INVASÃO DE DISPOSITIVO INFORMÁTICO: APORTE COM A LEGISLAÇÃO ESPANHOLA

INVASION OF COMPUTING DEVICE: CONTRIBUTION TO THE SPANISH LAW

Bruna de Oliveira da Silva Guesso Scarmanhã *
Mário Furlaneto Neto **
José Eduardo Lourenço dos Santos ***

Data de recebimento: 31/03/2014
Data da aprovação: 25/05/2014

RESUMO

A disseminação da rede mundial de computadores e a utilização de ferramentas que possibilitam a manipulação de dados fazem com que o direito à intimidade do cidadão fique cada vez mais exposto, exigindo que o Direito se encarregue de tutelá-la. Com a criminalização da invasão de dispositivo informático, buscou-se proteger a liberdade individual, nos aspetos pertinentes à intimidade, privacidade e vida privada. Assim, por meio de uma revisão bibliográfica e legislativa, procurou-se enfrentar os conceitos de liberdade, intimidade, privacidade e vida privada como alicerce e referencial teórico para discutir a estrutura do crime de invasão de dispositivo informático. A análise comparativa do delito em tela com a legislação espanhola possibilitou concluir que o legislador brasileiro se preocupou com a tutela das informações

* Graduanda em Direito pelo Centro Universitário Eurípides de Marília – UNIVEM. Bolsista Santander do Programa Ibero-Americanas. Membro do NEPI – Núcleo de Estudos em Direito e Internet. E-mail: <bruna.guesso@gmail.com>

** Delegado de Polícia e docente da Graduação e do Programa de Mestrado em Direito do Centro Universitário Eurípides de Marília – UNIVEM. Doutor em Ciência da Informação pela UNESP. Coordenador do NEPI – Núcleo de Estudos em Direito e Internet. E-mail: <mariofur@univem.edu.br>

*** Delegado de Polícia e docente da graduação em Direito do Centro Universitário Eurípides de Marília – UNIVEM. Vice-coordenador do NEPI – Núcleo de Estudos em Direito e Internet. E-mail: <jels@univem.edu.br>

estanques no dispositivo informático e que ações como o *man in the middle, cookies* e *sniffers*, que permitem acesso à informação durante o tráfego na rede mundial de computadores, podem se amoldar ao crime previsto no artigo 10 da Lei Federal nº 9.296/1996.

PALAVRAS-CHAVE
Crime informático; invasão; intimidade; privacidade.

ABSTRACT
The spread of the world wide web and using tools that allow the manipulation of data mean that the right to privacy of the citizen becomes increasingly exposed, demanding that the law is entrusted ourselves to safeguarding it. With the criminalization of invasion computing device aimed to protect individual liberty, the relevant aspects to intimacy, privacy and private life. Thus, through a literature review and legislative, sought to address the concepts of freedom, intimacy, privacy and private life as a foundation and theoretical framework to discuss the structure of the crime of invasion of computing device. The comparative analysis of the offense on the screen with Spanish law allowed the conclusion that Brazilian legislators worried about the protection of information in watertight computing device and that actions such as the man in the middle, cookies and sniffers that allow access to information during the traffic the world wide web, can adapt themselves to the crime under Article 10 of Federal Law No. 9.296/1996.

KEYWORDS
Computer crime, invasion, privacy, privacy.

INTRODUÇÃO

Mediante a criminalização da invasão de dispositivo informático buscou-se tutelar a liberdade individual, no que tange ao direito das pessoas manterem alguns aspectos de sua vida em sigilo, *in casu*, o sigilo dentro do contexto das comunicações informáticas.

O legislador infraconstitucional limitou-se a tutelar as informações armazenadas em dispositivos informáticos, ou seja, informações estanques, em um tipo penal que se assemelha ao disposto no artigo 4º da Convenção de Budapeste (Convenção de Cibercrimes, firmada na Hungria, em 2001, e em vigor no Conselho da Europa desde 2004), que sugere a criminalização da interferência de dados intencional e ilegítima, com a finalidade de danificar, apagar, deteriorar, alterar ou eliminar dados informáticos.

Porém, a análise do novo tipo penal impõe a necessidade de enfrentar algumas questões: o crime de invasão de dispositivo informático tutela a hipótese em que o acesso indevido às informações se opera durante o tráfico na rede mundial de computadores como, por exemplo, no golpe *man in the middle*[1] ou por meio da utilização de *cookies*[2] *e sniffers*[3]? Os sistemas de *cloud computer* se inserem no conceito de dispositivo informático? O excesso quanto à autorização para acesso ao dispositivo informático permite amoldar a conduta do agente à norma penal incriminadora?

Pretende-se buscar soluções aos questionamentos levantados, por meio de uma revisão bibliográfica e legislativa. Para tanto, analisar-se-á, inicialmente, os conceitos de liberdade, privacidade, intimidade e vida privada, como alicerce e referencial teórico para enfrentar a estrutura do crime de invasão de dispositivo informático, em comparação com o direito penal espanhol. Posteriormente, far-se-á uma análise crítica do artigo 154-A do CP.

---

[1] O homem do meio consiste na conduta de o agente, estando em um nó da rede, mandar comandos ao equipamento que está postulando uma requisição, permitindo identificar-se como o destinatário, tendo, assim, o acesso indevido à informação durante o seu tráfego na rede, sem a necessidade de invadir o dispositivo informático.

[2] Também denominado de testemunho da conexão, permite troca de dados entre o navegador e o servidor de dados, o que possibilita que o webmaster de um site possa obter informações sobre as preferências de acesso de um usuário.

[3] Permite interceptar e registrar o tráfico de uma rede de computadores.

1 O DIREITO À LIBERDADE E AS VERTENTES DOS DIREITOS À INTIMIDADE, PRIVACIDADE E VIDA PRIVADA

Em análise às dimensões dos direitos humanos, Wolkmer[4] aponta os "novos direitos advindos das tecnologias de informação (*Internet*), do ciberespaço e da realidade virtual em geral" enquanto direitos de quinta dimensão. Vale lembrar que a classificação em cinco dimensões é uma tendência da doutrina brasileira, apesar de não haver consenso a respeito, inclusive quanto aos temas das dimensões, em especial a partir da terceira. Pérez Luño[5], por sua vez, expõe a tendência da doutrina espanhola, tratando os novos direitos sob a ótica da terceira dimensão. Em comum, os autores abordam o viés do direito à liberdade e seus reflexos em relação aos direitos à privacidade, intimidade e vida privada.

Montesquieu *apud* SILVA[6] conceitua liberdade como "o direito de fazer tudo o que as leis permitem", porém Silva[7] adverte que este conceito traz um risco, pois deve levar em conta, para fins de validade, leis consentidas pelo povo. Mais aceitável, para o referido autor (Silva)[8], é o conceito trazido pela Declaração de 1789, condicionando o direito à liberdade aos limites que tangenciam os direitos dos demais membros da sociedade, os quais, por sua vez, têm direito ao gozo dos mesmos direitos; e enfatiza: somente a lei pode estabelecer tais limites, ou seja, senão aqueles que sejam nocivos à sociedade.

No meio ambiente *Internet*, o conceito de liberdade está correlacionado diretamente ao direito à livre manifestação do pensamento, ou seja, de autodeterminar-se de acordo com o seu pensamento. Porém, não se pode confundir liberdade de expressão com liberalidade, motivo pelo qual se impõem limites no agir do cidadão, a fim de viabilizar uma sociedade sadia.

O direito positivo, assim, se concentra em disciplinar apenas a liberdade objetiva, ou seja, assegurar ao homem o direito de agir livre de coações, sem ferir

---

[4] WOLKMER, Antonio Carlos. **Introdução aos fundamentos de uma teoria geral dos "novos" direitos.** In: WOLKMER, Antonio Carlos; LEITE, José Rubens Morato (org.). Os "novos" direitos no Brasil: natureza e perspectivas. São Paulo: Saraiva, 2003, p. 15.

[5] PÉREZ LUÑO, Antonio-Enrique. **La tercera generación de Derechos Humanos**. Navarra: Arazandi, 2006. 319p.

[6] Montesquieu (1956) *apud* SILVA, José Afonso da. **Curso de Direito Constitucional positivo**. ed. 34. São Paulo: Malheiros, 2011, p. 233.

[7] SILVA, José Afonso da. **Curso de Direito Constitucional positivo**. ed. 34. São Paulo: Malheiros, 2011.

8 *Ibidem*.

direitos e garantias fundamentais de outro ente social.

Dentro deste contexto, o preceito amplo de liberdade engloba outros direitos fundamentais como a privacidade, a intimidade e a vida privada, compondo, assim, uma linha de limites passíveis de manipulação.

Parte-se do pressuposto de que o indivíduo tem o direito de manter aspectos de sua vida em sigilo, seja no âmbito familiar, profissional, tanto quanto em face do vínculo social (elementos constitutivos da vida privada). Logo, busca-se assegurar que a informação de caráter íntima ou privada de cada pessoa não seja manipulada sem o seu consentimento, o que pode violar a tutela à liberdade.

O já mencionado Silva[9] pontua a privacidade enquanto gênero, dos quais são espécies a intimidade, a vida privada, o direito à honra, à imagem das pessoas, etc. Dessa forma,vale-se do pressuposto de que a privacidade constitui um conjunto mais amplo que a intimidade, pois todo íntimo é privado, mas nem todo o privado é íntimo, a ponto de agrupar no direito à privacidade (desígnio de direito da vida privada) o direito à intimidade (âmbito exclusivo que alguém reserva para si).

Por sua vez, Dotti[10] conceitua a intimidade como "a esfera secreta da vida do indivíduo na qual este tem o poder legal de evitar os demais", ou seja, evitar levar ao conhecimento de outrem aquilo que é pessoal, íntimo, reservado ou, em outras palavras, "repositório de segredos e particularidades do foro moral e íntimo do indivíduo" [11].

Nessas condições, sob a ótica da vida privada, têm-se aspectos da vida da pessoa voltados para o interior, que "debruça sobre a mesma pessoa, sobre os membros de sua família, sobre seus amigos" [12] e que buscam tutelar atentados contra os segredos da vida privada e à liberdade da vida privada, sem perturbações de *outréns*.

Tal questão ganha ainda maior amplitude quanto se aborda a temática sob o viés do meio ambiente *Internet*. Para Andrade[13]:

> Alçada ao núcleo de direitos basilares para o exercício pleno das liberdades individuais, a proteção à intimidade e à vida privada encontra-se amparada nas cartas

9 *Ibidem*.

10 DOTTI, René Ariel. **Proteção da vida privada e liberdade de informação**. São Paulo: RT, 1980, p.69.
11 *Ibidem*, p.208.

12 *Ibidem*, p.208.

13 ANDRADE. Allan Diego Mendes. **O direito à intimidade e à vida privada em face das novas tecnologias da informação**. [2013?]. Disponível em: <http://www.faete.edu.br/revista/odireito aintimidade20a_vida_privada_em_facedasnovastecnologiasdainformacao-all20diego.pdf>. Acesso em: 21 ago 2013.

> constitucionais dos países que assentam a ordem jurídica em um estado democrático de direito. No que tange ao ordenamento jurídico brasileiro, verifica-se que tal direito encontra-se assegurado pela Constituição Federal de 1988, em seu art. 5º, X.

No mesmo sentido, ao abordar o fator privacidade e informática, Silva[14] salienta que a informática, nomeadamente diante da difusão de arquivos de dados e a possibilidade de interconexão entre os arquivos, põe em cheque a individualidade do cidadão, amparada pelo art. 5º, X, da CF, ressaltando o *Habeas data*, enquanto remédio constitucional para o cidadão postular a correção quanto às inadequações de seus dados pessoais, sem se esquecer da eventual indenização por danos morais e materiais, bem como a criminalização de algumas condutas, como, por exemplo, os crimes contra a honra.

Na Espanha, os direitos compreendidos no entorno da liberdade informática compreendem um núcleo de faculdades em que o indivíduo tem o direito de decidir a quem, como e em quais circunstâncias seus dados e suas informações privadas e íntimas podem ser acessados. Trata-se, portanto, de priorizar a autotutela, deixando ao Direito a missão de disciplinar situações mais extremas.

Por outro lado, sob a perspectiva dos arquivos de dados pessoais, esse mesmo indivíduo tem o direito de saber sobre a existência de registro de seus dados, bem como conhecer a finalidade do arquivo e ter ciência de como se dá o acesso aos registros. No caso de dados inúteis, não atualizados, incompletos ou falsos, garante-se ao titular a capacidade de pedir o cancelamento ou a exclusão, possibilitando, inclusive, a postulação de indenização se houver danos materiais ou morais.

Considerando-se que os arquivos de dados pessoais hodiernos são eletrônicos, Álvarez B. de Bozo, Ávila Hernández e Peñaranda Quintero[15] dispõem que "A liberdade da Informação, seguindo a doutrina espanhola mais qualificada, é um novo direito fundamental que tem como propósito garantir às pessoas a faculdade para conhecer, acessar e controlar as informações que lhes concerne". Sob esta dimensão, Davara Rodríguez[16] explica que os dados pessoais têm conexão com

---

[14] *Ibidem*.

[15] ÁLVAREZ B. DE BOZO, M.; ÁVILA HERNÁNDERZ, F. M.; PEÑARANDA QUINTERO, H.R. **La libertad Informática: Derecho Fundamental en la Constitución Venezolana**. Revista Internacional de Derecho e Informática, año 2. n.1, jan./dez. 2000. Disponível em: <http://www.omdi.info/espanol/reivdi/ano2_n1/alvarez_2.htm>. Acesso em: 19 ago. 2013. Texto original: La libertad informática, siguiendo la doctrina española más calificada, es un nuevo derecho fundamental que tiene como propósito garantizar la facultad de las personas para conocer, acceder y controlar las informaciones que les conciernen".

[16] DAVARA RODRÍGUEZ, Miguel Ángel. **Manual de Derecho Informático.** Ed. 10. Navarra: Arazandi, 2008, p.55.

a intimidade (unidos ao indivíduo e em seu entorno social) e que a privacidade é a possibilidade de mantê-los em sigilo, resguardados de acesso e intromissões alheias, ressaltando, no entanto, que o surgimento da informática e a rápida transmissão de informações possibilitaram uma fonte potencial de agressividade contra a intimidade da pessoa em diferentes formas.

Ocorre que, no meio ambiente da rede mundial de computadores, a discussão sobre a intimidade, a vida privada e a privacidade não pode ficar restrita aos arquivos de dados pessoais. Assim, levando-se em conta que os computadores pessoais, em cujo contexto se inserem os dispositivos informáticos, interligados ou não à *Internet*, são utilizados como verdadeiros depósitos de informações, necessário se torna que tais informações também sejam objeto de alguma proteção pelo ordenamento jurídico.

Nesse contexto, ao tratar dos problemas e dos riscos jurídicos proporcionados pelas novas tecnologias, Perez Luño[17] assinala que "Sua potencialidade na difusão ilimitada de imagens e informações a faz um veículo especialmente poderoso para perpetrar ataques criminosos sobre os direitos legais básicos: a intimidade [...]" [tradução livre]. Da mesma forma, ressalva Davara Rodríguez[18] que a Constituição Espanhola dedica um capítulo sobre os "Direitos e Liberdades" [tradução livre], "Dos Direitos e Deveres Fundamentais"[19], ao dispor que "a Lei limitará o uso da Informática para garantir a honra e a intimidade pessoal e familiar dos cidadãos e o pleno exercício de seus direitos"[20] [tradução livre]. O autor salienta ademais não ser essa a única referência que a Constituição Espanhola faz ao emprego da informática, pois, mesmo referendando de forma direta e expressa, indica, no art. 105b, que a lei regulará "O acesso dos cidadãos aos arquivos e registros administrativos, salvo no que afete à segurança e defesa do Estado, a investigação dos crimes e a intimidade das pessoas"[21] [tradução livre].

---

[17] *Ibidem*, p.93. Texto original: "Su potencialidad en la difusión ilimitada de imágenes e informaciones la hace un vehículo especialmente poderoso para perpetrar atentados criminales contra bienes jurídicos básicos: la intimidad [...]".

[18] *Ibidem*, p.57. Texto original: Derechos y Libertades.

[19] *Ibidem*, p.57. Texto original: De los Derechos y deberes fundamentales.

[20] *Ibidem*, p.57. Texto original: "La Ley limitará el uso de la Informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

[21] *Ibidem*, p.57. Texto original: "El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas" .

Em 31 de julho de 2002, publicou-se a diretiva sobre a privacidade e as comunicações eletrônicas, dispondo uma harmonização das disposições dos Estados membros para garantir um nível equivalente de proteção "das liberdades e os direitos fundamentais, em especial o direito à intimidade, no que diz respeito ao tratamento de dados pessoais no setor das comunicações eletrônicas"[22] [tradução livre], evidenciando a preocupação espanhola em proteger os direitos fundamentais no meio ambiente *Internet*, promovendo a liberdade, mas dentro dos limites que possibilite respeito à intimidade e à vida privada.

Por ser inerente ao sistema jurídico, o direito à intimidade e à vida privada consagram-se entre os direitos e as liberdades fundamentais a serem assegurados ao indivíduo, impondo-se ao Estado tutelar a privacidade do homem na sociedade digital, ameaçada constantemente pelos novos meios da comunicação e de informação. Na seara infraconstitucional brasileira, esse aspecto foi objeto de disciplina pela criminalização da invasão de dispositivo informático, que será objeto de análise a seguir.

2 ANÁLISE DA ESTRUTURA DO CRIME DE INVASÃO DE DISPOSITIVO INFORMÁTICO

O crime de invasão de dispositivo informático é conceituado pelo artigo 154-A do Código Penal (CP) como o ato de **"**Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita" [23]. Trata-se de crime de menor potencial ofensivo, em que se prevê pena de três meses a um ano e multa em seu tipo penal *simplex* e cuja ação penal é pública condicionada à representação.

Importante destacar o objeto jurídico do crime, pois, no Direito Penal, prevalece, de forma majoritária, o entendimento de que sua função é tutelar bens jurídicos, que são bens relevantes para o homem, cuja importância acaba reconhecida pelo Direito, res-

[22] DAVARA RODRÍGUEZ, Miguel Ángel. **Manual de Derecho Informático.** Ed. 10. Navarra: Arazandi, 2008, p.65. Texto original: "de las libertades y los derechos fundamentales, en particular del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en sector de las comunicaciones electrónicas".

[23] BRASIL. Lei nº. 12.737, de 30 de novembro de 2012. **Ementa:** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 03 dez. 2012. ed. 232. Seção 1. p.1. Disponível em: http://www.in.gov.br/visualiza/index.jsp?jornal=1&pagina=1&data=03/12/2012>. Acesso em: 09 set. 2013.

ponsável, por sua vez, por proteger esses bens por meio de leis. Já o Direito Penal, como um todo, deve realizar uma seleção das condutas consideradas mais graves socialmente, com base nos bens jurídicos, a fim de atuar como uma das formas de controle social:

> [...] ações conflitivas de gravidade e significação social muito diversos se resolvem por via punitiva institucionalizada, mas nem todos que as realizam sofrem essa solução, e sim unicamente uma minoria ínfima deles, depois de um processo de seleção que quase sempre seleciona os mais pobres.[24]

Para Batista[25]:

> [...] a missão do Direito Penal *defende* (a sociedade), *protegendo* (bens, ou valores, ou interesses), *garantindo* (a segurança jurídica, ou a confiabilidade nela) ou *confirmando* (a validade das normas); ser-lhe-á percebido um cunho *propulsor*, e a mais modesta de suas virtualidades estará em *resolver* casos.

O citado autor prossegue, ainda, afirmando que

> podemos, assim, dizer que a missão do Direito Penal é a proteção de bens jurídicos, através da cominação, aplicação e execução da pena. Numa sociedade dividida em classes, o direito penal estará protegendo relações sociais (ou "interesses", ou "estados sociais", ou "valores") escolhidos pela classe dominante, ainda que aparentem certa universalidade, e contribuindo para a reprodução dessas relações. Efeitos sociais não declarados da pena também configuram, nessas sociedades, uma espécie de "missão secreta" do Direito Penal.[26]

Sobre as relações entre o bem jurídico e o Direito Penal, é possível afirmar que

> o bem jurídico não é somente o resumo conceitual de um resultado obtido mediante outras operações (como sugere a conhecida expressão "abreviatura da ideia de fim"), também não quando não se emprega com "ambicioso" fim de limitar constitucionalmente a legislação penal. Ao contrário, desempenha um papel produtivo importante

[24] ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. **Manual de Direito Penal brasileiro**: parte geral. 4. ed. São Paulo: Revista dos Tribunais, 2002, p. 60.

[25] BATISTA, Nilo. **Introdução crítica ao Direito Penal brasileiro**. 8. ed. Rio de Janeiro: Revan, 2002.

[26] *Ibidem*.

> já no nível primário da averiguação da estrutura de delito e, ato seguido (no segundo nível), na determinação do marco de ações compreendidas no tipo como "menoscabadoras do bem jurídico".[27] [tradução livre].

Definindo bens jurídicos, aliás, Muñoz Conde e Garcia Arán[28] afirmam que são "aqueles pressupostos que a pessoa necessita para sua autorrealização e para o desenvolvimento de sua personalidade na vida social" [tradução livre]. Tem-se também importante conceito apresentado por Toledo[29], para quem tais bens "são valores ético-sociais que o direito seleciona, com o objetivo de assegurar a paz social, e coloca sob sua proteção para que não sejam expostos a perigo de ataque ou a lesões efetivas".

Ao proteger a liberdade individual, na sua forma de inviolabilidade da intimidade e da vida privada, buscou-se preservar o direito de cada um ter seu universo pessoal protegido contra invasões e devastações. Por outro lado, ao tutelar a liberdade individual, nos aspectos do direito à intimidade e à privacidade, não se procurou proteger a rede mundial de computadores.

Nesse sentido, Bitencourt[30] salienta que o crime em tela tutela o direito à liberdade individual, dentro do contexto da "privacidade individual, pessoal ou profissional do ofendido", cuja "divulgação possa acarretar dano a outrem". De sua parte, em uma abordagem mais sintetizada, Nucci[31] dimensiona o objeto jurídico como sendo a "intimidade e vida privada". Como o tipo penal está inserido dentro do capítulo "dos crimes contra a liberdade individual", tem-se que este é o bem jurídico

---

[27] SCHÜNEMANN, Bernd. El principio de protección de bienes jurídicos como punto de fuga de los limites constitucionales de los penales y de su interpretación. In: HEFENDEHL, Roland (Ed.). **La teoria del bien jurídico**: ¿fundamento de legitimación del derecho penal o juego de abalorios dogmático? Barcelona: Macial Pons, Ediciones Jurídicas y Sociales, S. A. Madrid, 2007, p. 199. Texto original: "El bien jurídico no es sólo el resumen conceptual de un resultado obtenido mediante otras operaciones (como sugere la conocida expresión 'abreviatura de la idea de fin'), tampoco cuando no se emplea com el 'ambicioso' fin de limitar constitucionalmente la legislación penal. Por el contrario, desepeña un papel productivo importante ya en el nível primário de la averiguación de la estrutura de delito y, acto seguido (en el segundo nível), en la determinación del marco de acciones compreendidas en el tipo como 'menoscabadoreas del bien jurídico'".

[28] MUÑOZ CONDE, Francisco; GARCIA ARÁN, Mercedes. **Derecho penal, parte general**. 7. ed. Valência: Tirant lo blanch, 2007. Texto original: "aquellos presupuestos que la persona necessita para su autorrealización y el desarrollo de su personalidade em la vida social".

[29] TOLEDO, Francisco de Assis. **Princípios básicos de Direito Penal**: de acordo com a Lei n. 7.209, de 11/07/1984 e com a constituição federal de 1988. 5. ed. São Paulo: Saraiva, 2007, p. 16.

[30] BITENCOURT, Cézar Roberto. **Invasão de dispositivo informático**. Disponível em: <http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico/>. Acesso em: 22 ago 2013.

[31] NUCCI, Guilherme de Souza. **Manual de Direito Penal**. ed. 9. São Paulo: RT, 2013, p.742.

tutelado. Ocorre, pois, que uma pessoa só pode exercer a plena liberdade se tiver o direito de manter alguns aspectos de sua vida em segredo, *in casu*, informações armazenadas em dispositivo informático[32].

Evidenciam-se por objeto material os dispositivos informáticos, interligados ou não à rede mundial de computadores, tais como desktop, notebook, netbook, smartphone, ipod, tablet, Iphone, ou seja, dispositivos que contenham capacidade de armazenar o fluxo das comunicações informáticas, seja de uso pessoal, corporativo, comercial ou industrial. Exige-se, da mesma maneira, que seja alheio, portanto, pertencente a outrem e não ao próprio invasor. Dentro do contexto de objeto material, também se inserem os dados e as informações contidas no dispositivo informático invadido.

O verbo que compõe o núcleo do tipo, *invadir,* tem o sentido de violar, acessar, ingressar, sem autorização expressa ou tácita do titular do dispositivo informático. Como bem lembra Bintencourt[33], em regra, o verbo invadir, normalmente, é empregado para descrever tipos penais em que há emprego de força ou hostilidade. Contudo, no caso em discussão, a invasão se opera por meio fraudulento, por meio da violação indevida de sistema de segurança. A invasão deve infringir qualquer meio de proteção, como senha, antivírus e *software* de segurança para haver a perfeita tipificação do crime. Se não estiver presente o elemento normativo do tipo – sem autorização –, a conduta caracteriza um indiferente penal. Bitencourt[34] critica a exigência do elemento normativo do tipo, defendendo que o correto seria tutelar toda e qualquer violação indevida a dispositivo informático, tratando-se, assim, de crime não-transeunte, em que se determinará prova pericial no dispositivo informático do sujeito passivo para fins de comprovação da invasão, mediante violação indevida de mecanismo de segurança ou instalação de vulnerabilidades.

Para que a invasão se amolde à norma penal incriminadora, necessário que o agente haja com a finalidade específica de obter, adulterar ou destruir dados ou informações ou instalar vulnerabilidades para obter vantagem ilícita. Requer-se, pois, a presença de um dos elementos especiais do tipo, sob pena de estarmos diante de um fato atípico.

Importante esclarecer que, no contexto específico, obter tem o sentido de apropriar-se indevidamente; adulterar significa alterar, enquanto destruir implica

[32] BITENCOURT, Cézar Roberto. **Invasão de dispositivo informático**. Disponível em: <http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico/>. Acesso em: 22 ago 2013.

[33] *Ibidem*.

[34] *Ibidem*.

inutilizar dados. Instalar vulnerabilidade tem o sentido de estabelecer brecha que permita a invasão indevida ao dispositivo informático, necessitando-se, no entanto, que o agente vise a obter vantagem ilícita, o que não implica, necessariamente, vantagem econômica.

O parágrafo 1º do artigo em comento traz um delito por equiparação, ao incidir na mesma pena a conduta do agente que produz, oferece, distribuiu, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput*. Segundo Cabette[35], trata-se de um "tipo misto alternativo, ou seja, crime de ação múltipla ou de conteúdo variado, de forma que se a conduta do agente subsumir os dois núcleos em um mesmo contexto, responderá por um único crime". Buscou-se criminalizar toda a cadeia produtiva de dispositivo ou programa de computador que permita a invasão do objeto material do crime.

A exceção se dá em relação à teoria monista adotada no artigo 29 do CP, já que, a título de exemplo, aquele que oferece (fornece a título gratuito) e aquele que difunde (propaga) dispositivo ou programa de computador capaz de viabilizar a invasão deveriam responder como partícipes, já que concorrem, de alguma forma, para a prática da infração e deveriam responder pelas penas a eles comunicada. O legislador infraconstitucional, porém, aplicou ao caso a teoria dualista, em que se prevê um crime para os autores e outro para os partícipes. No entanto, se o agente produzir dispositivo ou programa de computador e utilizá-lo para invadir o objeto material do crime em pauta, responderá somente pelo *caput*.

Outro elemento a ser debatido tangencia a invasão de redes sociais, cujo acesso se dá, em regra, por meio de *login* e senha, hipótese em que também estar-se-ia violando a intimidade e a vida privada do titular da conta. Vislumbra-se que a invasão possa ser realizada em três hipóteses: mediante a invasão do dispositivo informático do titular da conta da rede social com o intuito de capturar o *login* e a senha, viabilizando o acesso; mediante capturados dados ou informações durante o tráfego na rede mundial de computadores; ou por meio da invasão do provedor da rede social, pessoa jurídica que armazena os dados e as informações dos clientes, dotado, inclusive, de outros dispositivos de segurança muito mais eficazes que o sistema de *login* e senha.

Vale frisar que o sistema *login* e senha caracterizam mecanismo de proteção, a ponto de sua violação caracterizar o elemento normativo do tipo;

[35] 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/artigos/23522>. Acesso em: 29 jul. 2013a.

causa de lacuna legislativa se concentra na hipótese de obtenção dos dados ou das informações durante o tráfego na rede, conduta essa que não se amolda à norma, pena incriminadora em comento.

Qualquer pessoa pode ser sujeito ativo do crime, não exigindo o tipo penal nenhuma condição especial do sujeito ativo. Por sua vez, sujeito passivo é o titular do dispositivo informático e, eventualmente, o titular da informação armazenada em um dispositivo informático alheio, podendo ser pessoa física ou jurídica; não se pode confundir, no entanto, com a pessoa referendada em um documento, pois esta será mera testemunha do fato. Trata-se de crime doloso, em que se reclama a presença dos elementos volitivos e intelectivos, ou seja, querer realizar a conduta e entender a ilicitude do fato. Tem-se, portanto, a livre e consciente vontade ilegítima de violar o dispositivo informático, sem expressa ou tácita permissão do titular dos dados resguardados.

Para a configuração do crime, contudo, demanda-se o elemento especial do tipo, ou seja, que o agente promova a invasão de dispositivo informático com a finalidade específica de obter, adulterar ou destruir dados ou informações, sem autorização expressa ou tácita do titular, ou instalar vulnerabilidades para obter vantagem ilícita. Essas locuções são figuras elementares especiais do tipo subjetivo do injusto que estabelecem adequação entre a infração praticada e o fim pretendido. Não, há nesse sentido, a previsão culposa do delito.

A consumação se opera com o simples ato de invadir, violando mecanismo de segurança, desde que o agente haja impelido pela finalidade de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Trata-se, então, de crime formal, não se formalizando a produção de resultado naturalístico[36]. A obtenção da vantagem ilícita caracteriza exaurimento do crime. Em que se pese admitir a forma tentada, tal circunstância é de difícil configuração na praxe forense (BITENCOURT, 2013).

O parágrafo 2º prevê uma causa de aumento de pena de um sexto a um terço a incidir sobre o *caput*, se da invasão resultar prejuízo econômico à vítima, enquanto o parágrafo 3º prevê qualificadora, com pena de reclusão de 6 (seis) meses a 2 (dois) anos e multa, se a conduta não constituir crime mais grave, no caso de a invasão resultar na obtenção de conteúdo de comunicações eletrônicas privadas,

[36] 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/artigos/23522>. Acesso em: 29 jul. 2013b; MAGGIO, Vicente de Paula Rodrigues. **Novo crime**: invasão de dispositivo informático, 07 abr. de 2013. Disponível em: <http://atualidadesdodireito.com.br/vicentemaggio/2012/12/16/invasao-de-dispositivo-informatico-cp-art-154-a/>. Acesso em: 22 ago. 2013.

segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido.

Verifica-se que nem todo conteúdo ou informação obtida por meio da invasão permitirá caracterizar a qualificadora. Não é porque se assinalou como sigilosa uma informação que ela estará tutelada pela norma em questão; é necessário que o sigilo esteja previsto em lei, como, por exemplo, documentos decorrentes de operações bancárias e de rendas.

O parágrafo 4º prevê uma causa de aumento de pena de um a dois terços a ser incidida, exclusivamente, sobre as hipóteses previstas no parágrafo 3º, caso o agente promova a **"**divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos".

Levando em conta a função exercida pelo sujeito passivo do crime, o parágrafo 5º antevê causa de aumento de pena de um terço à metade se o crime for perpetrado contra: Presidente da República, governadores e prefeitos; Presidente do Supremo Tribunal Federal; Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Sob a ótica da classificação doutrinária, Bittencourt (2013) assinala que o crime de invasão de dispositivo informático é comum, pois não preceitua condição especial do sujeito ativo; formal, já que se consuma com a simples prática das condutas de invadir, produzir, oferecer, distribuir, vender ou difundir o objeto material do crime, antecipando-se o resultado; material, nas figuras qualificadas, em que se estabelece a produção do resultado naturalístico; instantâneo, em que a consumação se opera no momento em que o agente pratica quaisquer das ações, esgotando-se aí a lesão jurídica; comissivo, porque é impossível praticá-lo mediante omissão; doloso, não havendo previsão da modalidade culposa; unissubjetivo (que pode ser praticado por alguém individualmente); plurissubsistente, cuja conduta pode ser desdobrada em mais de um ato, admitindo, em tese, a figura tentada.

Realizada a análise da estrutura do crime de invasão de dispositivo informático, necessário se torna fazer um aporte com o direito espanhol, tentando estabelecer uma exegese em relação à tutela da intimidade, estudo que se fará a seguir.

3 A TUTELA DA PRIVACIDADE NA LEGISLAÇÃO ESPANHOLA EM FACE DOS DELITOS INFORMÁTICOS

Em análise ao Código Penal Espanhol de 1995 (CPE), González Rus

descreve que a primeira vez em que o Direito Penal visou a proteger a privacidade do cidadão no meio ambiente *Internet* foi com o artigo 197.1, ao dispor, em sua primeira parte, que "O que, para descobrir os segredos ou violar a privacidade de outra pessoa, sem o seu consentimento, se apodere de seus papéis, cartas, e-mails ou quaisquer outros documentos a efeitos pessoais [...]"[37] [tradução livre]. Nota-se que o tipo penal buscou proteger a intimidade, ou seja, assegurar o direito de o cidadão manter determinados dados ou informações fora do conhecimento alheio.

O núcleo do tipo é o verbo *apodere,* que tem o sentido de apoderar-se, inserir-se na posse. Tem por objeto material os *papeles,* que não são apenas documentos escritos, mas, também, representações gráficas, desenhos e fotografias; *cartas,* que compreendem as correspondências entre duas pessoas; *mensajes de correo electrónico,* que constituem informações enviadas ou recebidas por meio telefônico ou mediante redes de transmissão de dados; e *cualesquiera otros documentos o efectos personales,* uma forma bem elaborada e genérica que permite incluir qualquer documento que contenha dados relevantes para a intimidade da vítima. Observa-se que o legislador infraconstitucional espanhol buscou tulelar os dados estanques, armazenados em um dos suportes elencados enquanto objeto material do crime. Exigi-se que o agente apodere-se dos papéis, cartas, mensagens de correio eletrônico ou quaisquer outros documentos de efeitos pessoais sem autorização do titular; assim, caso o elemento normativo do tipo não esteja presente, a conduta não se amoldará à referida norma penal incriminadora.

Conforme salienta Gonzáles Rus, "Se o acesso ao email ocorreu durante o processo de trasmissão, interferindo clandestinamente telecomunicações e gravá-las, o suposto típico aplicável é intercepção de telecomunicações"[38] [tradução livre]. Com isso, se for verificado o acesso indevido à informação durante a sua transmissão pela rede mundial de computadores, no golpe denominado *man in the middle*, a conduta se amoldará ao tipo penal previsto no artigo 197.1 *in fine*: [...] ou telecomunicações interceptar ou utilizar técnicas de dispositivos de escuta, transmissão, gravação

[37] GONZÁLES RUS, J. J. et al. **Sistema de Derecho Penal Español** – Parte Especial. DYKINSON, S.L. Madrid, 2011. 298p. Texto original: "El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos a efectos personales [...]".

[38] *Ibidem*, p. 306. Texto original: "Si el acceso al correo se ha producido durante el proceso de transmisión, interfiriendo las telecomunicaciones y grabando subrepticiamente los mismos, el supuesto típico aplicable es interceptación de telecomunicaciones".

ou reprodução de som ou imagem, ou de qualquer outro sinal de comunicação [...]"[39] [tradução livre].

A expressão genérica que faz alusão a qualquer outro sinal de comunicação permite inserir como possível de se amoldar ao tipo em tela a conduta do agente de interceptar pacote de informações por meio da *Internet*; a cláusula genérica, portanto, permitiu incluir, também, as inovações tecnológicas que possam surgir no futuro em matérias de comunicações eletrônicas ou telemáticas, permitindo com que o direito possa tutelar a intimidade, inclusive diante dos avanços tecnológicos.

Em tais condições, não se requer condição especial do sujeito ativo, de forma que pode ser perpetrado por qualquer pessoa, porém, se for praticado por encarregado ou responsável de arquivos, suportes informáticos, eletrônicos ou telemáticos, bem como arquivos de registros, a conduta possui maior desvalor, caracterizando qualificadora, nos termo do artigo 197.5, primeira parte. Se tais agentes, difundem, cedem ou revelam dados reservados, impõe-se causa de aumento de pena. Por sua vez, se cometido por funcionário público que se privilegie de seu cargo para a prática dos crimes do art. 197 CPE, impõe-se causa de aumento de pena, nos termos do art. 198 CPE, com inabilitação absoluta para o cargo pelo prazo de 6 (seis) a 12 (doze) anos. O sujeito passivo é o titular do segredo ou intimidade violada.

De acordo com Gonzáles Rus[40], trata-se de crime formal, em que a mera posse indevida do objeto ou do suporte que contenha o segredo ou as informações relativas à intimidade, consuma o crime, não se exigindo a produção de resultado naturalístico. Assim, o conhecimento do teor do material e sua propagação a outrem é mero exaurimento do delito.

O art. 197.1 do CPE também criminaliza a instalação não autorizada de *cookies*, *sniffers* e *hacking*, enquanto rotinas dispostas no computador do usuário, no momento em que recebe *e-mails* ou acessa algum *site*, cuja função é enviar regularmente a quem o instalou informações e dados sobre a navegação, permitindo a posse de conteúdos, mediante clara e grave vulnerabilidade da intimidade pessoal.

A Lei Orgânica 5/2010[41] introduziu, na legislação espanhola, uma nova

[39] Texto original: "[...] o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación [...]" - artigo 197.1 do Código Penal Espanhol.

[40] *Ibidem*, p. 306.

[41] ESPAÑA. Ley Orgânica 5/2010, de 22 de junio. **Ementa:** Ley Orgánica 5/210, de 22 de junio, por la que se modifica la Ley Orgânica 10/1995, de 23 de noviembre, del Código Penal .**Boletín Oficial del Estado**. Por Rey de España Juan Carlos I, 23 jun. 2010. Sección 1. p. 54811. Disponível em:<http://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-9953>. Acesso em: 09 set. 2013.

forma de punição para intrusão informática ou *hacking*, em que

> [...] por qualquer meio ou procedimento e vulnerando as medidas de segurança estabelecidas para prevenir, acessa sem autorização a dados ou software contidos em um sistema informático ou em parte do mesmo ou permaneça dentro do mesmo contra a vontade de quem tem o legítimo direito de excluir [...][42] [tradução livre]

O crime de intrusão informática também tutela a intimidade, sancionando o simples acesso não autorizado a um sistema informático. Compreende-se por sistema informático os computadores de uso pessoal, as agendas eletrônicas pessoais, os celulares, a rede intranet, extranet e as redes, servidores e outras infraestruturas de *Internet*. Por outro lado, pune-se, inclusive, o excesso em relação à permissão para o acesso ao sistema informático. Isso correrá quando, por exemplo, houver permissão do titular para acessar o sistema informático por um tempo determinado ou para a realização de uma tarefa, porém o agente acessa dados pessoais sem permissão.

Quando perpetrado por pessoa encarregada ou responsável pelo arquivo, suporte informático ou arquivos de dados pessoais, as penas são de três a cinco anos de prisão, caso o agente não ceda ou revele os dados; mas, se os dados forem cedidos ou revelados, a conduta merece melhor desvalor, motivo pelo qual se impõe pena de quatro a cinco anos de prisão. O maior desvalor da conduta se justifica, pois a condição profissional do autor impõe a ele o encargo e a responsabilidade de respeitar, ainda mais, a intimidade alheia, cujos dados pessoais de outréns estão sob sua responsabilidade.

CONSIDERAÇÕES FINAIS

A análise da estrutura do crime de invasão de dispositivo informático possibilitou concluir que o tipo penal buscou tutelar a liberdade individual, dentro do contexto da intimidade das informações estanques em um dispositivo informático, interligado ou não à rede mundial de computadores, desde que o sujeito passivo do crime adote algum mecanismo de segurança capaz de inviabilizar a invasão ao objeto material do crime. Assim, para as informações terem proteção, o agente terá

[42] Texto original: *Ley Orgánica* 5/2010: El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accesa sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo contra de voluntad de quien tenga el legítimo derecho a excluirlo [...] (ESPANHA, 2010)

que invadir o dispositivo informático, violando sistema ou dispositivo de segurança; caso o dispositivo informático não disponha de tal sistema, a conduta não se amoldará à norma penal incriminadora.

No entanto, a informação pode ser obtida com a utilização de outros recursos, como, por exemplo, por meio do golpe *man in the middle*, em que o agente, utilizando da linguagem informática, estando em um nó da rede, monitora o tráfego da rede e emite comandos para aquele que vai abrir uma requisição, se intitulado destinatário, obtendo, desse modo, a informação, sem que tenha invadido o dispositivo informático.

De acordo com a legislação espanhola, tal conduta poderá se amoldar na interceptação das comunicações, prevista no artigo 197.1 do CPE. No Brasil, o artigo 10 da Lei Federal n. 9.296/1996 criminaliza o modo de agir do agente que infringe as comunicações de informática, sem autorização judicial ou com objetivos não autorizados em lei.

Levando em conta que o artigo 5º, XII, da CF prevê o sigilo das comunicações de dados, regulamentado pelo artigo 1º, § único, da Lei nº 9.296/1996, que admite a quebra do sigilo do fluxo das comunicações de informática, por autorização judicial, no curso de investigação criminal ou instrução criminal, a conduta denominada *man in the middle* se amolda ao tipo penal previsto no artigo 10 da Lei Federal nº 9.296/1996[43].

Discute-se se a utilização de ferramentas como *cookies* e *sniffers* também se enquadram na referida norma penal incriminadora. Verifica-se, ainda, que a legislação penal espanhola tem previsão expressa quanto à utilização de tais ferramentas, sem o conhecimento do usuário da *Internet*. Considerando que tais ferramentas possibilitam monitorar o fluxo do acesso individual do internauta na rede mundial de computadores, alimentando um banco de dados da empresa que possibilita estabelecer as preferências do usuário, em patente violação à intimidade, ao nosso ver, tal procedimento se amolda ao tipo penal previsto no artigo 10 da Lei Federal nº 9.296/1996, salvo se houver consentimento do internauta para a instalação do programa espião.

Ressalta-se, porém, que, quanto ao emprego do *cookie*, somente caracterizará interceptação do fluxo das comunicações de informática se instalado e monito-

[43] BRASIL. Lei nº 9.296/1996, de 24 de julho de 1996. **Ementa:** Regulamenta o inciso XII, parte final, do artigo 5º da Constituição Federal**. Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 25 jul. 1996. ed. 143. Seção 1. p.1. Disponível em:<http://www.in.gov.br/visualiza/index.jsp?jornal=1&pagina=1&data=25/07/1996>. Acesso em: 09 set. 2013.

rado por terceiro, ainda que com o conhecimento do responsável legal ou administrador do *site* e sem conhecimento do internauta monitorado.

A invasão de sistemas de *cloud computer* também permite caracterizar o crime em comento, pois em que pese o depósito informático invadido não ser o da própria vítima, continua a pertencer a outrem, *in casu*, a pessoa jurídica que presta tal serviço.

No que tange ao excesso quanto ao consentimento, não se permite amoldar a conduta do sujeito ativo ao crime ora investigado. Assim, se foi permitido ao agente o acesso remoto a um dispositivo informático detentor de mecanismo de segurança para fins de reparo e o mesmo aproveita a oportunidade para obter, adulterar ou destruir dados ou informações contidas no objeto material do crime, o modo de proceder não se enquadra à norma penal incriminadora em tela, pois o núcleo do tipo penal exige que a invasão se dê de forma clandestina, fraudulenta; por outro lado, pensar de forma diferente disso resulta em ferir o princípio da estrita legalidade penal, que não permite o emprego da analogia *in malan partem*.

Vale frisar, no entanto, que o legislador deveria ter tutelado toda e qualquer informação armazenada em um dispositivo informático contra o acesso indevido, independentemente de ter o aparelho mecanismo de segurança. Ademais, a expressa inserção de cláusula genérica possibilitaria tornar a norma sempre atual, considerando ou não os avanços tecnológicos que ainda surgirão e evitando-se discussões jurídicas quanto à, por exemplo, legalidade do emprego de ferramentas como *cookies* e *sniffers*, trazendo, finalmente, maior segurança quanto à efetiva tutela da intimidade na rede mundial de computadores.

Não se pode deixar de consignar, além disso, que o legislador infraconstitucional criminalizou uma conduta que, em regra, será crime meio para a prática de outros delitos, como, por exemplo, crimes contra a honra e furto mediante fraude praticado por meio da *Internet*, o que fará com que seja absorvido em face do princípio da consunção.

REFERÊNCIAS

ÁLVAREZ B. DE BOZO, M.; ÁVILA HERNÁNDERZ, F. M.; PEÑARANDA QUINTERO, H.R. **La libertad Informática: Derecho Fundamental en la Constitución Venezolana**. Revista Internacional de Derecho e Informática, año 2. n.1, jan./dez. 2000. Disponível em: <http://www.omdi.info/espanol/reivdi/ano2_n1/alvarez_2.htm>. Acesso em: 19 ago. 2013.

ANDRADE. Allan Diego Mendes. **O direito à intimidade e à vida privada em face das novas tecnologias da informação**. [2013?]. Disponível em: <http://www.faete.edu.br/revista/odireito aintimidade20a_vida_privada_em_facedasnovastecnologiasdainformacao-all20diego.pdf>. Acesso em: 21 ago 2013.

BATISTA, Nilo. **Introdução crítica ao Direito Penal brasileiro**. 8. ed. Rio de Janeiro: Revan, 2002.

BITENCOURT, Cézar Roberto. **Invasão de dispositivo informático**. Disponível em: <http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico/>. Acesso em: 22 ago 2013.

BRASIL. Lei nº. 12.737, de 30 de novembro de 2012. **Ementa**: Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 03 dez. 2012. ed. 232. Seção 1. p.1. Disponível em: <http://www.in.gov.br/visualiza/index.jsp?jornal=1&pagina=1&data=03/12/2012>. Acesso em: 09 set. 2013.

_____ . Lei nº 9.296/1996, de 24 de julho de 1996. **Ementa**: Regulamenta o inciso XII, parte final, do artigo 5º da Constituição Federal. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 25 jul. 1996. ed. 143. Seção 1. p.1. Disponível em:http://www.in.gov.br/visualiza/index.jsp?jornal=1&pagina=1&data=25/07/1996>. Acesso em: 09 set. 2013.

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/artigos/23522>. Acesso em: 29 jul. 2013a.

_____ . O novo crime de invasão de dispositivo informático. **Consultor Jurídico**, 04 fev. 2013. Disponível em: <http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico>. Acesso em: 20 ago 2013b.

DAVARA RODRÍGUEZ, Miguel Ángel. **Manual de Derecho Informático**. Ed. 10. Navarra: Arazandi, 2008. 534p.

DOTTI, René Ariel. **Proteção da vida privada e liberdade de informação**. São Paulo: RT, 1980.

ESPAÑA. Ley Orgânica 5/2010, de 22 de junio. **Ementa**: Ley Orgánica 5/210, de 22 de junio, por la que se modifica la Ley Orgânica 10/1995, de 23 de noviembre, del Código

Penal. **Boletín Oficial del Estado**. Por Rey de España Juan Carlos I, 23 jun. 2010. Sección 1. p. 54811. Disponível em:<http://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-9953>. Acesso em: 09 set. 2013.

GONZÁLES RUS, J. J. et al. **Sistema de Derecho Penal Español** – Parte Especial. DYKINSON, S.L. Madrid, 2011.

MAGGIO, Vicente de Paula Rodrigues. **Novo crime:** invasão de dispositivo informático, 07 abr. de 2013. Disponível em: <http://atualidadesdodireito.com.br/vicentemaggio/2012/12/16/invasao-de-dispositivo-informatico-cp-art-154-a/>. Acesso em: 22 ago. 2013.

MUÑOZ CONDE, Francisco; GARCIA ARÁN, Mercedes. **Derecho penal, parte general**. 7. ed. Valência: Tirant lo blanch, 2007.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**. ed. 9. São Paulo: RT, 2013.

PÉREZ LUÑO, Antonio-Enrique. **La tercera generación de Derechos Humanos**. Navarra: Arazandi, 2006.

SCHÜNEMANN, Bernd. El principio de protección de bienes jurídicos como punto de fuga de los limites constitucionales de los penales y de su interpretación. In: HEFENDEHL, Roland (Ed.). **La teoria del bien jurídico:** ¿fundamento de legitimación del derecho penal o juego de abalorios dogmático? Barcelona: Macial Pons, Ediciones Jurídicas y Sociales, S. A. Madrid, 2007.

SILVA, José Afonso da. **Curso de Direito Constitucional positivo**. 34. ed. São Paulo: Malheiros, 2011.

TOLEDO, Francisco de Assis. **Princípios básicos de Direito Penal**: de acordo com a Lei n. 7.209, de 11/07/1984 e com a constituição federal de 1988. 5. ed. São Paulo: Saraiva, 2007.

WOLKMER, Antonio Carlos. **Introdução aos fundamentos de uma teoria geral dos "novos" direitos**. In: WOLKMER, Antonio Carlos; LEITE, José Rubens Morato (org.). Os "novos" direitos no Brasil: natureza e perspectivas. São Paulo: Saraiva, 2003.

ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. **Manual de Direito Penal brasileiro**: parte geral. 4. ed. São Paulo: Revista dos Tribunais, 2002.