será analisada a (in)eficácia do artigo 154-A do Código Penal, introduzido pela Lei n. 12.737/12, que trata do delito de invasão de dispositivo informático.

4 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 algumas pessoas desvirtuaram esse fim 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.

Dessa forma, o objetivo deste capítulo será examinar, com ênfase na doutrina especializada, a (in)eficácia do crime de invasão de dispositivo informático, à luz dos princípios constitucionais limitadores do poder punitivo estatal.

4.1 Bem jurídico e sujeitos do delito

Com o objetivo de estudar a (in)eficácia do crime de invasão de dispositivo informático, introduzido no Brasil pela Lei 12.737/12, passar-se-á a descrever minuciosamente o seu tipo penal, a fim de estabelecer uma relação entre a sua finalidade e a sua real proteção à privacidade e à intimidade, ou seja, a sua eficácia ou não.

Inserido de forma tímida pela Lei 12.737/12, 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; DE CARVALHO; DE 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.

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, de Carvalho e de 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*.

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

Dessa forma, caracterizados o bem jurídico tutelado e os sujeitos do delito de invasão de dispositivo informático, descrever-se-ão os elementos integrantes desse tipo penal no próximo subcapítulo.

4.2 Elementos do tipo

Dispõe o artigo 154-A do Código Penal, *in verbis*:

> 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.

Conforme visto no primeiro capítulo, todo 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; DE CARVALHO; DE CARVALHO, 2014).

4.2.1 Tipo objetivo

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 e 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 *on-line* como também mediante acesso físico direto do agente ao dispositivo informático.

Mediante violação indevida de mecanismo de segurança é a forma com a 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; DE CARVALHO; DE 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; DE CARVALHO; DE CARVALHO, 2014).

Sem autorização expressa ou tácita do titular do dispositivo, no entendimento do autor supracitado, 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, de Carvalho e de 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 autor supracitado 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).

Dessa forma, entendidos os elementos que compõem o tipo objetivo do crime de invasão de dispositivo informático, há de se verificar o seu elemento subjetivo.

4.2.2 Tipo subjetivo

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).

Destaca Prado, de Carvalho e de Carvalho (2014) que, como visto, na primeira parte do *caput*, há o elemento subjetivo especial do tipo representado pelo “fim de obter, adulterar ou destruir dados ou informações” e, na segunda parte, pela finalidade de se “obter vantagem ilícita”.

Essas expressões, portanto, caracterizam a necessidade de dolo do agente, ou seja, de ter a intenção de obter, adulterar ou destruir e pela finalidade de obter vantagem ilícita, não havendo que se falar na modalidade culposa.

4.3 Consumação e tentativa

De acordo com Prado, de Carvalho e de 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 estamos 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).

Igualmente será possível o reconhecimento da tentativa, pois tal como ocorre na modalidade prevista no *caput*, há a possibilidade de fracionamento do *iter criminis* no que diz respeito aos comportamentos narrados (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.

4.4 Ação Penal

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, também introduzido pela Lei n. 12.737/12, *in verbis:*

> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Como se vê, a ação penal 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).

Aqui, com relação à figura equiparada prevista no §1º do art. 154-A, Nucci (2013) destaca que há uma figura típica inadequada, tendo em vista que a produção ou venda de programa de computador que permita a invasão não tem vítima determinada. Sendo assim, segundo o mesmo autor, interessa à sociedade a sua punição, impedindo-se que chegue a violar dados de alguém. Contudo, constituindo crime de ação pública condicionada à representação, inexiste quem possa fazê-lo a não ser que se encontre a ofendida pela conduta.

4.5 Visão doutrinária e jurisprudencial

Conforme demonstrado quando da análise do conceito analítico de crime no primeiro capítulo, reside na tipicidade o grande problema da caracterização da infração penal nos crimes cibernéticos, tendo em vista que a velocidade com que as novas tecnologias e os novos delitos surgem é proporcionalmente inversa à da adequação e criação de tipos penais pelos legisladores. Dessa forma, as condutas não previstas em lei, apesar de causarem lesões a bens jurídicos, serão consideradas atípicas, pois inexistente a tipicidade.

A lei n. 12.737/12, 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 exacerbadamente brandas.

Segundo o mesmo 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 e etc.

Destaca-se, neste ponto, que com a edição da Lei n. 12.965/14, conhecida como Marco Civil da Internet, houve um avanço da legislação neste sentido, de forma a regulamentar o prazo mínimo para a guarda de log[11] 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 no capítulo anterior.

Temos, 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.

Podemos citar, para ilustrar o enquadramento de novas condutas ilícitas em tipos penais já existentes, o caso em que são repassadas, via aplicativo “WhatsApp”, imagens pornográficas de uma pessoa sem autorização desta.

[11] “Conforme conceituado no capítulo anterior, são informações sobre a utilização de determinado serviço na internet pelo usuário, tais como data, horário, número do IP, bastante úteis na identificação do possível autor de algum delito”.

Se a vítima for menor de idade, aplica-se o art. 241-A do Estatuto da Criança e do Adolescente, tipo penal criado justamente com essa finalidade, para coibir a divulgação de imagens íntimas de menores de idade. Se maior de idade, com o intuito de difamar (atingir a reputação da pessoa), o enquadramento possível seria o crime de difamação, previsto no art. 139 do Código Penal, ante a inexistência de tipificação específica para o caso. Por outro lado, se o delito foi praticado com violação de mecanismo de segurança, com o objetivo de obter, adulterar ou destruir dados, o crime cometido é o do art. 154-A do Código Penal. Ou seja, pelo elemento subjetivo do agente será feito o seu enquadramento legal.

Corroborando 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. É a posição de Cabette (2013, texto digital):

> 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.

No mesmo sentido, Dodge (2013, p. 333), entende que "a necessidade de tipos penais que disciplinem a comunidade digital há tempos é um eco de importante setor da doutrina jurídica, preocupada com questões afeitas à dogmática penal".

De outra banda, há doutrinadores que veem com pessimismo a Lei 12.737/12, especialmente com relação à sua eficácia, entendendo, inclusive, que 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):

> Em debate promovido na FecomercioSP, no dia 01.03.13, sob a coordenação de Renato Opice Blum e Rony Vainzof, tive a oportunidade de externar meu pessimismo em relação à eficácia penal da lei acima referida. A crença de que a lei penal possa ter efeito preventivo está cada vez mais discutida. Ninguém concordaria com a ausência de tutela da nossa privacidade, intimidade; lei tem que existir para nos proteger. O problemático é esperar que isso seja feito pela lei penal. Eu, particularmente, confio mais em medidas civis (determinadas por juiz civil, como remoção de uma notícia ofensiva). Confio mais em indenizações. Quem conhece minimamente 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 autor supracitado defende a desnecessidade de criação de novos tipos penais, além da posição de que a área civil tem mais condições tutelar a privacidade das pessoas, com base em medidas cautelares e indenizações.

Na mesma linha, Colli (2010, pg. 184) defende a desnecessidade da neocriminalização dos crimes cibernéticos, sob o argumento de que "os cibercrimes são velhos crimes em novas mídias, ou seja, não há que se falar em crimes que ainda não existem, mas sim em necessária atividade de hermenêutica jurídica baseada na subsunção dos fatos à norma penal incriminadora".

O autor acima mencionado diz que a solução para os problemas não está na criação de novos tipos penais, chamando a busca frenética pela criação de novos tipos penais aplicáveis a fatos que já são considerados crimes de processo de legiferância neocriminalizadora. Dessa forma, bastaria a interpretação e a aplicação dos tipos penais existentes para a incriminação dos delitos cibernéticos, ainda que cometidos com novos meios.

Na mesma linha, Corrêa (2002) entende ser mais importante do que a tipificação desta ou aquela nova conduta investir no quesito prevenção, tendo em vista que a maioria dos crimes se encontra tipificada em nosso ordenamento, e a busca incessante pela normatização das novas condutas nunca perseguirá o seu real objetivo: propiciar a segurança.

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 explicitado no primeiro capítulo. Vejamos: além de o crime imputado ser típico, ou seja, estar 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 sua 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 encontrava, 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.

Outrossim, 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 exemplos nos crimes de furto de valores bancários pela internet. É o que demonstra a jurisprudência, como se percebe na maioria das decisões. Nesse sentido, ementa de julgado do Tribunal Regional Federal da 4ª Região:

> DIREITO PENAL. FURTO QUALIFICADO. SUBTRAÇÃO DE VALORES DE CONTA CORRENTE. FRAUDE PELA INTERNET. LITISPENDÊNCIA NÃO VERIFICADA. DESCLASSIFICAÇÃO PARA INVASÃO DE DISPOSITIVO INFORMÁTICO ALHEIO. ART. 154-A DO CP. NÃO OCORRÊNCIA. AUTORIA COMPROVADA. DOSIMETRIA. SENTENÇA MANTIDA. 1. O objeto da ação penal em trâmite na 2ª Vara da Seção Judiciária do Rio Grande do é distinto do analisado no presente feito. Logo, afasta-se a hipótese de litispendência invocada pela defesa, porque as três operações bancárias objeto deste inquérito não faziam parte da ação penal nº 0007969-66.2007.4.05.8400. 2. Não há falar em desclassificação para o art. 154-A do Código Penal, pois os réus, mediante sua conduta, não apenas "invadiram dispositivo eletrônico alheio para obter vantagem ilícita", tendo efetivamente subtraído a quantia de R$ 3.046,97 (três mil e quarenta e seis reais e noventa e sete centavos) pertencentes à empresa vítima. Incide, por óbvio, o art. 155, §4º, do CP. 3. De acordo com as provas dos autos, o valor foi subtraído, através de fraude eletrônica perpetrada por um dos réus, de conta corrente, agência Ahú/Curitiba/PR da Caixa Econômica Federal, cuja titular é a empresa, vítima do furto. O montante, então, foi direcionado para a conta do outro réu. 4. O réu Paulo Henrique confessou, no interrogatório da investigação. Por sua vez, o acusado James Dean confirmou, em sedes policial e judicial, a prática criminosa, inclusive no que se refere ao codenunciado. 5. Os réus não obtiveram êxito em afastar as provas que recaem sobre si, devendo ser mantida a condenação pela prática do crime previsto no art. 155, §4º, II e IV, do Código Penal. 6. Não há o que se reformar na reprimenda aplicada, porquanto corretamente fixada na sentença, inclusive no tocante à substituição das privativas de liberdade por restritivas de direitos. (TRF4, ACR 5002347-69.2010.404.7000, Sétima Turma, Relatora p/ Acórdão Salise Monteiro Sanchotene, juntado aos autos em 16/07/2014)

No caso em tela, segundo a acusação formulada pelo MPF, os denunciados, por meio de fraude que induziu a vítima à erro com a utilização de um programa fraudador (trojan), obtiveram os dados bancários e subtraíram valores depositados na conta da vítima, incorrendo, assim, nas sanções do art. art. 155, § 4º, II, do Código Penal.

Como bem destacado pela Relatora, os réus, mediante sua conduta, não apenas "invadiram dispositivo eletrônico alheio para obter vantagem ilícita", mas efetivamente subtraíram a quantia de R$ 3.046,97 (três mil e quarenta e seis reais e noventa e sete centavos) pertencentes à empresa vítima. Incide, por óbvio, o art. 155, §4º, do CP, por se tratar de crime de furto qualificado, e não mera invasão de computador pertencente a terceiro.

Dessa forma, como se vê, o crime de invasão de dispositivo informático foi o meio para os réus conseguirem acesso à conta corrente da vítima e praticarem o furto de valores. Assim, pelo princípio da consunção, o crime-meio é absorvido pelo crime-fim, não havendo que se falar em desclassificação do furto mediante fraude para o delito de invasão de dispositivo informático.

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.

Além disso, com o intuito de complementar a pesquisa, foi feita uma solicitação para a Polícia Civil/RS para que fossem repassados dados estatísticos de ocorrências e termos circunstanciados do crime em questão. Todavia, o retorno foi negativo, no sentido de que a DIPLANCO (Divisão de Planejamento e Coordenação da Polícia Civil) não possui condições fornecer o levantamento para este tipo penal por não existir código específico para esse delito nas ocorrências.

4.6 A in(eficácia) do artigo 154-A do Código Penal

Especificamente com relação à problemática do artigo 154-A, foco central do estudo, passar-se-á análise da relação entre a sua finalidade e a sua eficácia, ou seja, o se o delito de invasão de dispositivo informático obteve êxito em tutelar liberdade individual, a intimidade e a privacidade das pessoas.

Quanto ao seu tipo penal objetivo, Nucci (2013) entende que 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.

Segundo o mesmo autor, 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.

No mesmo sentido, Greco (2014) preleciona que tal exigência impede que alguém seja punido pelo tipo penal previsto quando, também, mesmo indevidamente, ingresse em dispositivo informático alheio sem que, para tanto, viole mecanismo de segurança, pois que inexiste. Temos como exemplo os computadores, que nem todas as pessoas colocam senhas de acesso, permitindo que qualquer pessoa que a eles tenha acesso possa conhecer o seu conteúdo. Contudo, mesmo sem a existência de senha de acesso, a ninguém é dado invadir computador alheio, a não ser que ocorra permissão tácita ou expressa do proprietário.

No entanto, segundo o autor supracitado, para fins de configuração típica, tendo em vista a exigência contida no tipo penal em análise, somente haverá infração penal se houver, por parte do agente invasor, uma violação indevida do mecanismo de segurança.

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 no capítulo anterior, 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 autor 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. Dessa forma, o desvalor da ação nesse caso seria justificadamente exacerbado como ocorre, por exemplo, no caso de furto qualificado.

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, conforme o conceito analítico de crime visto no primeiro capítulo, 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[12], caso alguém invadisse uma residência com as portas e janelas estivessem abertas. Ou seja, a tutela penal deixa de proteger quem, por um descuido ou por acaso, está desprotegido e justamente necessitaria da sua proteção.

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 que vemos diariamente nos meios de informação em que houve prévia divulgação de uma foto íntima da pessoa.

Este 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

[12] "Art. 150: Entrar ou permanecer, clandestina ou astuciosamente, ou contra a vontade expressa ou tácita de quem de direito, em casa alheia ou em suas dependências".

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 acima mencionadas, após o suicídio 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.

Nesse sentido, a tutela penal se faz necessária para coibir a prática desse tipo de delito. Contudo, como se denota pela análise do presente estudo, a deficiência técnica dos legisladores aliada à pressa pela edição de uma lei que teve vítima da invasão de dispositivo informático uma pessoa famosa, foram inimigas de uma perfeita tipificação penal.

Os princípios constitucionais limitadores do poder punitivo estatal abordados no primeiro capítulo servem como linhas que delineiam a atuação do Estado e impedem que sejam cometidos excessos. No mesmo passo, o conceito analítico de crime referido no segundo capítulo, resultado de uma evolução dogmática construída por longo período, trouxe os elementos que constituem o crime e são necessários para o início da persecução penal.

Como visto, o elemento da tipicidade é o grande desafio para os legisladores frente aos crimes cibernéticos, uma vez que a velocidade com que esse tipo de delito surge é proporcionalmente inversa à da criação e adequação dos tipos penais.

Apesar de tudo isso, sendo indubitável que o direito penal é necessário para proteger os bens jurídicos dos delitos cibernéticos praticados, era necessária a criação de um novo tipo penal para tutelar a invasão de dispositivo informático ou era possível ser feito o seu adequado enquadramento com os tipos penais existentes?

Será que a expressão “violação indevida do mecanismo de segurança”, constante no *caput* do art. 154-A, não poderia ter sido suprimida? Ou assim, limitando o tipo penal à existência de algum mecanismo, não condicionou a eficácia do artigo?

E ainda, levando em consideração a baixa pena cominada e por consequência a aplicação do rito previsto no Juizado Especial Criminal e os seus respectivos institutos despenalizadores, não está se tornando precária a proteção aos bens jurídicos tutelados pelo

crime em questão? Estas e outras indagações serão respondidas a seguir, finalizando este estudo.

5 CONCLUSÃO

As pessoas, em um mundo cada vez mais globalizado e competitivo, velam pela 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 novos 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.

Dessa forma, esta monografia ocupou-se em apresentar, no primeiro capítulo do desenvolvimento, alguns princípios relativos aos crimes cibernéticos que atuam como limitadores constitucionais do poder punitivo estatal, destacando-se, em especial, o princípio

da legalidade. Percebeu-se que, apesar de aplicados a todos os tipos de crimes, os princípios destacados se relacionam de forma especial com os delitos cibernéticos, uma vez que estes possuem um caráter *sui generis* e merecem atenção particular para que seja possível uma perfeita persecução penal.

Em seguida, fez-se o estudo de alguns conceitos preliminares que tivessem pertinência à compreensão do tema, com especial atenção ao elemento da tipicidade, integrante do conceito analítico de crime, uma vez que reside aí a grande discussão do tema em questão, a aplicação da conduta à norma.

Na sequência, abordou-se a análise histórica da internet, no Brasil e no mundo, para que fosse possível o entendimento do surgimento dos crimes cibernéticos no país. Além disso foi analisado o conceito de crime cibernético, que por sinal é peculiar e adequado à legislação vigente, adotando-se a classificação dos crimes cibernéticos como sendo as 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.

O segundo capítulo também analisou de forma breve a legislação brasileira existente com relação a este tipo de crime, destacando que o foco central não era esgotá-las, uma vez que o objetivo está no artigo 154-A, que tipifica o crime de invasão de dispositivo informático. Nesse sentido, foram feitas considerações acerca da lei n. 12.727/12 que introduziu ao código penal o referido artigo, bem como a respeito dos projetos de lei em tramitação no Brasil acerca do tema. Constatou-se que a falta de regulamentação com relação aos crimes cibernéticos de uma forma geral, ao passo que alguns crimes como o *cyberbullyng*, por exemplo, sequer são tipificados, ao contrário de outros países.

Na sequência, foram abordadas características da persecução penal dos crimes cibernéticos que o caracterizam como um delito *sui generis*, eis que indissociável a vinculação do direito material com o processual neste tipo de delito. Dentre elas, as dificuldades de identificação da autoria e dos conflitos de competência, por ser um delito que ultrapassa fronteiras. Após, com o objetivo de complementar o estudo, foi feita uma breve abordagem sobre o direito comparado, a fim de consultar como os demais países reagem acerca deste tipo de crime.

Como o objetivo geral do trabalho estava centrado na análise da (in)eficácia do crime de invasão de dispositivo informático, o capítulo final partiu da análise minuciosa do tipo penal em questão, a fim de se estabelecer uma relação entre a sua finalidade e a sua real proteção à privacidade. Em seguida, foi feito estudo a respeito da visão doutrinária e jurisprudencial acerca da lei n. 12.737/12, que introduziu o art. 154-A ao Código Penal, e do artigo em si, percebendo-se que há uma dificuldade em relação à adequação típica de fatos à normas já existentes, bem como a utilização do crime de invasão de dispositivo informático para cometimento de delito mais grave, sendo assim, absorvido.

Além disso, buscou-se apresentar considerações acerca da (in)eficácia do crime de invasão de dispositivo informático, foco central do estudo. Foram apresentadas análises doutrinárias acerca do tipo penal e questões que exprimem a importância da proteção à intimidade e à privacidade, sendo que, em caso de violação, podem causar danos irreversíveis à vítima.

Diante da análise do problema proposto para este estudo – O crime de 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, qual seja a de proteger a liberdade individual das pessoas contra a invasão de dispositivo informático, punir e reprimir este tipo de conduta. A edição de normas penais deve respeitar os princípios constitucionais e beirar a perfeição técnica, o que foi deixado a desejar pelos legisladores ao elaborarem a lei em questão, motivados pelo clamor social proporcionado pela divulgação de fotos íntimas da atriz Carolina Dieckmann na época.

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 provido do mecanismo de segurança.

Frisa-se que nem sempre o enquadramento de condutas às normas já existentes é possível, devendo, sobretudo, ser respeitado o princípio da legalidade.

Apesar de a área cível ser um caminho para ressarcir o abalo sofrido pela vítima, sabe-se que a maioria 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 e tampouco de estatísticas policiais referentes, 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 na pesquisa, 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: prover a segurança jurídica através da proteção dos bens jurídicos e direitos.

Por fim, como bem salientou Beccaria, para que o exercício do *jus puniendi* estatal se dê de forma regular, basta que as leis sejam simples e claras, sem criar embaraços e obstáculos que dificultem a punição e causem insegurança jurídica na sociedade.

REFERÊNCIAS

BARROSO, Luís R. **Temas de Direito Constitucional**. Rio de Janeiro: Renovar, 2005. Tomo III.

BECCARIA, Cesare B. M. de. **Dos delitos e das penas.** 2. ed. São Paulo: Martins Fontes, 2002. Lucia Guiducini e Alessandro Berti Contessa tradutores.

BITENCOURT, Cezar R. **Tratado de Direito Penal**. 18. ed. São Paulo: Saraiva, 2012.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 19. ed. atual. São Paulo: Malheiros Editores, 2006.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Disponível em:< http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 10 ago. 2015.

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. Decreto-Lei nº. 3.689, de 03 de outubro de 1941. **Código de Processo Penal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689Compilado.htm>. Acesso em: 10 ago. 2015.

BRASIL. Decreto-Lei nº. 99.710, de 21 de novembro de 1990. **Convenção sobre os Direitos da Criança**. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D99710.htm>. Acesso em: 14 set. 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. **Superior Tribunal de Justiça**. Conflito de Competência nº 66.981/RJ, da 3ª Seção Criminal. Autor: Justiça Pública. Réu: Ricardo Aragon Tamayo. Suscitante: Juízo Federal da 4ª Vara Criminal da Seção Judiciária do Estado do Rio de Janeiro. Suscitado: Juízo Federal da 1ª Vara Criminal do Júri e das Execuções Penais da Seção Judiciária do Estado de São Paulo. Relator: Min. Og Fernandes. Brasília, 16 de fevereiro de 2009. Disponível em:<https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=4714199&num_registro=200601611027&data=20090305&tipo=5&formato=PDF>. Acesso em: 24 ago. 2015.

BRASIL. **Superior Tribunal de Justiça**. Conflito de Competência nº 111.338/TO, da 3ª Seção Criminal. Autor: Justiça Pública. Suscitante: Juízo de Direito da Vara Criminal de Palmas/TO. Suscitado: Juízo Federal da 7ª Vara Criminal da Seção Judiciária do Estado de São Paulo e Juízo Federal e Juizado Especial Federal de Pato Branco/PR. Relator: Min. Og Fernandes. Brasília, 23 de junho de 2010. Disponível em:<https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=10567302&num_registro=201000615960&data=20100701&tipo=5&formato=PDF >. Acesso em: 14 set. 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 abril 2014. Disponível em: <http://www.tjrs.jus.br/busca/search?q=cache:www1.tjrs.jus.br/site_php/consulta/consulta_processo.php%3Fnome_comarca%3DTribunal%2Bde%2BJusti%25E7a%26versao%3D%26versao_fonetica%3D1%26tipo%3D1%26id_comarca%3D700%26num_processo_mask%3D70049844483%26num_processo%3D70049844483%26codEmenta%3D5759123+70049844483++++&proxystylesheet=tjrs_index&client=tjrs_index&ie=UTF-8&lr=lang_pt&site=ementario&access=p&oe=UTF-8&numProcesso=70049844483&comarca=Comarca%20de%20Nova%20Prata&dtJulg=29/04/2014&relator=Naele%20Ochoa%20Piazzeta&aba=juris>. Acesso em: 24 set. 2015.

BRASIL. **Tribunal Regional Federal da 4ª Região**. Apelação Criminal nº 5002347-69.2010.404.7000/PR, 7ª Turma. Apelante: Paulo Henrique da Cunha Vieira. Apelado: Ministério Público Federal. Relatora: Juíza Federal Salise Monteiro Sanchotene. Porto Alegre, 15 jul. 2014. Disponível em: <http://jurisprudencia.trf4.jus.br/pesquisa/inteiro_teor.php?orgao=1&documento=6794986&termosPesquisados=5002347-6920104047000|5002347-69.2010.404.7000>. 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

CHEMIN, Beatris F. **Manual da Univates para trabalhos acadêmicos**: planejamento, elaboração e apresentação. 2. ed. Lajeado: Univates, 2012.

COLLI, Maciel. **Cibercrimes: Limites e perspectivas à investigação policial de crimes cibernéticos**. 1. ed. Curitiba: Juruá, 2010.

DIP, Andrea; AFIUNE, Giulia. Como um sonho ruim. **Pública: Agência de Reportagem e Jornalismo Investigativo**, São Paulo, 19 de 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. Subprocuradora-Geral da República Raquel Elias Ferreira Dodge coordenadora.

ERDELYI, Maria Fernanda. Itamaraty ainda estuda adesão à Convenção de Budapeste. **ConJur**, São Paulo, 29 maio 2008. Disponível em: < http://www.conjur.com.br/2008-mai-29/itamaraty_ainda_estuda_adesao_convencao_budapeste>. Acesso em: 02 set. 2015

FERRAJOLI, Luigi. **Direito e razão: teoria do garantismo penal**. 4. ed. São Paulo: Editora Revista dos Tribunais, 2014. Ana Paula Zomer Sica, Fauzi Hassan Choukr, Juarez Tavares e Luiz Flávio Gomes tradutores.

GOMES, Luiz F; MOLINA, Antonio G. P de. **Direito Penal: parte geral**. 2. ed. 2. vol. São Paulo: Editora Revista dos Tribunais, 2009.

GOMES, Luiz F. Lei Carolina Dieckmann e sua (in)eficácia. **Revista Jus Navigandi**, 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. vol 2. Rio de Janeiro: Impetus, 2014.

INELLAS, Gabriel C. Z de. **Crimes na internet**. 2. ed. São Paulo: Editora 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. vol. 2. São Paulo: Editora Atlas, 2013.

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: Editora Revista dos Tribunais, 2013.

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

RIBEIRO, Thiago de L. **O direito aplicado ao cyberbulling: honra e imagem nas redes sociais**. 1 ed. Curitiba: InterSaberes, 2013. E-book. Disponível em: <http://univates.bv3.digitalpages.com.br/users/publications/9788582127995/pages/-2 >. Acesso em: 10 ago. 2015.

SAWAYA, M. R. **Dicionário de informática e internet inglês/português**. São Paulo: Nobel, 1999.

TONETTO, Maurício. Defenda-se das fraudes virtuais. **Zero Hora**, Porto Alegre, p. 32, 3 jul. 2015.

TOLEDO, Francisco de A. **Princípios básicos de direito penal**. 5. ed. São Paulo: Saraiva, 2000.

TOURINHO FILHO, Fernando da C. **Manual de processo penal**. 16. ed. São Paulo: Saraiva, 2013.

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

ZAFFARONI, Eugenio R; PIERANGELI, José H. **Manual de Direito Penal Brasileiro**. Parte Geral. 5. ed.. São Paulo: Revista dos Tribunais, 2004.