UNIVERSIDADE FEDERAL DE JUIZ DE FORA
FACULDADE DE DIREITO

Daniel Dore Lage

Do crime de invasão de dispositivo informático: Uma análise do tipo penal à luz da legalidade estrita

Juiz de Fora
2013

DANIEL DORE LAGE

Do crime de invasão de dispositivo informático: Uma análise do tipo penal à luz da legalidade estrita

Trabalho apresentado à Disciplina de MONOGRAFIA DE CONCLUSÃO DO CURSO DE DIREITO, como parte dos requisitos para obtenção do título de Bacharel em Direito.

Orientador: Leandro Oliveira Silva

Juiz de Fora

2013

Ficha catalográfica elaborada através do Programa de geração
automática da Biblioteca Universitária da UFJF,
com os dados fornecidos pelo(a) autor(a)

Lage, Daniel Dore.
Do crime de invasão de dispositivo informático: Uma análise do tipo penal à luz da legalidade estrita / Daniel Dore Lage. -- 2013.
58 f.

Orientador: Leandro Oliveira Silva
Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Juiz de Fora, Faculdade de Direito, 2013.

1. Direito Penal. 2. Invasão. 3. Informática. 4. Crime. I. Silva, Leandro Oliveira, orient. II. Título.

DANIEL DORE LAGE

Do crime de invasão de dispositivo informático: Uma análise do tipo penal à luz da legalidade estrita

Trabalho apresentado à Disciplina de MONOGRAFIA DE CONCLUSÃO DO CURSO DE DIREITO, como parte dos requisitos para obtenção do título de Bacharel em Direito.

Aprovada em 30 de agosto de 2013

BANCA EXAMINADORA

Prof. Leandro Oliveira Silva - Orientador

Universidade Federal de Juiz de Fora

Prof. Doutor Cleverson Raymundo Sbarzi Guedes

Universidade Federal de Juiz de Fora

Prof. Doutor Luiz Antonio Barroso Rodrigues

Universidade Federal de Juiz de Fora

RESUMO

Recentemente foi aprovada a lei 12.737/2012 que tipifica o crime de invasão de dispositivos informáticos no Brasil. Tal lei foi aprovada às pressas pelo Congresso Nacional, sensibilizado com a repercussão dada ao tema após a situação ocorrida contra uma famosa atriz de televisão, que teve fotos íntimas divulgadas na internet contra sua vontade. Trata-se de tipo penal com muitos elementos abertos, que necessitam ser limitados para uma aplicação correta aos casos concretos. Acreditamos que a motivação explicada pelos legisladores foi idônea, porém, incriminaram uma série de condutas de forma totalmente atécnica, o que torna o artigo 154-A do Código Penal claro exemplo de expansão penal desarrazoada. As condutas incriminadas pelo artigo 154-A do Código Penal atentam contra privacidade e tem como objeto material a informática. O legislador, desta forma, "condensou" em um tipo penal a diretriz dada pela "Convenção de Budapeste" sobre criminalidade informática. Após uma análise de seus elementos, concluímos que uso excessivo expressões dúbias na redação do artigo gera uma grave violação ao princípio da legalidade estrita, o que torna o tipo penal carente de eficácia. Ao final, sugerimos uma redação alternativa ao tipo penal.

Palavras-chave: 1. Crime. 2. Informático. 3. Invasão. 4. Computador. 5. Privacidade

ABSTRACT

Recently a Brazilian law that criminalizes the invasion of computing devices was passed. This law was rushed through Congress, because of the attention given to the subject after a situation occurred with a famous television actress, who had intimate photos published on the Internet against her will. The crime definition contains many open elements that need to be limited for a proper application to concrete cases. We believe that the motivation explained by legislators is suitable, however, they made a number of dutties a crime, in a completely non-technical way, which makes the article 154-A of the Brazilian Penal Code a clear example of unreasonable criminal expansion. The conducts under Article 154-A of the Criminal Code undermines privacy and have computing as material object. The legislator "condensed" in a legal offense the guidelines given by the "Budapest Convention" on computer crime. After an analysis of its elements, we conclude that the overuse of dubious expressions in the writing is a serious violation to the principle of strict legality, which makes the criminal type lack effectiveness. At the end, we suggest an alternative writing to this criminal type.

Keywords: 1. Crime. 2. Computer. 3. Invasion. 4. Privacy

SUMÁRIO

Introdução

É notório que a tecnologia evolui diariamente. Na mesma medida em que ela se desenvolve beneficamente, malfeitores utilizam-na também para cometer ilícitos; Existem crimes, hoje, inimagináveis há alguns anos. Vivemos na chamada "sociedade de risco", em que as pessoas consentem em correr os riscos gerados por atividades alheias em prol de uma vida melhor. É uma questão delicada: as pessoas desejam informações variadas, instantâneas, comunicação barata, dentre outros benefícios. Esquecem, porém, que, utilizando tais serviços, ficam sujeitas a fraudes, violações de privacidade, dentre outros injustos. É preciso, portanto, estabelecer legislação que contenha regras de utilização e limites para que o uso prejudicial a terceiros seja minorado o quanto for possível.

No Brasil, muito foi discutido sobre tal legislação, porém nada de concreto surgiu devido à falta de infraestrutura para investigar e punir tais crimes, além do desinteresse governamental para combatê-los. Por exemplo, nos Estados Unidos e na União Europeia, esta regulamentação foi feita há pelo menos duas décadas, a exemplo de Portugal, que apresenta a Lei de Criminalidade Informática desde 1991, estando muito à frente do Brasil, vindo este a ter seu primeiro projeto de lei **relevante** sobre o tema apenas no ano de 1999 – O PL 84/99.

Ocorre que nenhum dos projetos de lei correntes no Poder Legislativo havia prosperado até o final de 2012. Os juristas interessados sempre estudaram o tema de forma tímida, baseados estritamente no que foi produzido em sede de direito comparado, tendo como principal referência a "*Convenção de Budapeste sobre Cibercrimes*", de novembro de 2001, que define os parâmetros conceituais sobre tal matéria na União Europeia.

Recentemente foi aprovada a lei 12.737/2012 que tipifica o crime de invasão de dispositivos informáticos no Brasil. Tal lei foi aprovada às pressas pelo Congresso Nacional, sensibilizado com a repercussão dada ao tema após a situação ocorrida contra uma famosa atriz de televisão, que teve fotos íntimas divulgadas na

internet contra sua vontade. Sob o pretexto da não existência de lei específica sobre o assunto, pretendeu "fazer" justiça, como é típico em nossa atual sociedade.

A expansão penal desarrazoada é uma constante em nosso ordenamento jurídico, que gera problemas de ineficácia e ineficiência. Vivemos em tempos onde criar inúmeras leis penais apazigua o ânimo da população, porém não trata os problemas sociais que motivaram tal ação. Os problemas que poderão surgir podem ser resumidos a estas perguntas: O tipo penal criado pela lei 12.737/2012 está de acordo com o princípio da estrita legalidade? O tipo penal de invasão de dispositivo proíbe quais situações? O tipo penal abarca, adequadamente, as situações pretendidas? Era necessária a criação deste tipo penal?

Este é um estudo dogmático, pois se trata de tipo penal com muitos elementos abertos, heteronômicos, normativos, e até mesmo confusos, que necessitam ser limitados para uma aplicação correta aos casos concretos. Acreditamos que a motivação explicada pelos legisladores foi idônea, porém, incriminaram uma série de condutas de forma totalmente atécnica, o que torna o artigo 154-A do Código Penal claro exemplo da expansão penal desarrazoada, na definição de SILVA-SÁNCHEZ[1], pois não foram respeitados os princípios garantistas de direito penal; percebe-se que a lei foi aprovada sem maiores discussões jurídicas, apenas para satisfazer a população.

Nesta pesquisa propomos estudar a técnica legislativa empregada na elaboração do artigo 154-A do Código Penal e confrontá-la com os estudos doutrinários sobre este tema. O tipo, da forma que está escrito, incorre em vários equívocos em relação à doutrina do direito penal material.

Esta obra é composta das seguintes discussões:

No primeiro capítulo apresentamos a função garantidora do tipo penal, relacionando os conceitos de garantismo penal e legalidade estrita, de forma a embasar a análise do tipo penal e confirmando sua necessidade em nosso ordenamento.

[1] **SILVA SÁNCHEZ, Jesús-María**. A expansão do direito penal: aspectos da política criminal nas sociedades pós-industriais.

No segundo capítulo traremos a redação do tipo penal 154-A, estudaremos o bem jurídico-penal tutelado, definindo quais bens jurídicos o artigo 154-A do Código Penal visa proteger. Além disto, estabelecemos uma classificação deste tipo penal, apresentando também os sujeitos deste delito, tanto o sujeito ativo como o passivo. Ainda estudaremos os aspectos subjetivos do tipo penal, demonstrando a existência do dolo e inexistência do tipo culposo. Após estas considerações, trataremos do texto da lei, com foco nas possíveis interpretações que a teoria garantista nos permite dentro da linguagem utilizada pelo legislador.

No terceiro e último capítulo concluímos o estudo, apresentando as críticas pertinentes.

1) A relevância do tipo penal no Estado de Direito

Para realizar uma análise científica da estrutura de uma lei, é necessário definir os pressupostos teóricos adotados, os quais validarão as críticas feitas adiante. O ponto de partida deste trabalho é a noção de uma escola de direito penal mínimo, em sua vertente constitucional conhecida como teoria do garantismo penal, proposta por Luigi Ferrajoli, cuja obra é expoente doutrinário.

1.1) O GARANTISMO PENAL E O PRINCÍPIO DA ESTRITA LEGALIDADE

O garantismo, em apertada síntese, trata-se de modelo de ordenamento jurídico, sugerido por FERRAJOLI[2], sendo um conjunto ideal de garantias individuais e processuais dadas aos cidadãos como forma de proteção contra arbitrariedades exercidas pelos órgãos públicos. Trata-se de teoria aplicável a todos os campos do direito, não apenas ao direito penal. Mas neste estudo, o foco está voltado ao direito penal material, o qual estipula direitos e proibições.

Importa-nos aqui o garantismo na acepção de modelo normativo de direito, uma das significações estudadas pelo referido autor. O sistema normativo garantista preza pelo bem dos indivíduos, estipulando a presunção de inocência e a liberdade individual como regra, e a punição penal apenas quando se tem absoluta certeza de que o cidadão cometeu uma infração típica, ilícita e culpável, e que as sanções civis e administrativas serão insuficientes ao caso. Trata-se de um sistema racional, surgido da influência iluminista e do liberalismo, cuja importância para este estudo é o entendimento de que o Estado de Direito não deve interferir nas esferas individuais sem a certeza de ter acontecido um dano maior à sociedade. Estas garantias se efetivam através de postulados e normas otimizadoras da aplicação das leis

[2] **FERRAJOLI, Luigi**. Direito e razão: teoria do garantismo penal. São Paulo: Editora Revista dos Tribunais, 2002.

chamadas de **princípios**. Os dez princípios basilares em um sistema garantista enunciados por FERRAJOLI[3] são os seguintes:

> 1) princípio da **retributividade** ou da consequencialidade da pena em relação ao delito; 2) princípio da **legalidade**, no sentido lato ou estrito; 3) princípio da **necessidade** ou da economia do direito penal; 4) princípio da **lesividade** ou da ofensividade do evento; 5) princípio da **materialidade** ou da exterioridade da ação; 6) princípio da **culpabilidade** ou da responsabilidade pessoal; 7) princípio da **jurisdicionariedade**, também em sentido lato ou no sentido estrito; 8) princípio **acusatório**, ou da separação entra juiz e acusação; 9) princípio de **ônus da prova** ou da verificação; 10) princípio do **contraditório** ou da defesa, ou da falseabilidade.

Estes dez princípios, nas palavras do autor, "definem as regras do jogo fundamental do direito penal".

Tais princípios definem que o direito penal tem por função aplicar uma pena ao sujeito que comete uma infração (retributividade), desde que esta conduta esteja prevista em lei (legalidade), seja danosa (lesividade), que a pena aplicada seja realmente necessária (necessidade), aplicável somente ao agente que realizou a conduta (pessoalidade), proposta e provada pela acusação em ação penal (ônus probatório da acusação), em órgão judicial competente (jurisdicionariedade), sendo possibilitado ao acusado o direito à plena defesa e ao contraditório (ampla defesa e contraditório).

Inegável, porém, que a principal e mais importante garantia no sistema sugerido pelo autor reside no **princípio da legalidade**, em suas duas acepções estudadas: Legalidade em sentido amplo (mera legalidade) e em sentido estrito (estrita legalidade)[4].

O princípio da legalidade está previsto em nossa Constituição Federal:

> Art. 5º, inc. XXXIX - Não haverá crime sem lei anterior que o defina, nem pena sem prévia cominação legal.

O doutrinador BITENCOURT[5], de forma didática, explica seu significado:

> Pode-se dizer que, pelo princípio da legalidade, a elaboração de normas incriminadoras é função exclusiva da lei, isto é, nenhum fato pode ser considerado crime e nenhuma pena criminal pode ser aplicada sem que antes de ocorrência desse fato exista uma lei definindo-o como crime e

[3] **FERRAJOLI, Luigi**. Direito e razão... pág. 75
[4] **FERRAJOLI, Luigi**. Direito e razão... pág. 76
[5] **BITENCOURT, Cezar Roberto**. Tratado... pág. 41

> cominando-lhe a sanção correspondente. A lei deve definir com precisão e de forma cristalina a conduta proibida.

Através do princípio da legalidade é possível a determinação abstrata do que é uma conduta punível, desde que sejam respeitadas suas duas acepções: 1) a **mera legalidade** (Legalidade em sentido amplo), que deve ser entendida como a simples reserva legal, em outras palavras, a existência de uma lei anterior regularmente elaborada que vincula os magistrados em sua tomada de decisão; 2) a **estrita legalidade**, que se trata da reserva absoluta de lei, voltada ao legislador e intimamente relacionada com o princípio da taxatividade, como será mais bem abordado a seguir.

Consoante FERRAJOLI[6], a "**mera legalidade**" deve ser entendida como regra semântica que identifica o direito vigente como objeto exaustivo e exclusivo da ciência penal, estabelecendo que somente as leis digam o que é delito.

Diferentemente, o princípio da "estrita legalidade" deve ser entendido como "técnica legislativa dirigida a excluir as convenções pessoais referidas não a fatos, mas diretamente a pessoas." Com isto, pretende-se que as normas criadas sejam regulamentares, não constitutivas, significando que não se deve admitir a existência de tipos penais incriminadores voltados a determinadas pessoas, mas apenas os de aplicação geral e impessoal.

Extraímos desses princípios as seguintes consequências: primeiramente, fica estipulada uma liberdade intangível de atuação estatal sobre a esfera de direitos de seus cidadãos, estabelecendo o que o Estado pode ou não fazer; Como segunda consequência, estabelece-se verdadeira igualdade entre os indivíduos, visto que todos os cidadãos são passíveis de serem punidos pela mesma lei, não havendo leis 'direcionadas' a certas pessoas.

É perceptível a aproximação entre a "legalidade estrita" e a necessária clareza do texto penal. FERRAJOLI[7] entende que

> tal conteúdo [a lei penal] seja formado por pressupostos típicos dotados de significado unívoco e preciso, pelo que será possível seu emprego como figuras de qualificação em proposições judiciais verdadeiras ou falsas." Não se admite, portanto, tipos penais que incriminam condutas que não sejam

[6] **FERRAJOLI, Luigi**. Direito e razão... pág. 302
[7] **FERRAJOLI, Luigi**. Direito e razão... pág. 76

> taxativamente reguladas, ou seja, que permitem interpretações dúbias ou demasiadamente extensivas sob o risco de criação de verdadeiros "tipos de autor".

A legalidade estrita garante a verificabilidade e a falseabilidade dos tipos penais abstratos, assegurando, mediante as garantias penais, a denotação taxativa da ação, do dano e da culpabilidade. A importância deste princípio se traduz em um sistema penal que preza pelas garantias de seus cidadãos no estabelecimento prévio e claro do que é punível.

1.2) A FUNÇÃO GARANTIDORA DO TIPO PENAL

O direito penal garantista e o princípio da legalidade estrita estão intimamente ligados à ideia de **tipo-garantia**, expressando que o tipo penal possui função garantidora no Estado de Direito. Neste sentido relembra TAVARES[8]

> O princípio da legalidade, inserido no art. 5º, XXXIX, da Constituição da República, pelo qual se exige uma certa descrição da conduta criminosa, tem por escopo evitar possa o direito penal transformar-se em instrumento arbitrário, orientado pela conduta de vida ou pelo ânimo. Considerando que a função primeira do direito penal é a de delimitar as áreas do justo e do injusto, mediante um procedimento ao mesmo tempo substancial e informativo, a exata descrição dos elementos que compõem a conduta criminosa serve, primeiramente, ao propósito de sua materialização [...] depois, como instrumento de comunicação entre o Estado e os cidadãos, pelo qual se assinalam as zonas do proibido e do permitido [...]

Tipo penal é a representação legal de um "modelo" de conduta. Dito de outra maneira, seria uma definição, criada pelo legislador através de lei, na qual descreve de forma abstrata uma ou mais condutas que, caso venham a ser praticadas futuramente, devem ter como consequência a aplicação de uma pena ali cominada.

SILVA[9] elucida,

> Pode-se dizer que o tipo penal é uma construção abstrata sob a forma de um modelo conceitual que descreve, esquematicamente, um comportamento humano cuja realização é proibida pela lei penal, em sentido formal e estrito, pois tal conduta é portadora de qualidades ético, social e juridicamente reprováveis e intoleráveis por parte da ordem jurídico-penal vigente, já que se traduzem em lesão ou ameaça de lesão a um bem jurídico possuidor de dignidade penal.

---

[8] **TAVARES, Juarez**. Teoria do Injusto Penal. Pág. 173.
[9] **SILVA, Leandro Oliveira.** Teoria da Tipicidade. Em Direito Penal Acadêmico – Parte Geral... pág 383

> O tipo penal não apresenta uma estrutura arbitrária, aleatória e livre, submetida aos caprichos do legislador e tampouco sua elaboração pode ser fruto de irrestrita e ilimitada criação imaginativa legislativa, mas, ao contrário, deve ser resultado de uma racional e refletida valoração da realidade e dos valores mais preciosos a ela, o que dá origem a um modelo abstrato que se refere a fatos concretos futuros (...).

O tipo penal, portanto, representa muito mais do que a criminalização de condutas. Trata-se de seleção de bens jurídicos que o legislador entende ser digna da proteção penal, seja pela insuficiência ou pela impossibilidade das tutelas cíveis. É o que a doutrina chama de **função político-criminal** do tipo penal relacionada com o caráter fragmentário do direito penal, que só deve atuar em *ultima ratio.*

A importância dos tipos penais decorre da função de garantia que eles exercem em nossa sociedade. Os tipos penais são a verdadeira expressão do princípio da legalidade, visto que possibilitam a todo cidadão saber se sua ação é punível ou não. A doutrina chama isto de **função limitadora** do tipo penal.

Quando se fala em segurança jurídica, devemos compreender que os cidadãos não podem ser surpreendidos quando o Estado pretender restringir sua esfera de liberdade. Aqui reside o caráter garantidor do tipo penal. O legislador, representante do povo, legitima a intervenção estatal quando da prática de injustos, desde que estes sejam previstos em lei. Daí a necessidade de clareza, do emprego de técnicas legislativas, da realização de estudos para a elaboração do tipo penal. Através deles existe a certeza do que não é considerado crime. Também através deles podemos entender quais condutas podem ser consideradas ilícitas e culpáveis. O tipo penal é o limite redutor e o fundamento necessário do direito de punir do Estado.

1.3) DA NECESSIDADE DE UM TIPO PENAL ESPECÍFICO

O Brasil não possuía legislação específica sobre o tema até a aprovação da Lei 12.737/2012. Havia discussões acerca da necessidade ou não da criação de tipos penais para incriminar os crimes informáticos, visto que os primeiros estudiosos do assunto confundiam o objeto do crime e meio de prática do crime.

Ilustrando o que foi dito trazemos um trecho do estudo de MIRANDA[10] que lista vários tipos penais que considera crimes informáticos a serem reprimidos:

> Poderíamos citar, a título ilustrativo, alguns crimes atualmente perpretados com o uso de alta tecnologia: O estelionato em todas as suas formas, lavagem de dinheiro, os crimes de colarinho branco, furto, a modalidade conhecida por "salami slicing" (fatiamento de salame, em que o ladrão faz regularmente transferências eletrônicas de pequenas quantias de milhares de contas para a sua própria, muitas vezes camuflada por campanhas de arrecadação de donativos de modo a não despertar suspeitas), serviços subtraídos, o contrabando, a pornografia infantil, parafilia, invasões de privacidade, apologia de crimes, violações à propriedade intelectual ou industrial, violações à Lei do software, pixações em sites oficiais do governo, vandalismo, sabotagem, dano, propagação de vírus de computador, a pirataria em geral, espionagem, tráfico de armas e drogas, lesões a direitos humanos (terrorismo, crimes de ódio, racismo, etc.), destruição de informações, jogos ilegais, dentre inúmeros outros, apenas para explicitar a complexidade da matéria tratada. A experiência tem mostrado quão delicada é uma investigação de crimes por computador, seja pela falta de experiência policial, seja pela adoção de procedimentos desatualizados para a alta tecnologia empregada.

Nesta passagem MIRANDA sugere a criação de tipos já existentes em nossa legislação penal, como estelionato, furto, dano, violação à propriedade intelectual, dentre outros, que utilizam a informática como meio de execução. Em resposta a esta constatação, alguns autores contrapunham-se à necessidade de nova legislação, consoante a posição de COLARES[11], para quem os crimes tradicionais, "cometidos por meio eletrônico, não necessitam de legislação específica, pois já se encontram sob a égide da legislação vigente" Afirma ainda que "alguns [tipos penais] necessitam apenas de ligeiras mudanças, para se adaptarem à sua consumação na Internet".

Em posição intermediária, o Deputado Federal Leo Alcântara, relator da análise e justificativa do PL 84/99, expôs no sentido de que seria possível a aplicação de alguns dos crimes já existentes, porém o princípio da estrita legalidade exige clareza no que se quer incriminar[12]:

> Alguns especialistas posicionam-se contra a criação de novos tipos legais para parte das condutas aqui tipificadas, entendendo já estarem

[10] **MIRANDA, Marcelo Baeta Neves**. Abordagem dinâmica aos crimes via internet. 1999. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1828>

[11] **COLARES, Rodrigo Guimarães**. Cybercrimes: os crimes na era da informática. 2002. Disponível em: <http://jus2.uol.com.br/texto.asp?id=3271>.

[12] **PIAUHYLINO, Luiz.** Comissão de Constituição e Justiça e de redação: Projeto de Lei nº 84, de 1999. Disponível em: <http://www.camara.gov.br/sileg/integras/1774.pdf>.

> contempladas na legislação penal vigente. Segundo eles, por exemplo, o dano ocasionado a dado ou programa de computador, enquadra-se no dano feito em coisa alheia, tipificado no código Penal no seu artigo 163 que dispõe:
>
> Art. 163. Destruir, inutilizar, ou deteriorar coisa alheia:
>
> Pena – detenção, de um mês a seis meses, ou multa.
>
> Não haveria necessidade, portanto, de novo tipo penal, para cuidar de tal conduta.
>
> Todavia, tendo em vista a exigência constitucional da lei anterior para definir o crime e impor a respectiva pena, não sendo admissível o uso de analogia ou ampliações para incriminar determinada conduta, preferimos adotar uma postura de prudência, reconhecendo como legítima a postulação de tal matéria em lei nova. É inegável a existência de dificuldades na punição das ações aqui enfocadas. Dando-lhes tratamento específico, colmatamos qualquer lacuna que porventura pudesse vir a ser invocada pelos agentes de conduta para evadir-se à justa sanção da sociedade, e eliminamos as referidas dificuldades.

Estudos doutrinários posteriores classificam os crimes informáticos em categorias como faz a maior parte da doutrina nacional, mesmo que através de nomes diferentes, como exemplificam GOMES[13], VIANNA[14] e WENDT[15], mas que, da mesma forma, os dividem semanticamente em crimes informáticos próprios, impróprios e mistos.

Tal classificação é de suma importância para esta pesquisa, sendo a demonstração de que existiam crimes informáticos não tipificados, devendo possuir legislação penal específica em alguns casos, e que em outros casos, seria necessário apenas o ajuste de alguns tipos já contidos no Código Penal. Entendemos que a melhor classificação seria dividi-los em:

I) **crimes impróprios de informática**: são os crimes já puníveis em nossa legislação penal, **cometidos através de meios informáticos**, sem lesar dados ou informações[16]. Atingem bens jurídicos já devidamente protegidos em nossa

---

[13] **GOMES, Ricardo Reis.** Crimes Puros de Informática. Págs. 7 e ss.

[14] **VIANNA, Túlio Lima**. Fundamentos de direito penal informático: do acesso não autorizado a sistemas computacionais. Págs. 13 e ss.

[15] **WENDT, Emerson**. Crimes cibernéticos. Pág. 19

[16] O tópico 2.1.3 desta monografia estuda os bens jurídicos protegidos nos crimes de informática. Neste ponto, importa saber que são protegidos a privacidade de forma mais ampla, as informações contidas nos dispositivos informáticos, e caso a caso, o patrimônio, a honra, etc.

legislação penal, sem ter como objeto material os dados informáticos. O usuário utiliza meios lícitos para cometer outros crimes, por exemplo: fraudes, estelionato, calúnia, difamação e injúria em e-mails, redes sociais e sites; armazenagem e divulgação de material pedófilo, tipificados nos artigos 241-B e 244-B, §1º da Lei 8.069/90; crimes contra a ordem tributária contido no artigo 2º, V da Lei 8.137/90; crimes da Lei de Falências constante no artigo 168, §1º, III da Lei 11.101/05. A informática é mero meio para praticar tais crimes.

II) **crimes próprios de informática** (ou ainda crimes informáticos): são aqueles que tem como **objeto material da conduta dados (informações) e sistemas computacionais**. O agente interfere de forma ilícita em dispositivo informático alheio para ter conhecimento do que ali está armazenado ou adulterar/destruir tais informações, sem atingir a propriedade ou honra de outrem. São crimes exclusivamente contra a privacidade que atingem tanto as informações, quanto os dispositivos que as armazenam. São exemplos: O caput do artigo 154-A do Código Penal e também a interceptação ilegal de dados informáticos tipificada em parte do caput do artigo 10 da Lei 9296/96.

III) **crimes informáticos mistos**, aqueles crimes que **tutelam além dos dados, bens jurídicos diferentes da privacidade**, como o patrimônio, a honra. O indivíduo prejudica o dispositivo informático de forma ilícita e ainda atinge o patrimônio, a honra. Enquadramos aqui as formas qualificadas e majoradas elencadas nos parágrafos 1º, 2º, 3º, 4º e 5º do artigo 154-A do Código Penal. Além delas, enquadramos o artigo 313-A e 313-B do mesmo código.

Desta forma, percebemos que o artigo 154-A tipificou alguns crimes próprios de informática, como a invasão de dispositivo (chamada na doutrina estrangeira de acesso não autorizado), a obtenção, adulteração ou destruição de dados e instalação/difusão de códigos maliciosos. Tipificou, porém, inúmeras majorantes e formas qualificadas destes crimes, de acordo com uma série de possibilidades de resultados. Poderia, neste ponto, atualizar alguns tipos penais, adequando-os aos meios informáticos.

Entendemos que era necessária sim a criminalização de algumas condutas da categoria **crimes próprios de informática**, em respeito à legalidade estrita e a função garantidora do tipo penal. As condutas criadas protegem a privacidade dos

titulares dos dispositivos informáticos contra novas condutas lesivas, que nem sempre poderão ser ressarcidas na esfera civil. Como dissemos, o único crime próprio de informática tipificado em nosso ordenamento punia a interceptação de dados informáticos na forma do artigo 10 da Lei 9.296/96. Com a criação do artigo 154-A do Código Penal, passam a ser penalmente puníveis novas condutas que atentam contra privacidade e que tem como objeto material a informática. O legislador, desta forma, “condensou” em um tipo penal a diretriz dada pela “Convenção de Budapeste” sobre criminalidade informática. Ocorre, porém, que o legislador fez isto de forma atécnica, criminalizando condutas já abarcadas por outros tipos penais, e utilizando expressões dúbias na redação do artigo, como veremos no próximo capítulo, o que entendemos ser uma grave violação à legalidade estrita.

2) ANÁLISE DO TIPO PENAL

Invasão de dispositivo informático

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.

2.1) OBJETO MATERIAL DA CONDUTA E BEM JURÍDICO PROTEGIDO

O tema “bem jurídico-penal” serve como baliza à intervenção mínima do Direito Penal em um Estado garantista, sendo o parâmetro que limita os legisladores na escolha do que poderá ser considerado crime em nossa sociedade. Neste tópico estudaremos quais são os bens jurídicos que o legislador escolheu como dignos da proteção penal do artigo 154-A.

2.1.1) O que é bem jurídico-penal?

Trata-se de conceito em constante evolução e definição variável por decorrência do momento histórico e carga cultural adotados para defini-lo. A título de ilustração, este conceito transformou-se de uma concepção de direito subjetivo do Estado, conceito dado por BINDING[17], que entendia que tal direito subjetivo possuía função de limitar os cidadãos por meio de normas, evoluindo até a ideia de direito fundamental atualmente[18].

Em breves palavras, é possível considerar bem jurídico como um valor social assegurado pela Constituição e que é essencial ao desenvolvimento humano. Cada cultura, em cada momento histórico, é que determina se o bem jurídico elencado é merecedor de proteção no âmbito penal. Na definição de ROXIN[19], os bens jurídicos são

> pressupostos imprescindíveis para a existência em comum, que se caracterizam numa série de situações valiosas, como (...) a vida, a integridade física, a liberdade de atuação, ou a propriedade, que toda a gente conhece, e [que] o Estado social deve também proteger penalmente.

[17] Apud **PRADO, Luiz Regis**. Bem Jurídico-penal e constituição. Págs. 32-33

[18] Para um estudo aprofundado da evolução do conceito de bem jurídico, recomendo a leitura do livro de Luiz Regis Prado

[19] Apud **PRADO, Luiz Regis**. Bem Jurídico-penal e constituição. Pág. 47

A importância de conhecer os bens jurídicos envolvidos em uma pesquisa decorre de conhecer suas funções, papéis peculiares que eles desempenham para harmonizar a aplicação do direito. Enumera o autor[20] como funções dos bens jurídicos:

> 1. Função de garantia ou de limitar o direito de punir do Estado: o bem jurídico é erigido como conceito limite na dimensão material da norma penal (...) limita o legislador em sua atividade no momento de produzir normas penais.
>
> 2. Função interpretativa (...) não é possível interpretar, nem portanto conhecer, a lei penal, sem lançar mão da ideia de bem jurídico (...)
>
> 3. Função individualizadora (...) [para a criação de um crime] leva-se em conta a gravidade da lesão ao bem jurídico (...)
>
> 4. Função sistemática: [o bem jurídico seria o] elemento classificatório decisivo na formação dos grupos de tipos da parte especial do Código Penal.

2.1.2) Objeto material da conduta e bem jurídico

Outro ponto importante neste tópico é diferenciar bem jurídico de objeto material da conduta criminosa. Pelo que foi exposto, é possível confundir ambos os conceitos por serem abstratos. Tal confusão pode ocorrer pois a conduta criminosa é lesiva tanto ao objeto material quanto ao bem jurídico; O objeto material da conduta criminosa é atingido no mundo fático, enquanto o bem jurídico é atingido apenas no plano jurídico-normativo.

Para ilustrar, usaremos um exemplo de furto, sem adentrar em discussões doutrinárias, reproduzindo o entendimento majoritário da doutrina:

Considere que José furtou a televisão de Antônio quando este estava trabalhando. Eis o artigo penal que pune tal conduta:

"Furto

Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel"

Objeto material do furto: A coisa alheia móvel, no caso, a televisão de Antônio.

Bens jurídicos protegidos contra o furto: O direito à posse e à propriedade.

---

[20] **PRADO, Luiz Regis**. Bem Jurídico-penal e constituição. Págs. 60-61

No exemplo acima é fácil visualizar os conceitos estudados. O problema maior se dá quando o bem jurídico protegido coincide com o objeto material do delito, como é o caso de um crime de injúria:

"Injúria

Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro"

Objeto material da injúria: A disposição da honra.

Bem jurídico protegido: O direito a dispor da própria honra.

Vistas estas noções, devemos arrematar que o legislador constituinte escolheu bens jurídicos dignos de proteção, originando os chamados direitos fundamentais na Constituição Federal de 1988. Desta forma, a atividade legiferante infraconstitucional está vinculada em sua escolha de bens jurídicos merecedores de proteção no âmbito penal. Devem ser respeitados os princípios de um Estado Democrático de Direito Garantista, como intervenção mínima, legalidade estrita e ampla, taxatividade, entre outros. O direito penal deve agir sempre como última solução de conflitos. É preciso, portanto, um verdadeiro estudo durante o processo legislativo, visando dirimir conflitos com outras formas de tutela, como a responsabilidade cível e administrativa, evitando, se possível, a repressão penal. O legislador, representante da sociedade, deve estar vinculado sempre às regras e valores constitucionais, sabendo distinguir o que deve ou não ser criminalizado.

2.1.3) O bem jurídico penal protegido

Qual é o bem jurídico penal (ou quais são?) que se torna(m) protegido(s) a partir da tipificação da invasão a dispositivos informáticos?

A matéria foi discutida na doutrina nacional antes da promulgação do artigo 154-A de nosso Código Penal. Inicialmente, os autores, de forma generalizada, entendiam que este crime e seus similares, ainda não tipificados, eram de conteúdo patrimonial, devido ao clássico exemplo de furto em que um "hacker" invadiria o

computador de uma pessoa para furtar dados. GOMES[21] nega a aplicação do crime patrimonial ao caso

> porque o furto é um crime material onde há a diminuição do patrimônio do sujeito passivo, e, em contrapartida, um aumento do patrimônio do sujeito ativo. Quando um arquivo é furtado de outro computador, não é uma diminuição patrimonial, pois o mesmo não é retirado da posse do sujeito passivo. Na verdade, o arquivo é copiado por aquele que comete o ato [...] não há subtração e, por conseguinte, não há o furto.

O autor explica que para o cometimento dos crimes informáticos seria necessário o uso de equipamentos informáticos como instrumentos, e que o crime se dirigisse necessariamente contra dados.

Posteriormente, VIANNA[22] estuda o "acesso não autorizado a sistema informático" baseado na doutrina europeia sobre crimes informáticos. Criou classificação similar a de GOMES. Porém, VIANNA entende que estes crimes teriam como bem jurídico protegido a informação, corolário da privacidade.

Os especialistas do assunto tendiam a seguir a doutrina europeia continental, como analisou CRESPO[23], elegendo também a informação, e sua forma de representação, os dados, como bens protegidos por estes crimes. Este autor, porém, nega que a informação seja o único bem jurídico protegido. Argumenta que os "crimes digitais" [24] são complexos e pluriofensivos, ou seja, atingem mais de um bem jurídico. Não definiu, porém, quais são os outros bens jurídicos a serem tutelados. Da mesma forma de entendimento, WENDT[25].

Porém, o Projeto de Lei 84/99, que trazia o entendimento baseado na doutrina europeia sobre o assunto, não prosperou por não poder mais ser modificado de acordo com o regimento interno da Câmara dos Deputados. Com a rápida edição da Lei 12.737 de novembro de 2012, a maior parte da doutrina nacional[26] que estudou o tema a partir de então manifestou o entendimento de que **o tipo penal 154-A**

---

[21] **GOMES, Ricardo Reis.** Crimes Puros de Informática.

[22] **VIANNA, Túlio Lima**. Fundamentos de direito penal informático: do acesso não autorizado a sistemas computacionais. Pág. 10

[23] **CRESPO, Marcelo Xavier de Freitas**. Crimes digitais. Págs. 56-58

[24] Nomenclatura utilizada por **CRESPO**.

[25] **WENDT, Emerson**. Crimes cibernéticos. Págs. 18-20

[26] BITENCOURT, CABETTE, CAVALCANTE, NUCCI.

protege a privacidade em sentido mais amplo, da qual a intimidade é sua espécie. Os autores justificam utilizando como principal argumento a localização topográfica do crime no código penal, dito em outras palavras, o local onde o artigo foi "encaixado" na referida lei. Vejamos:

Código Penal - PARTE ESPECIAL

TÍTULO I - DOS CRIMES CONTRA A PESSOA

CAPÍTULO VI - DOS CRIMES CONTRA A LIBERDADE INDIVIDUAL

SEÇÃO IV - DOS CRIMES CONTRA A INVIOLABILIDADE DOS SEGREDOS

154-A - Invasão de dispositivo informático

Pelo diagrama acima, é fácil entender o que os autores colocaram para nós: Trata-se de crime contra as pessoas, mais especificamente contra seu direito a liberdade, em sua acepção de privacidade.

Esta também é a justificativa constante do projeto que deu origem à lei 12.737/2012[27]. Segundo o legislador, a invasão de dispositivo informático deve aproveitar a vasta jurisprudência existente sobre o crime de violação de correspondência, visto que utilizam verbos com semântica semelhante ("invadir" e "devassar"). Até o momento[28] não se sabe sobre a ocorrência de qualquer denúncia pelo cometimento de invasão a dispositivo informático, o que impossibilita estudar o tratamento dado pelos magistrados a esta discussão.

Concordamos com a doutrina atual que afirma ser a liberdade individual o bem jurídico penal protegido pelo crime em estudo. Entendemos esta posição como mais acertada por considerar que a proteção à liberdade abarca não apenas a privacidade, mas também a proteção à informação. Quando se realiza a conduta de invasão de dispositivo informático, podemos inferir que houve invasão a uma esfera privada de um indivíduo. O cunho patrimonial é apenas secundário, pois nem sempre o invasor sabe a que informação terá acesso, e não se pode falar em crime

[27] **TEIXEIRA, Paulo** e outros. Projeto de Lei 2793/2011. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>

[28] Início de agosto de 2013.

patrimonial quando o bem não possui valor ao seu dono, seja econômico ou pessoal. Da mesma maneira entendemos a tutela à honra como secundária, visto que a invasão pode ocorrer apenas para transtornar a vida da vítima, como nos casos de instalação de vulnerabilidades, de destruição aleatória de informações. Por isto, acreditamos que criminalizar a invasão tem por objetivo primário a proteção à privacidade de uma pessoa, considerando que as condutas deste tipo penal são pluriofensivas e podem atingir outros bens jurídicos, como os já citados.

Em relação aos que pregam a proteção à informação, concordamos que este tipo tem a finalidade de evitar o acesso a informações privadas. Parece-nos, porém, que esta tutela pode ser deduzida de uma proteção ampla à privacidade, levando em conta que qualquer invasão ocorrerá contra um dispositivo informático de uma pessoa física ou jurídica[29], não vislumbrando a ocorrência deste crime sem que seja atingida a esfera privada de algum sujeito de direitos.

Existe ainda o argumento utilizado pelos autores nacionais, o posicionamento topográfico do artigo 154-A. A posição que ele ocupa no Código Penal deve também ser levada em conta, não como argumento único, mas como tese complementar. Neste argumento, consideramos também acertada a doutrina dominante. Ficaria descaracterizada aqui também a hipótese de ser um crime predominantemente patrimonial.

Sintetizando, este estudo tem como referência que o artigo 154-A do Código Penal protege, de forma imediata, a privacidade, e que também possui, de forma mediata, condutas ofensivas a outros bens jurídicos, como o patrimônio, a honra, entre outros, a depender das circunstâncias apresentadas.

[29] Sobre o direito à privacidade das pessoas jurídicas, recomendamos a leitura do trabalho de **MATOS, Eneas de Oliveira**. Direitos da personalidade e pessoa jurídica

2.1.4) Nomenclatura

Segundo CRESPO[30], “uma das primeiras questões que deve ser observada quando se pretende discorrer sobre tais ilícitos reside na nomenclatura”. É preciso analisar os termos que utilizamos, pois o vernáculo faz parte da ciência jurídica. Provavelmente o leitor já se deparou com diversos nomes para as condutas em estudo: “*cybercrimes”*, crimes virtuais, crimes digitais, crimes cibernéticos, crimes de informática, entre outras, muito difundidas pela mídia. Esta confusão, segundo CRESPO[31],

> se dá por dois motivos: 1) a constante evolução tecnológica faz com que muito frequentemente haja novos mecanismos, aparelhos e técnicas disponíveis, sendo intuitivo que isso interfere no vocabulário; 2) no mais das vezes, os termos são cunhados na língua inglesa e, depois, introduzidos em nosso vocabulário ou ‘nacionalizados’, havendo forte presença de neologismos.

Como forma de parâmetro, VIANNA coloca em sua tese que “a boa técnica manda que se dê nome aos delitos com base no bem jurídico por ele protegido” [32]. Cita ainda FRAGOSO[33]:

> A classificação dos crimes na parte especial do código é questão de técnica legislativa, e é feita com base no bem jurídico tutelado pela lei penal, ou seja, a objetividade jurídica dos vários delitos ou das diversas classes de intenções.

Ao considerarmos os bens jurídicos em estudo, podemos eliminar expressões relacionadas à cibernética, “a ciência que busca estabelecer uma teoria geral do controle, seja ele tanto de seres inanimados, quanto de organismos vivos, ou mesmo de máquinas [...]”[34].

---

[30] **CRESPO, Marcelo Xavier de Freitas**. Crimes digitais. Pág 47

[31] Idem.

[32] **VIANNA, Túlio Lima**. Fundamentos de direito penal informático: do acesso não autorizado a sistemas computacionais. Pág. 9

[33] Idem.

[34] Idem, pág. 11

Também concordamos com este autor que entende incabível a nomenclatura crimes virtuais. O termo virtual refere-se à simulação gráfica de um objeto real. Não entendemos ser protegido um bem jurídico simulado.

A maior parte da doutrina brasileira utiliza a expressão “crimes informáticos” como a doutrina espanhola o faz. Trata-se de nomenclatura criada com base no objeto material da conduta de invasão, mas que também se adequa aos bens jurídicos protegidos: informática é a ciência que estuda os meios de armazenar, processar e transmitir informações automatizadamente. Considerando a informação um corolário da privacidade, e que a invasão é uma conduta relacionada à violação da privacidade[35], entendemos que esta nomenclatura é a mais adequada e será utilizada ao longo deste trabalho.

2.2) CLASSIFICAÇÃO DO TIPO

É sempre útil buscar a classificação de um crime, como forma de indexá-lo cientificamente. Eis nossa percepção:

Trata-se de um **crime comum**, visto que pode ser praticado por qualquer pessoa; Em relação à classificação em crime de dano ou de perigo, devemos considerar que: a) O **caput** do artigo 154-A trata-se de um **crime de dano**, visto que exige uma lesão ao bem jurídico protegido – a invasão fere a privacidade de outrem - para sua consumação. b) Diversamente, os **crimes equiparados** à invasão, contidos no §1º, seriam **crimes de perigo**, pois bastam as condutas realizadas, independentemente da ocorrência do dano efetivo à privacidade, para que sejam punidos.

Quanto à classificação que leva em consideração se são crimes materiais, formais ou de mera conduta, entendemos que se trata de **crime formal,** pois não é necessário que a conduta produza o resultado esperado para que seja punida. Diferem-se dos crimes de mera conduta por possuírem um resultado natural. Não necessitam, porém, realizar tais resultados para se consumarem, como os crimes materiais.

[35] Conforme será explicado no tópico 2.5.1 ‘a’.

Consideramos também que se trata de **crime de concurso eventual**, podendo ser cometido por um ou mais agentes; Além disto, pensamos que o caput é um **crime instantâneo de efeitos permanentes,** enquanto as condutas equiparadas do parágrafo 1º seriam apenas **crimes instantâneos,** sem produzir efeitos no tempo.

Importante também situá-lo de acordo com a doutrina dos crimes informáticos[36]. Se considerássemos apenas o caput do artigo 154-A, concluiremos que é um **crime próprio de informática**. Como foi visto, porém, os crimes descritos nos parágrafos do artigo 154-A protegem também outros bens jurídicos, sendo condutas consideradas **crimes informáticos mistos**.

2.3) SUJEITOS DO DELITO

2.3.1) Sujeito ativo

MAGGIO[37], por todos na doutrina esclarece: *"O crime de acesso não autorizado é um crime comum, ou seja, pode ser praticado por qualquer pessoa, não sendo necessária qualquer característica ou qualidade pessoal para o efetivo cometimento do delito"*. Desta forma, não se exige que o delinquente seja técnico em informática, ou mesmo que trabalhe em serviços relacionados à tecnologia da informação para invadir dispositivos alheios.

[36] Visto no capítulo 1.3 deste trabalho.

[37] **MAGGIO, Vicente de Paula Rodrigues.** Novo crime: Invasão... Disponível em:<http://atualidadesdodireito.com.br/vicentemaggio/2012/12/16/invasao-de-dispositivo-informatico-cp-art-154-a>

2.3.2) Sujeito passivo

CABETTE[38] explica que “qualquer pessoa que tenha sua privacidade violada pelo invasor é sujeito passivo da infração”. BITENCOURT[39], porém, discorda desta ideia e explica que

> sujeito passivo não se confunde com prejudicado; embora, de regra, coincidam, na mesma pessoa, as condições de sujeito passivo e prejudicado, podem recair em sujeitos distintos. Aquele é o titular do bem jurídico protegido e, na hipótese, lesado, enquanto este é qualquer pessoa que, em razão do crime, sofre prejuízo ou dano material ou moral; o primeiro será a vítima da relação processual-criminal, e o segundo será testemunha, embora interessada.

Em uma leitura baseada na estrita legalidade e no garantismo penal, é preciso interpretar de forma restritiva o texto legal. Podemos afirmar que apenas serão sujeitos passivos dos crimes contidos no artigo 154-A:

- o proprietário do dispositivo violado, visto que o caput do crime exige que o dispositivo informático objeto da conduta seja de alguém que não o invasor;

- o titular das informações acessadas, que também está protegido no final caput;

- o titular das comunicações eletrônicas privadas, dos segredos comerciais ou industriais e das informações sigilosas, conforme o parágrafo 3º

Não podemos generalizar onde o legislador restringiu. Limitando os sujeitos passivos às três hipóteses existentes na lei, veremos a real amplitude do tipo penal. Acreditamos que tais sujeitos podem ser pessoas físicas ou jurídicas, nestas últimas inclusas tanto as pessoas jurídicas de direito privado quanto de direito público (administração direta e indireta).

---

[38] **CABETTE, Eduardo Luiz Santos**. Primeiras impressões... Disponível em:<http://jus.com.br/revista/texto/23522>. No mesmo sentido, **MAGGIO.**

[39] **BITENCOURT, Cezar Roberto**. Invasão de dispositivo informático. Disponível em**: <**http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico>

2.4) ASPECTOS SUBJETIVOS DO TIPO

2.4.1) Dolo

Todos os doutrinadores referenciados neste trabalho concordam que o tipo estudado pode apenas ser realizado na forma dolosa. De acordo com o artigo 154-A, o sujeito deve agir com livre vontade e consciência atual de invadir dispositivo informático alheio. Trata-se do dolo natural da concepção finalista de crime, sem elementos normativos.

Desta forma, discordamos de BITENCOURT quando diz que *"é necessário que o agente tenha consciência que a sua conduta é ilegítima"* [40]. Esta afirmativa nos remete ao conceito de '*dolus malus',* da superada teoria neoclássica, que continha em seu bojo a consciência sobre a ilicitude da conduta. Tal consciência, atualmente, foi deslocada para a análise da culpabilidade da conduta.

2.4.2) Especiais fins de agir

São elementos subjetivos do tipo que não integram o dolo, visto que ele se encerra com a vontade e consciência de obter o resultado da conduta. Na verdade, os fins especiais de agir ampliam e fundamentam a ilicitude do fato. *"Eles especificam o dolo, sem a necessidade de se concretizarem, sendo suficiente que existam no psiquismo do autor*"[41].

O caput do artigo 154-A e seu parágrafo primeiro vinculam a vontade do agente a três fins especiais de agir. Dividindo o texto da lei, teríamos:

Fins específicos de agir no crime de invasão (154-A caput)

I) *obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo*

II) *ou instalar vulnerabilidades para obter vantagem ilícita*

---

[40] **Idem.**

[41] **BITENCOURT, Cezar Roberto.** Tratado de direito penal: parte geral. Pág. 321 e 322.

Fim específico de agir nos crimes equiparados à invasão (154-A §1º)

III) *§ 1º (...) com o intuito de permitir a prática da conduta definida no caput.*

Os fins de agir são elementares do tipo, o que significa dizer que o agente que pratica a invasão (ou seus crimes equiparados) sem estas finalidades descritas, não pratica os crimes dos artigos 154-A e 154-A, §1º do Código Penal.

O limite destes elementos normativos será analisado no subtítulo seguinte.

2.4.3) Culpa

Não há previsão de modalidade culposa. Conforme o princípio da excepcionalidade do crime culposo, contido no artigo 18, parágrafo único do código penal, salvo casos expressos, nenhum agente deve ser punido por crime senão quando o pratica de forma dolosa. A culpa precisa de previsão expressa em lei para que seja punível no direito penal.

CABETTE[42] ilustra com o caso do técnico em informática contratado para consertar computadores pessoais, que acaba, por imperícia, imprudência ou negligência, apagando os dados do dispositivo do contratante. Esta é uma situação bastante comum que não é digna de sanção penal, embora seja passível de indenização na esfera da responsabilidade cível. Não há tipo culposo de invasão, logo não há crime.

[42] **CABETTE, Eduardo Luiz Santos**. Primeiras impressões sobre a Lei nº 12.737/... Disponível em: <http://jus.com.br/revista/texto/23522>.

2.5) DO TIPO OBJETIVO

O legislador utilizou muitas expressões que podem assumir sentidos diversos, o que prejudica a interpretação do texto legal. **LUIZ FLÁVIO GOMES**[43] confirma esta afirmativa quando diz: "*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."* Em matéria penal, conforme o princípio da legalidade estrita e da taxatividade, não devem existir dúvidas na conduta que se quer incriminar, pois seus limites devem estar claros a qualquer cidadão, como forma de garantia à liberdade pessoal. Sabe-se, porém, que a evolução da hermenêutica permite a adoção de elementos normativos quando estritamente necessário, que é o caso dos crimes informáticos.

Como provavelmente não teremos uma reedição próxima deste tipo penal, é preciso interpretá-lo de forma a aproveitar o máximo do que foi produzido. Com algumas técnicas e questionamentos que julgamos pertinentes, poderemos aplicar, mesmo que parcialmente, o que foi elaborado pelo legislador.

Pela complexidade da estrutura do tipo penal, dividiremos o artigo em partes para facilitar o estudo. Em cada uma delas, serão destacadas as expressões que admitem mais de uma interpretação, apresentaremos as definições que consideramos adequadas, e, logo após, uma análise crítica do sentido que estas expressões representam para o crime em estudo.

2.5.1) Art. 154-A caput: Invasão simples

a) Invadir dispositivo informático alheio

[43] **LUIZ FLÁVIO GOMES.** Lei "Carolina Dickman" e sua (in)eficácia. Disponível em:< http://www.lfg.com.br/conteudos/artigos/direito-criminal/artigo-prof-luiz-flavio-gomes-lei-carolina-dickman-e-sua-in-eficacia>.

I) INVADIR - O verbo nuclear do tipo penal é “invadir”. Segundo o *Michaelis Moderno Dicionário da Língua Portuguesa*, pode assumir as seguintes significações pertinentes[44]:

> 1 Entrar à força em: *Átila invadiu a Gália.*
>
> 2 Assumir indevidamente ou por violência; usurpar: *Detestava que invadissem suas atribuições. (...)*
>
> 4 Avassalar, dominar, tomar: "Invadia-os o cansaço" (Machado de Assis).

A invasão no tipo penal, pela semântica relacionada, conota o ‘entrar’ o ‘usurpar’, o ‘domínio’, mesmo que mínimo, do dispositivo informático alheio. Ao invadir um dispositivo, o agente deve, de alguma forma, ter controle dos processos que ocorrem no dispositivo invadido, daí o porquê de ele ter acesso às informações contidas.

Julgamos esta uma infeliz escolha do legislador. O verbo nuclear “invadir”, possui amplitude variada, porém não possui nenhum sentido específico aplicável à Ciência da Computação. Muito mais lógico seria utilizar o verbo “acessar”, consagrado na doutrina comparada como crime autônomo inclusive, visto que para esse ramo científico o acesso deve ser entendido como a ação de ler, escrever ou executar dados armazenados em dispositivos informáticos. [45] Estas ações, em linguagem técnica, são, conforme VIANNA [46]:

> **Leitura** é a recuperação dos dados armazenados no sistema com sua consequente interpretação como informações humanamente inteligíveis. A **escrita** consiste na inserção, remoção ou alteração de dados no sistema. A **execução** de dados, mais precisamente de programas, é o processamento de informações automatizadas de acordo com as instruções preestabelecidas.

O verbo acessar, como podemos concluir, está diretamente relacionado aos fins específicos de agir que compõem este tipo penal.

---

[44] Disponível em: <http://michaelis.uol.com.br/moderno/portugues/index.php?lingua=portugues-portugues&palavra=invadir>

[45] **VIANNA, Túlio Lima**. Fundamentos de direito penal informático (...) pág. 93

[46] Idem.

Curiosamente, o verbo “invadir” substituiu o verbo “devassar” antes da promulgação da lei. Segundo o mesmo dicionário[47], devassar significa:

> 1 Invadir ou observar (aquilo que é defeso ou vedado): *Devassar a casa do vizinho*.
>
> 2 Ter vista para dentro de: *Nossa janela devassa os outros apartamento*s.
>
> 3 Descobrir, penetrar, esclarecer: "...o desejo nos levou a devassar os segredos dessas terras afastadas" (Gonçalves Dias). *vtd*
>
> 4 Olhar, contemplar: "Saíra, abriu os olhos e devassou a sombra com pavor" (Coelho Neto).

Apesar de atuarem em uma das concepções como verbos sinônimos, parece-nos ainda que o legislador agiu de forma inadequada mais uma vez: “devassar” seria mais apropriado do que o verbo “invadir” para criminalizar o acesso às informações contidas nos dispositivos alheios por possuir uma semântica mais próxima com o bem jurídico privacidade.

II) DISPOSITIVO INFORMÁTICO - Trata-se do objeto material da conduta de invasão. Tal expressão é problemática à primeira vista: o que se considera dispositivo informático? Por ser nosso referencial teórico a estrita legalidade, não podemos interpretar de forma extensiva tais conceitos.

A técnica científica nos orienta a começar qualquer estudo de um objeto estabelecendo seus limites, classificando-o. Delimitando os dispositivos por seu adjetivo “**informático**”, ou os quais se referem à informática, poderemos chegar a um conceito útil.

A doutrina[48] atribui ao engenheiro francês Philippe Dreyfus a utilização da palavra “informática” como junção das palavras “informação” e “automática”.

---

[47] Disponível em: <http://michaelis.uol.com.br/moderno/portugues/index.php?lingua=portugues-portugues&palavra=devassar>

[48] **VIANNA, Túlio Lima**. Fundamentos de direito penal informático (...) pág. 10 e **GRECO, Rogério.** Comentários sobre o crime (...). Disponível em: <http://www.rogeriogreco.com.br/?p=2183>

Devemos entender que serão objetos materiais da conduta quaisquer dispositivos que processem informações de maneira automatizada. Essas informações automatizadas por meio eletrônico são chamadas de “dados”. Conforme esclarece GRECO,

> para que se possa considerar um sistema [rectius: dispositivo] informático se deve verificar necessariamente a realização das seguintes tarefas básicas:
>
> Entrada: Aquisição dos dados;
>
> Processo: Tratamento dos dados;
>
> Saída: Transmissão dos resultados” .
>
> Assim, de acordo com a conceituação e requisitos apontados acima, o dispositivo informático seria todo aquele aparelho capaz de receber os dados, trata-los, bem como transmitir os resultados, a exemplo do que ocorre com os computadores, smartphones (...) etc.

Devemos considerar, portanto, quaisquer aparelhos que recebam informações eletrônicas (dados), processem-nas e devolvam um resultado, tudo isso de forma automatizada. Esta constatação demonstra que a expressão **“dispositivo informático”**, quando interpretada literalmente, é demasiadamente vaga, pois vislumbraria possibilidades absurdas, como por exemplo, um automóvel, visto que possui um painel eletrônico onde processa informações e retorna um resultado ao seu usuário.

Por isso não podemos nos valer apenas da interpretação gramatical. Devemos buscar a finalidade pretendida pelo legislador por interpretação teleológica, e verificar se o vernáculo é adequado de acordo com o princípio da legalidade estrita.

Considerando o bem jurídico em estudo, a privacidade, o ideal seria entendermos como dispositivos apenas os **aparelhos eletrônicos que guardam dados pessoais de seu usuário**. Guardar no sentido de armazenar, manter em depósito.

Desta forma, eliminaríamos as hipóteses absurdas, sem precisar, porém, elaborar um rol que defina quais aparelhos serão considerados, ou não, dispositivos

informáticos passíveis de sofrer invasão. Não esquecendo os fins específicos de invadir que já tivemos conhecimento, seriam passíveis de invasão, por exemplo, computadores, telefones celulares, smartphones, tablets, câmeras digitais, filmadoras, dispositivos de armazenamento de dados como pendrives e HD's externos.

III) ALHEIO - Este elemento normativo assume a mesma conotação que a doutrina utiliza para os crimes patrimoniais. O dispositivo informático deve ser necessariamente de propriedade ou posse alheia. Caso não o seja, não haverá o crime de invasão de dispositivo, impossibilitando caracterizar como crime a hipótese onde um sujeito invade o próprio dispositivo informático. Entendemos pertinentes as anotações de BITENCOURT[49] sobre o elemento normativo "coisa alheia" do crime de furto, por considera-las também aplicáveis ao tipo em estudo:

> A condição "alheia" é elemento normativo indispensável à tipificação (...); sua ausência torna a conduta atípica. A expressão alheia tem o sentido de coisa que não tem ou nunca teve dono. Por isso, as coisas sem dono (res nullius), abandonadas (res derelicta) e as coisas comuns (res communes omnium) não podem ser objeto (...) [do crime].
>
> Não há necessidade de identificar o proprietário ou possuidor. A comprovação de que pertence a alguém tem a finalidade de excluir a res nullius, res derelicta (...).

Desta forma, trata-se de elementar do tipo penal, já conhecida dos juristas, sem maiores problemas em sua hermenêutica.

IV) QUAL É A CONDUTA INCRIMINADA PELA EXPRESSÃO "INVADIR DISPOSITIVO INFORMÁTICO ALHEIO"?

Trata-se do núcleo da conduta criminosa, ou seja, a invasão a dispositivo informático alheio. Parte da doutrina[50] entende que o caput do artigo 154-A apresenta dois núcleos de conduta (verbos 'invadir' e 'instalar'). Discordamos,

[49] **BITENCOURT, Cezar Roberto**. Tratado de direito penal: parte especial vol. 3. Pág 35.

[50] **MAGGIO, Vicente de Paula Rodrigues**. Novo crime: Invasão ... Disponível em:<http://atualidadesdodireito.com.br/vicentemaggio/2012/12/16/invasao-de-dispositivo-informatico-cp-art-154-a>

juntamente com BITENCOURT[51]. O verbo nuclear é apenas “invadir”, se considerarmos a estrutura do tipo. O verbo “instalar”, como será visto, compõe apenas uma das finalidades específicas de agir. Em uma breve justificativa, entendemos que a conduta de invadir é um antecedente necessário para possibilitar a instalação de vulnerabilidade. Considerarmos também a impossibilidade de interpretarmos de forma ampliativa um tipo penal à luz da estrita legalidade.

Trata-se de crime formal, que se consuma com a invasão; caso atinja qualquer uma das finalidades específicas, será considerado como exaurimento do crime. A intenção do legislador era, segundo o projeto de lei, de não criar tipos de mera conduta

> cuja simples prática - independentemente do resultado obtido ou mesmo da específica caracterização da intenção do agente - já corresponderia à consecução da atividade criminosa. Tal estratégia redacional, típica de uma sociedade do risco e de uma lógica de direito penal do inimigo, busca uma antecipação da tutela penal a esferas anteriores ao dano, envolvendo a flexibilização das regras de causalidade, a tipificação de condutas tidas como irrelevantes, a ampliação e a desproporcionalidade das penas e a criação de delitos de perigo abstrato, dentre outras características. [52]

Concordamos com o legislador que os crimes de mera conduta devem ser evitados no atual estágio garantista que chegamos. Porém não acreditamos serem os crimes formais a solução para tal problema. Melhor seria se o legislador tivesse criado tipos de crimes materiais, ou seja, que exigem a verdadeira lesão ao bem jurídico para que sejam relavantes à persecução penal. Caso adotasse o verbo “acessar”, em seu conceito técnico, teria criado um crime material, que se consumaria com a leitura, escrita ou execução dos dados. Neste ponto o legislador não refletiu seu pensamento no texto legal.

Outro ponto em que não agiu bem, em nossa opinião, foi ao utilizar a expressão “dispositivo informático” por ser esta demasiadamente ampla. Será que todos os operadores do direito buscarão o mesmo sentido que buscamos ao estudar a expressão “dispositivo informático”? Será que o legislador quis abarcar a amplitude que verificamos neste trabalho? O ideal seria acrescer um artigo definindo

---

[51] **BITENCOURT, Cezar Roberto**. Invasão de dispositivo informático.

[52] **TEIXEIRA, Paulo** e outros. Projeto de Lei 2793/2011. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>

“dispositivo informático”, não em um rol fechado, mas em uma definição, tal qual fizemos.

b) conectado ou não à rede de computadores

I) CONECTADO - Devemos entender a comunicação entre duas partes, sua união. São considerados dispositivos informáticos conectados aqueles que podem trabalhar de forma conjunta, estando disponíveis reciprocamente para realização de tarefas.

II) A REDE DE COMPUTADORES - Quando o assunto é rede de computadores na ciência da informática, deve-se compreender um conjunto de dois ou mais dispositivos informáticos, autônomos e que se interligam para compartilhar informações e componentes. Trata-se de união feita por cabos (rede de telefonia ou fibras ópticas), ondas de rádio (Wi-fi), satélites, etc.

Esta união visa uma melhoria no desempenho do trabalho realizado, seja para compartilhar informações diretamente entre os dispositivos, sem a necessidade de levar um conteúdo de um dispositivo para outro, seja para, por exemplo, compartilhar um acessório que apenas um dos dispositivos tenha, como por exemplo, uma impressora. A *INTERNET* é a maior rede a nível mundial (por ser a rede pública por excelência) à qual os dispositivos se conectam para obter tais benefícios. Da mesma forma existem redes menores, como um escritório de uma empresa ou até mesmo um ponto de acesso portátil

Para a adequação típica, portanto, o legislador utilizou expressão ampla, que admite qualquer tipo de união entre dispositivos, móveis ou fixos, via cabos, via ondas de rádio/satélite.

III) QUAL É O SENTIDO QUE “CONECTADO OU NÃO À REDE DE COMPUTADORES” IMPLICA NA CONDUTA DE INVASÃO?

O próprio legislador esqueceu-se de explicar tal expressão na justificativa do projeto de lei, não fazendo consideração alguma sobre ela. BITENCOURT afirma

que é irrelevante que o dispositivo esteja conectado à internet, sendo esta a confirmação de que a “proteção penal não é da rede mundial de computadores, mas da privacidade individual...” [53]. Outros autores, consoantes às palavras de MAGGIO, afirmam ser "indiferente o fato de o dispositivo estar ou não conectado à rede...”. [54]

Entendemos aqui, por interpretação teleológica, que a intenção do legislador foi explicitar que o crime pode ser cometido tanto através de outro dispositivo, como diretamente contra o dispositivo “alvo”. O agente pode invadir o dispositivo tanto estando no mesmo local que o objeto do crime, quanto à distância, enviando comandos através da *INTERNET.*

Um detalhe não percebido pela doutrina, mas que faz diferença nesta análise é a determinação “a rede de computadores”. Pode haver quem interprete a determinação da rede através da utilização do artigo definido feminino “a” restritivamente. Não se trataria, portanto, de qualquer rede de computadores, mas apenas à rede mundial, a INTERNET. De forma leiga, por muito tempo se entendeu como 'internet' qualquer menção à rede de computadores. Claro que se trata de um entendimento simplista, comparado às definições de rede de computadores apresentadas neste trabalho, porém não podemos ignorar que esta confusão era comum até o início dos anos 2000. Portanto, poder-se-ia arguir que uma invasão através de uma rede privada não caracterizaria a invasão conectada à rede de computadores.

Por este enfoque, identificamos uma falha na redação da lei, visto que os casos de invasão através de uma rede local não estariam claramente abarcados neste tipo penal, o que, imaginamos, não foi a intenção do legislador.

Esta divagação perde o sentido quando o legislador utiliza a expressão “ou não”. Se o fato de estar conectado ou não à rede de computadores não interfere na conduta, a melhor opção seria suprimir tal expressão do tipo penal, por ser uma expressão inócua ao resultado incriminador.

---

[53] **BITENCOURT, Cezar Roberto**. Invasão de dispositivo informático. Disponível em**: <**http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico>.

[54] **MAGGIO, Vicente de Paula Rodrigues**. Novo crime: Invasão ... Disponível em:<http://atualidadesdodireito.com.br/vicentemaggio/2012/12/16/invasao-de-dispositivo-informatico-cp-art-154-a>

c) mediante violação indevida de mecanismo de segurança

Outra dificuldade gerada na hermenêutica deste tipo penal reside aqui. Consoante assinala BITENCOURT[55], o tipo contém um elemento normativo de ilicitude, o que exige juízo de valor para que a adequação típica se veja completa. Em outras palavras, é necessário saber quando a violação é "indevida" (injusta) ou devida (justa). Exige ainda que a violação seja de "mecanismo de segurança", limitando o âmbito da violação ilícita. Vejamos o sentido de tais expressões e algumas observações que devemos extrair delas.

I) MEDIANTE VIOLAÇÃO INDEVIDA - Conforme assinalamos, trata-se de elemento normativo da ilicitude. Está diretamente relacionado com o verbo nuclear **"invadir"**, que em sua semântica prevê uma violação indevida. Como estudamos na parte geral do direito penal, esta expressão normalmente é analisada após a confirmação da tipicidade da conduta. Aqui, porém, ocorre de maneira distinta: a valoração da ilicitude está contida na adequação típica. O operador do direito deve analisar se a invasão viola a lei (não incidindo qualquer das excludentes de ilicitude) ou se não foi autorizada (a privacidade é um direito disponível).

II) MECANISMO DE SEGURANÇA - Chama-nos a atenção esta expressão quando da leitura do artigo: o que são mecanismos de segurança para o direito penal? Considerando que o tipo penal confere **proteção à privacidade** do ofendido, e se tratando de **dispositivos informáticos**, podemos inferir através de uma interpretação teleológica que se trata de uma "barreira", uma proteção colocada pelo titular dos dados, de forma a proteger o conteúdo privado contra violações não autorizadas. Estas barreiras, pensamos, podem assumir inúmeras formas, como visto na doutrina nacional. A doutrina entende que tais barreiras são programas de computador como *firewalls, antivírus*, ou até a colocação de senha contra o livre

[55] **BITENCOURT, Cezar Roberto**. Invasão de dispositivo informático. Disponível em**:** **<**http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico>.

acesso a certos dados. Estes programas dificultam o acesso externo às informações contidas nos dispositivos protegidos.

III) CRÍTICA

Ao optar por utilizar o elemento normativo da ilicitude como componente da adequação típica, entendemos que o legislador fez mal ao limitar com a expressão "mecanismo de segurança". Conforme o entendimento de BITENCOURT[56],

> teria sido mais correto, e suficiente, se a *elementar normativa* tivesse se limitado a locução "mediante violação indevida", por que, assim, abrangeria *qualquer violação não autorizada* dos computadores, ou, como diz o texto legal, a violação de todo e qualquer "dispositivo informático", independentemente de haver ou não *dispositivo de segurança*, independentemente de ter sido violado ou não eventual *mecanismo de segurança* etc.

Exigir que um dispositivo informático contenha um "mecanismo de segurança" para que seja penalmente protegido uma situação estranha, como CABETTE[57] exemplificou:

> É como se o legislador considerasse não haver violação de domicílio se alguém invadisse uma casa que estivesse com as portas abertas e ali permanecesse sem a autorização do morador e mesmo contra a sua vontade expressa! Não parece justo nem racional presumir que quem não instala proteções em seu computador está permitindo tacitamente uma invasão, assim como deixar a porta ou o portão de casa abertos ou destrancados não significa de modo algum que se pretenda permitir a entrada de qualquer pessoa em sua moradia. A forma vinculada disposta no tipo penal ("mediante violação indevida de mecanismo de segurança") poderia muito bem não ter sido utilizada pelo legislador que somente deveria chamar a atenção para a invasão ou instalação desautorizadas e/ou sem justa causa. Isso seria feito simplesmente com a locução "mediante violação indevida" sem necessidade de menção a mecanismos de segurança.

Complementando a crítica, GRECO[58]:

> mesmo sem a existência de senha de acesso, a ninguém é dado invadir computador alheio, a não ser que ocorra a permissão expressa ou tácita de seu proprietário. No entanto, para fins de configuração típica, tendo em vista

---

[56] **Idem.**

[57] **CABETTE, Eduardo Luiz Santos**. Primeiras impressões sobre a Lei nº 12.737/... Disponível em: <http://jus.com.br/revista/texto/23522>.

[58] **GRECO, Rogério.** Comentários sobre o crime... Disponível em: <http://www.rogeriogreco.com.br/?p=2183>

> a exigência contida no tipo penal em análise, somente haverá a infração penal se houver, por parte do agente invasor, uma violação indevida do mecanismo de segurança.

Diante da vasta crítica doutrinária, entendemos que seria melhor alterar esta expressão “mediante violação indevida de mecanismo de segurança” pela simples expressão “sem autorização”, suprimindo a incerteza gerada pela expressão “violação de mecanismo de segurança”. O fato de o agente invadir um dispositivo informático já é lesivo à privacidade por si só.

d) 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

O final do caput do artigo 154-A exige ainda que a invasão seja cometida com ao menos um destes fins especiais de agir:

I) FIM DE OBTER, ADULTERAR OU DESTRUIR DADOS OU INFORMAÇÕES SEM AUTORIZAÇÃO EXPRESSA OU TÁCITA DO TITULAR DO DISPOSITIVO OU;

Quando o agente pratica a invasão, ele visa obter (adquirir, copiar para si, tomar do titular), adulterar (modificar o conteúdo, no todo ou em parte), ou destruir (excluir, fazer desaparecer) dados ou informações. São formas de exaurimento do crime, visto que a conduta se consuma com a invasão. É válido lembrar que “dados” são a representação eletrônica das informações. Desta forma o legislador não precisaria utilizar a expressão “ou informações” no caput do artigo.

Estes efeitos no dolo específico do agente somente seriam incriminados sem a autorização do titular das informações protegidas. GRECO[59] conclui que “havendo essa autorização, o fato praticado será considerado atípico. Aqui, como se percebe, o consentimento do ofendido é considerado como uma causa legal de exclusão da tipicidade”.

---

[59] **GRECO, Rogério.** Comentários sobre o crime... Disponível em: <http://www.rogeriogreco.com.br/?p=2183>

Mais uma vez o legislador utiliza expressões desnecessárias: poderia sem prejuízo suprimir do texto legal a parte “expressa ou tácita”. O texto da lei poderia ser escrito de forma mais enxuta, sem prejuízo hermenêutico, da seguinte forma: “e com o fim de obter, adulterar ou destruir dados sem autorização do titular do dispositivo”.

II) [FIM DE] INSTALAR VULNERABILIDADES PARA OBTER VANTAGEM ILÍCITA.

O legislador elege outra finalidade que o agente pode ter ao invadir dispositivo informático alheio: a instalação de vulnerabilidades. Na doutrina[60], alguns autores entendem que este trecho do tipo penal refere-se a outra conduta típica, com verbo nuclear “instalar”. Discordamos deste entendimento e a justificativa[61] do PL 2793/2011 ratifica nossa posição:

> (...) estabelece a necessidade de intenção específica de “instalar vulnerabilidades, obter vantagem ilícita ou obter ou destruir dados ou informações não autorizados” - ou seja, pune-se apenas quando a conduta do agente estiver relacionada a determinado resultado danoso ou quando o objetivo do agente for efetivamente censurável (...)

GRECO[62] nos apresenta um conceito técnico de “vulnerabilidade” no âmbito da informática:

> Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil [CERT.BR]:
>
> Uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.
>
> Um ataque de exploração de vulnerabilidades ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.

---

[60] **CABETTE, Eduardo Luiz Santos**. Primeiras impressões sobre a Lei nº 12.737/... Disponível em: <http://jus.com.br/revista/texto/23522> e **MAGGIO, Vicente de Paula Rodrigues.** Novo crime: Invasão... Disponível em:<http://atualidadesdodireito.com.br/vicentemaggio/2012/12/16/invasao-de-dispositivo-informatico-cp-art-154-a>.

[61] **TEIXEIRA, Paulo e outros**. Projeto de Lei 2793/2011. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>.

[62] **GRECO, Rogério.** Comentários sobre o crime... Disponível em: <http://www.rogeriogreco.com.br/?p=2183>.

No caso do crime estudado, a invasão objetiva a instalação destas vulnerabilidades. O agente deve, primeiramente, invadir o dispositivo informático alheio. A instalação da vulnerabilidade é posterior à invasão. Isto é feito através da escrita ou mesmo da adulteração de dados no sistema, o que poderia estar caracterizado na primeira finalidade exigida pelo legislador. Quando os dados inscritos tem função destrutiva ou ainda exploram ou geram falhas em um sistema, são chamados de códigos maliciosos.

O CERT.BR[63] elaborou uma cartilha de orientação aos usuários da internet, explicando o que seriam os chamados códigos maliciosos:

> Códigos maliciosos (malware) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário.
>
> Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Além disto, os códigos maliciosos são muitas vezes usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de spam.

Esses códigos são amplamente conhecidos por outros nomes, tais como vírus, cavalos de tróia, keyloggers, spywares, dentre muitas outras espécies[64].

2.5.2) Crimes equiparados ao de invasão

§ 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.

O legislador contemplou a criação de outro crime, com pena equiparada à da invasão simples. É crime de ação múltipla que pune quem fornece instrumentos para a prática da invasão simples. Conforme esclarece BITENCOURT[65],

---

[63] O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira.

[64] Recomendamos a leitura da cartilha para informações sobre estas espécies.

[65] **BITENCOURT, Cezar Roberto**. Invasão de dispositivo informático. Disponível em**:** **<**http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico>.

> o autor dessas condutas *não é autor direto da invasão de dispositivo informático*, mas um "colaborador" *sui generis*, isto é, expressamente previsto em lei como tal, independentemente de ser alcançado pelo concurso de pessoas, como, normalmente ocorreria, pois pratica condutas declaradamente acessórias, para permitir a execução da invasão. Logicamente, a tipicidade de sua conduta não é abrangida pela norma secundária de ampliação constante do art 29 do CP, mas decorre do próprio texto legal (154-A § 1º).

É formado cinco verbos nucleares: "produz, oferece, distribui, vende ou difunde". De suma importância considerar que, caso o agente pratique mais de uma destas condutas, no mesmo contexto fático, caracteriza-se o cometimento de um único crime, não existindo concurso entre estas condutas.

Apresenta também outro fim especial de agir - "com o intuito de permitir a prática da conduta definida no caput" – caracterizando outro crime formal, que se consuma com a produção, o oferecimento, a venda ou difusão, sendo mero exaurimento eventual invasão simples realizada com estes instrumentos.

2.5.3) Figuras Qualificadas

As figuras qualificadas explicitam maior desvalor ao crime de invasão informática visto que resultam, no caso, lesões de efeitos permanentes. Ocorre crime qualificado quando a conduta do caput produzir algum dentre os resultados do parágrafo terceiro. O legislador entendeu que merecem um grau maior de reprovabilidade quatro resultados da conduta:

SE DA INVASÃO RESULTAR:

a) A OBTENÇÃO DE CONTEÚDO DE COMUNICAÇÕES ELETRÔNICAS PRIVADAS,

Novamente uma expressão polissêmica: afinal, a que conteúdo ou a que comunicações eletrônicas este dispositivo legal se refere? Entendemos que se refere a qualquer espécie de comunicação entre pessoas, distintas de segredos comerciais, e informações sigilosas que vieram expressos no bojo deste mesmo parágrafo.

O legislador novamente foi infeliz na elaboração da lei: definiu como pena do artigo 154-A, §3º reclusão de 6 meses a 2 anos, **se a conduta não constitui crime mais grave**. Ocorre que o artigo 10º da Lei 9.296/1996 diz que "constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática", sendo aplicável pena de 2 a 4 anos de reclusão. Esta conduta é crime desde 1996 em nosso ordenamento, punido de forma mais grave. Logo não poderemos aplicar a qualificadora do parágrafo. Não há que se falar em revogação parcial do artigo 10º da lei 9.296/1996 por considerarmos que se trata de lei mais específica sobre interceptação de comunicação.

b) [A OBTENÇÃO DE] SEGREDOS COMERCIAIS OU INDUSTRIAIS,

Segredos comerciais ou industriais estão associados ao conteúdo da Lei 9.279/1996 a qual trata da propriedade industrial. Esta lei trata de assuntos variados, como marcas, patentes, desenho industrial. Mas o ponto de maior interesse e conexão com o artigo 154-A do Código Penal refere-se ao artigo 195 da referida lei:

> Art. 195. Comete crime de concorrência desleal quem:
>
> XI - divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;
>
> XII - divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o inciso anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude;
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa

Pela leitura destes incisos, seriam segredos comerciais ou industriais quaisquer informações relacionadas à atividade industrial desde que não sejam de conhecimento público. O legislador pretendeu desvalorar a espionagem industrial feita através de dispositivos informáticos. Assim, se o agente obtém informações industriais, responderá pelo crime do artigo 154-A, § 3º do Código Penal. Como veremos à frente[66], se depois de obter tais dados o agente divulgar, comercializar ou transmitir estes dados a terceiros, terá seu crime majorado de um a dois terços. Desta forma, entendemos que o artigo 195, XI e XII da Lei 9.279/1996 foi

[66] Tópico 3.5.4 'B' desta monografia.

parcialmente revogado em relação à divulgação de dados industriais obtidos ilicitamente.

c) [A OBTENÇÃO DE] INFORMAÇÕES SIGILOSAS, ASSIM DEFINIDAS EM LEI,

Outra expressão aberta, chamada doutrinariamente de norma penal em branco homogênea, exigindo que sua interpretação seja complementada por lei diversa que defina o que são informações sigilosas. Atualmente, a Lei 12.527/2011 define o que são informações sigilosas:

> Art. 4º Para os efeitos desta Lei, considera-se:
>
> I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
>
> III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

Desta forma, caso o invasor obtenha informações temporariamente restritas por conta da segurança social ou do Estado, incidirá nesta qualificadora. Veja bem: a lei 12.527/11 define o que são consideradas informações sigilosas[67], e também limitando quais informações poderão ser classificadas como sigilosas, atendendo à remissão feita no parágrafo 3º do artigo 154-A. Logo, não se pode dizer que não existe lei definindo o que são tais informações.

d) OU O CONTROLE REMOTO NÃO AUTORIZADO DO DISPOSITIVO INVADIDO

Quando o agente tem acesso ao dispositivo informático alheio, ele poderá obter, adulterar, apagar ou inserir dados no dispositivo invadido. Para que a invasão se torne qualificada, o agente passa a ter controle total sobre os processos do dispositivo invadido, atuando como se fosse seu proprietário. O controle remoto se

[67] Ver o Capítulo IV, Seção II da lei 12.527/2011, em especial o artigo 23, para algumas hipóteses de informações que podem ser sigilosas.

dá quando o criminoso atua à distância, através de rede informática, como definimos anteriormente. Conforme BITENCOURT, “o maior desvalor desta conduta reside na permanência dos efeitos nocivos da conduta do agente, que mantém sob o seu controle as ações da vítima, observando, controlando e lesando, à distância, os bens jurídicos tutelados desta” [68].

Não apenas pela permanente lesão à privacidade do ofendido, tal conduta é ainda mais reprovável pelas possibilidades dadas ao invasor. O invasor poderá atuar como se o ofendido fosse, atuando fraudulentamente em nome alheio, o que pode gerar problemas mais graves do que a simples lesão à privacidade, visto que o ofendido desconhece sobre o controle externo de seu dispositivo informático.

2.5.4) Causas de aumento de pena

Neste tópico trataremos das causas de aumento de pena previstas no artigo 154-A.

A) Majorante aplicável à invasão simples e crimes equiparados (154-A §2º)

“§ 2º - Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico”

Esta causa de aumento somente é aplicável ao caput e ao parágrafo 1º porque as formas qualificadas de invasão (parágrafo 3º) possuem suas próprias majorantes (parágrafos 4º e 5º) como veremos a seguir. Trata-se de tratamento mais severo dado às condutas delituosas quando estas resultarem prejuízos econômicos à vítima. São os casos onde, além da lesão à privacidade, a vítima tem seu patrimônio de valor econômico lesado. Trata-se da hipótese em que o bem jurídico atingido é o patrimônio do indivíduo.

[68] **BITENCOURT, Cezar Roberto**. Invasão de dispositivo informático. Disponível em**:** **<**http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico>.

Interessante relatar a observação feita por CAVALCANTE[69]:

> se a vítima sofreu prejuízo econômico porque o invasor dela subtraiu valores, não haverá o crime do art. 154-A, com essa causa de aumento do § 2º, mas sim o delito de furto qualificado. Isso porque, conforme explicado acima, o furto é mais específico que o delito de invasão.
>
> Quando então seria o caso de aplicar o § 2º?
>
> Nas hipóteses em que da invasão ocasionar prejuízo, desde que não seja um delito mais específico. Ex: incidirá essa causa de aumento se, por conta da invasão, a vítima teve sua máquina danificada, precisando de consertos.

B) Majorantes aplicáveis às formas qualificadas do §3º

Pela posição topográfica destas causas de aumento, entendemos que são aplicáveis apenas às formas qualificadas de crime. Vejamos:

"§ 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"

Trata-se de agravamento causado por resultados mais lesivos, tal qual ocorre com as hipóteses qualificadoras. São também descrições de exaurimento do crime de invasão qualificado, entendidas pelo poder legislativo como ainda mais reprováveis do que as condutas qualificadas.

Percebemos que o parágrafo 4º, de forma geral, aumenta a pena em razão da publicidade dada às informações obtidas, visando reprovar ainda mais a lesão ao direito à privacidade.

Por "divulgação" entendemos a apresentação a público, sendo este restrito ou indefinido (como é o caso de disponibilizar em um site na internet), dos dados obtidos ilicitamente da vítima. Quanto maior a repercussão da divulgação, maior a lesão ao bem jurídico, e maior o desvalor da ação. [70]

---

[69] **CAVALCANTE, Márcio André Lopes**. Primeiros comentários à Lei ... Disponível em: <http://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html>

[70] Este seria o crime praticado pelo agente que divulgou fotos da famosa atriz que já referimos

Quanto às expressões “comercialização” e “transmissão a terceiro, a qualquer título”, entendemos que possuem o mesmo sentido: criminalizar a transmissão dos dados a outrem, seja a título oneroso, seja a título gratuito.

Aqui reside outro exagero do legislador, que utiliza-se de palavras desnecessárias. Sem prejuízos, a expressão “comercialização” pode ser suprimida do texto legal, visto estar abarcada pela “transmissão a terceiro, a qualquer título”.

Caso o agente pratique o art. 154-A, §§ 3º e 4º o delito deixa de ser de competência do Juizado Especial Criminal, considerando que, aplicada a causa de aumento sobre a reprimenda prevista no § 3º o crime terá pena máxima superior a 2 anos.[71]

§ 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.

O parágrafo quinto cuida de majorante aplicável ao crime de invasão qualificada (artigo 154-A, §3º). Em relação à vítima da invasão, o legislador entendeu que sendo pessoa ocupante de cargos de chefia do poder público, a invasão resultará mais lesiva por poder atingir interesses públicos. Por isso, este crime deve ter maior reprovabilidade, incidindo obrigatoriamente a causa de aumento de pena nos limites de um terço à metade.

Não se entende, porém, o porquê de não se estender esta maior reprovabilidade contra a administração pública como um todo. Entendemos como correta a hipótese majorante em relação aos chefes da administração pública, por serem pessoas públicas. Porém, entendemos que seria possível considerar crime

[71] **CAVALCANTE, Márcio André Lopes**. Primeiros comentários à Lei ... Disponível em: <http://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html>

qualificado a invasão de dispositivo informático feita contra a administração pública, dado à gravidade que a conduta pode gerar.

Cabe ressaltar que o artigo 313-B de nosso Código Penal considera crime funcional a alteração de dados informáticos da Administração Pública, não discernindo o cargo público das vítimas. Por que, então, o particular não deve ser punido da mesma forma, ou seja, atuando contra a Administração Pública em geral, visto que sua conduta é mais lesiva pelo simples fato de que ele empreende maior esforço para invadir sistemas informáticos públicos do que o próprio funcionário, que por sua posição, já teria maior facilidade para tal empreendimento?

3. Conclusões

Diante de tantas críticas e definições podemos concluir que era necessária a criminalização de algumas condutas da categoria dos crimes próprios de informática, em respeito à legalidade estrita e a função garantidora do tipo penal.

Sabemos que a tendência no Direito Penal é a de criminalizar apenas as condutas que não podem ser devidamente tratadas na esfera civil, e que o ideal é que existam poucos tipos penais incriminadores. Ocorre que, no estado atual desta ciência, não vislumbramos estes reflexos totais do garantismo, mas ao contrário, uma vasta expansão penal. Por que então sugerir a criação de um novo tipo penal? Para chegarmos ao estágio do absoluto garantismo penal, devemos, transitoriamente, adequar nossa principiologia e aplicar, dentro do possível, o máximo de seus postulados. A lei já foi criada e está vigente em nosso ordenamento; Cabe a nós, operadores do direito, interpretá-la e estuda-la de acordo com o ideal que perseguimos.

Entendemos que as novas condutas incriminadas pelo artigo 154-A do Código Penal atentam contra privacidade e tem como objeto material a informática. O legislador, desta forma, “condensou” em um tipo penal a diretriz dada pela “Convenção de Budapeste” sobre criminalidade informática. Ocorre, porém, que o legislador fez isto de forma atécnica, utilizando expressões dúbias na redação do artigo, o que entendemos ser uma grave violação ao princípio da legalidade estrita.

Da forma como está redigido, o tipo penal 154-A não respeita o princípio da estrita legalidade, o que o torna, em tese, inaplicável. Dentre os pontos críticos, destacamos:

I) Não deveria, por exemplo, ter utilizado o verbo “invadir”, quando poderia utilizar termo mais adequado como “acessar”, termo consagrado na doutrina europeia e amplamente utilizado na Ciência da Computação;

II) da mesma forma a exigência de “violação indevida de mecanismo de segurança” parece-nos uma grande desatenção, primeiramente por ser uma elementar do tipo que é totalmente dúbia, podendo assumir muitas

concepções, e também pelo fato de que os dispositivos que não possuam alguma forma de proteção restariam desprotegidos por uma lei que criminaliza justamente a privacidade dos indivíduos;

III) Criar excessivas qualificadoras e causas de aumento de pena, utilizando expressões demasiadamente amplas, como “informações sigilosas”, “controle remoto não autorizado” complicam a interpretação da lei aplicável, visto que nos remete a muitas leis penais extravagantes de conteúdo relacionado, o que gera incerteza para sua aplicação;

IV) A maior proteção dada exclusivamente aos chefes dos poderes públicos, enquanto que uma invasão contra a administração pública é punida da mesma forma que a invasão ao dispositivo de um particular parece-nos também falta de atenção ao legislar.

Nossa sugestão para uma nova redação deste tipo penal seria:

“Acesso não autorizado

Art. 154-A Acessar, sem autorização, dispositivo informático alheio.

Pena -

§ 1º Para efeitos deste crime, considera-se dispositivo informático aparelhos eletrônicos que contenham dados pessoais.

§ 2º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde programas ou instruções de computador com o intuito de permitir a o acesso não autorizado.

§ 3º Se o acesso resulta prejuízo econômico ao ofendido ou é contra a Administração Pública:

Pena -

§ 4º Na hipótese do § 2º, aumenta-se a pena de um a dois terços se houver divulgação ou transmissão a terceiros, a qualquer título, das informações obtidas.“

Sugerimos, a adoção de um crime material através do verbo “acessar”, o que exige a verdadeira lesão ao bem jurídico privacidade para sua consumação, abrangendo o mesmo escopo do vigente 154-A, de forma mais clara e técnica. Da mesma forma, mantivemos os crimes equiparados e a qualificadora pelo prejuízo econômico. Acrescentamos, porém, a qualificadora à hipótese de invasão contra a Administração Pública. Mantivemos também a majorante por conta da divulgação ou transmissão de dados a terceiros, por entender que tais condutas violam de maneira acentuada a privacidade do ofendido.

Não nos manifestamos em relação às penas correspondentes por não ser o escopo deste trabalho. Porém cremos que as penas privativas de liberdade não são as mais adequadas ao caso. Infratores com tal conhecimento técnico poderiam prestar penas restritivas de direito, e até mesmo, compartilhar suas habilidades na informática em prol do desenvolvimento dos sistemas públicos e da educação.

Revisado o artigo 154-A concluímos este trabalho, gratos pela iniciativa do Poder Legislativo em atuar nesta nova área de interesse do Direito, a Informática.

4. Referências bibliográficas

BITENCOURT, Cezar Roberto. Invasão de dispositivo informático. Atualidades do Direito, 7 fev. 2013. Disponível em**: <** http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico/>. Acesso em: 13 mai. 2013.

_____. Tratado de direito penal: parte especial vol. 3 – 7. Ed. São Paulo. Saraiva, 2011

_____. Tratado de direito penal: parte geral – 15. Ed. Rev., atual. e ampliada. São Paulo. Saraiva, 2010

CABETTE, Eduardo Luiz Santos. Primeiras impressões sobre a Lei nº 12.737/12 e o crime de invasão de dispositivo informático. Jus Navigandi, Teresina, ano 18, n. 3493, 23 jan. 2013. Disponível em: <http://jus.com.br/revista/texto/23522>. Acesso em: 13 mai. 2013.

CAVALCANTE, Márcio André Lopes. Primeiros comentários à Lei n.° 12.737/2012, que tipifica a invasão de dispositivo informático. Disponível em: <http://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html> Acesso em: 07/01/13.

Cartilha de Segurança para Internet, versão 4.0 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: http://cartilha.cert.br/cc/. Acesso em: 30 jun. 2013.

COLARES, Rodrigo Guimarães. Cybercrimes: os crimes na era da informática. Jus Navigandi, Teresina, ano 6, n. 59, out 2002. Disponível em: <http://jus.com.br/artigos/3271/cybercrimes-os-crimes-na-era-da-informatica>. Acesso em: 2 jun. 2008.

CRESPO, Marcelo Xavier de Freitas. Crimes digitais. São Paulo. Saraiva, 2011.

FERRAJOLI, Luigi. Direito e razão: teoria do garantismo penal. São Paulo: Editora Revista dos Tribunais, 2002.

LUIZ FLÁVIO GOMES. Lei "Carolina Dickman" e sua (in)eficácia. LFG Conteúdo Jurídico: Direito criminal. 07 mar. 2013. Disponível em:< http://www.lfg.com.br/conteudos/artigos/direito-criminal/artigo-prof-luiz-flavio-gomes-lei-carolina-dickman-e-sua-in-eficacia>. Acesso em: 13 mai. 2013.

GOMES, Ricardo Reis. Crimes Puros de Informática. Monografia – Centro Universitário de Brasília, Brasília, 2001.

GRECO, Rogério. Comentários sobre o crime de Invasão de dispositivo informático – Art. 154-A do Código Penal. 2013. Disponível em: <http://www.rogeriogreco.com.br/?p=2183>. Acesso em: 13 mai. 2013.

_____. Curso de Direito Penal - Parte Geral – Vol. I – 11ª ed. Rio de Janeiro: Impetus, 2009.

_____***.*** *Curso de Direito Penal - Parte Especial - Vol. II - 10ª Ed. Rio de Janeiro: Impetus, 2013.*

MAGGIO, Vicente de Paula Rodrigues. Novo crime: Invasão de dispositivo informático – CP, art. 154-A**.** Atualidades do Direito, 7 abr. 2013. Disponível em: <http://atualidadesdodireito.com.br/vicentemaggio/2012/12/16/invasao-de-dispositivo-informatico-cp-art-154-a/>. Acesso em: 11 abr. 2013.

MATOS, Eneas de Oliveira. Direitos da personalidade e pessoa jurídica. Jus Navigandi, Teresina, ano 10, n. 797, 8 set. 2005 . Disponível em: <http://jus.com.br/revista/texto/7247>. Acesso em: 20 mai. 2013.

Michaelis Moderno Dicionário da Língua Portuguesa. Editora Melhoramentos. 2009. Disponível em: <http://michaelis.uol.com.br/moderno/portugues/>

MIRANDA, Marcelo Baeta Neves. Abordagem dinâmica aos crimes via internet. Jus Navigandi, Teresina, ano 4, n. 37, dez. 1999. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1828>,. Acesso em: 24 abr. 2008.

NUCCI, Guilherme de Souza. Código Penal Comentado. 13ª Ed. Editora RT, 2013

PIAUHYLINO, Luiz. Comissão de Constituição e Justiça e de redação: Projeto de Lei nº 84, de 1999. Disponível em: <http://www.camara.gov.br/sileg/integras/1774.pdf>. Acesso em 24 abr. 2008.

PRADO, Luiz Regis. Bem Jurídico-penal e constituição. 3ª ed. Ver., atual e ampl. – São Paulo. RT, 2003.

SILVA, Leandro Oliveira. Teoria da Tipicidade. Em Direito Penal Acadêmico – Parte Geral / Rafael de Castro Alves Medina (Org.) 1ª ed., pág. 379 e ss. – Rio de Janeiro. 2008.

SILVA SÁNCHEZ, Jesús-María. A expansão do direito penal: aspectos da política criminal nas sociedades pós-industriais. Tradução da 2ª ed. Espanhola: Luiz Otávio de Oliveira Rocha. São Paulo. RT, 2002. (Série as ciências criminais no século 21: v. 11)

TAVARES, Juarez. Teoria do Injusto Penal. 3. Ed. Rev. E ampl. – Belo Horizonte: Del Rey, 2003.

TEIXEIRA, Paulo e outros. Projeto de Lei 2793/2011. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>. Acesso em: 04 fev. 2013.

VARGAS, José Cirilo de. Introdução ao estudo dos crimes em espécie. Belo Horizonte: Del Rey, 1993.

VIANNA, Túlio Lima. Fundamentos de direito penal informático: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003

WENDT, Emerson. Crimes cibernéticos: ameaças e procedimentos de investigação. Rio de Janeiro. Brasport, 2012.

ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. Manual de Direito Penal brasileiro: parte geral. São Paulo. RT, 1997.