DOS CRIMES INFORMÁTICOS SOB A ÓTICA DO MEIO AMBIENTE DIGITAL CONSTITUCIONALIZADO E DA SEGURANÇA DA INFORMAÇÃO

Caio Eduardo Costa Cazelatto*
Antonio Carlos Segatto**

RESUMO: Com o advento da *Internet* e dos computadores, a proteção da informação ganha paulatinamente maior destaque. Com esses instrumentos à disposição do uso particular, novos e diferentes modos de se praticar condutas ilícitas são constantemente praticadas. Assim, a pesquisa visou analisar, por meio do método bibliográfico, os crimes informáticos sob a ótica do meio ambiente digital constitucionalizado e da Segurança da Informação, explorando seus reflexos perante o ordenamento jurídico. Para tanto, estabeleceu-se a caracterização do ambiente digital constitucionalizado, através da conceituação e classificação do meio ambiente. Ainda, explorou-se o *nomen juris*, a conceituação e classificação dos crimes informáticos, além de apresentar os mais cometidos em meio às novas tecnologias da informação, como: a difamação, a calúnia, a injúria, o furto, o estelionato e a invasão de dispositivo informático alheio.

PALAVRAS-CHAVE: Crimes Informáticos; Meio Ambiente Digital; Segurança da Informação.

INTERNET CRIMES FROM THE POINT OF VIEW OF CONSTITUTIONALIZED DIGITAL ENVIRONMENT AND THE SAFETY OF INFORMATION

ABSTRACT: The protection of information slowly gains relevance with the advent of the Internet and computers. New and different modes of practicing illicit

* Discente do curso de Direito da Universidade Estadual de Maringá - UEM, Maringá (PR); Bolsista PIBIC/CNPq/FA-UEM; E-mail: caiocazelatto@gmail.com

** Doutor em Direito pela Pontifícia Universidade Católica de São Paulo PUCSP; Docente Adjunto na Universidade Estadual de Maringá - UEM, Maringá (PR).

acts are constantly being invented by digital tools available to all. Current research analyzes through a bibliographical review the crime committed on the Internet from the point of view of constitutionalized digital environment and the safety of information. Its consequences within juridical ordering are explored. Constitutionalized digital environment is characterized by providing the concept and classification of the environment. The nomen juris was explored, or rather, the concept and classification of Internet crimes, coupled to those frequently practiced due to new technologies, such as defamation, calumny, violence against one´s good name, robbery, theft and the invasion of the other´s information devise.

KEY WORDS: Internet Crimes; Digital Environment; Safety of Information.

DE LOS CRÍMENES INFORMÁTICOS DESDE LA PERSPECTIVA DEL MEDIOAMBIENTE DIGITAL CONSTITUCIONALIZADO Y DE LA SEGURIDAD DE LA INFORMACIÓN

RESUMEN: Con el adviento de la Internet y de los ordenadores, la protección de la información cobra, paulatinamente, más destaque. Con tales instrumentos a la disposición del uso particular, nuevos y distintos modos de practicarse conductas ilícitas son constantemente practicadas. Así, la investigación buscó analizar, por medio del método bibliográfico, los crímenes informáticos desde la perspectiva del medioambiente digital constitucionalizado y de la Seguridad de la Información, explotando sus reflejos frente al ordenamiento jurídico. Para ello, se estableció la caracterización del ambiente digital constitucionalizado, por medio de la conceptualización y clasificación del medioambiente. Aún, se explotó el nomen juris, la conceptualización y clasificación de los crímenes informáticos, además de presentar los más cometidos en medio a las nuevas tecnologías de la información, como: la difamación, la calumnia, la injuria, el hurto, el estelionato y la invasión del dispositivo informático ajeno.

PALABRAS-CLAVE: Crímenes Informáticos; Medioambiente Digital; Seguridad de la Información.

INTRODUÇÃO

O presente trabalho teve como finalidade analisar os aspectos jurídico-penais e criminológicos dos crimes informáticos sob a ótica do meio ambiente virtual constitucionalizado e da segurança da informação.

Com os óbices de controle do âmbito informático surge o dever de direcionar a atenção não somente do legislador, como também de toda ciência jurídica aos crimes informáticos. O tema é atual e relevante à seara do Direito, uma vez que há pouco esclarecimento e amparo jurídico brasileiro acerca das condutas realizadas por instrumentos informáticos conectados à *Internet*.

Inicialmente, o estudo apresentou a conceituação e evolução dos computadores e da *Internet*, como o surgimento dos primeiros maquinários computadorizados e a disseminação do acesso à Grande Rede.

Outro aspecto destacado foi a Segurança da Informação, em que pese, conta com três conteúdos essenciais: a integralidade, a disponibilidade e a confidencialidade, demonstrando-se o aparato estatal e não-estatal acerca da garantia de segurança em âmbito virtual.

De igual modo, foi delimitado o espaço informático através da conceituação e da classificação de meio ambiente constitucionalizado, sendo este dividido, hodiernamente, em artificial, natural, cultura, do trabalhado e, mais recentemente, informático. Assim, relacionou os deveres, inerentes aos direitos fundamentais, de respeito, proteção e promoção deste novo meio.

A partir de então, as análises se aprofundaram perante os crimes informáticos, sendo estabelecido seu *nomen juris,* frente às diversas tentativas doutrinárias ao termo mais adequado, sua conceituação e sua classificação em três categorias: próprios, que são crimes praticados conta o aparato informático; impróprios, que são executados mediante o uso de aparatos informáticos; e mistos, que se concretiza tanto contra como por meio de computadores.

Por fim, a pesquisa selecionou os crimes mais comuns dessa espécie, como os contra honra, presentes os crimes de difamação, calúnia e injúria; os contra patrimônio, especialmente os crimes de furto e estelionato; e os de invasão de dispositivo informático alheio, que foi tipificado recentemente por meio da Lei nº. 12.737/2012.

2 DA EVOLUÇÃO DO COMPUTADOR E DA INTERNET

A criminalidade informática está intrinsecamente associada à evolução dos computadores e, principalmente, ao surgimento da *Internet*, sendo indispensável realizar uma breve abordagem histórica desses instrumentos.

O computador adveio da necessidade de se criar uma máquina de calcular que sintetizasse o raciocínio humano a um processo mecânico. Os primeiros exemplares digitais, Colossos, Eniac e Enivac, eram máquinas gigantescas e repletas de válvulas, que foram construídos com propósitos militares[1].

Com o tempo, emergiu o desafio de transformá-los em um meio de comunicação entre as pessoas, o que foi concretizado nos anos de 1970. Entretanto, o grandioso tamanho desses modelos os tornava inviáveis para o uso doméstico e, devido a isso, buscou-se o aprimoramento dos computadores em micromáquinas. Essa expectativa foi alcançada com a criação do minicomputador PDP8, chegando em pouco tempo aos usuários domésticos[2].

Em relação à *Internet*, pode-se defini-la como uma rede mundial de usuários que, simultaneamente, trocam informações. Segundo a Agência Nacional de Telecomunicações, ANATEL, pela Norma nº. 004/95, a *Internet* é o "nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores, bem como o 'software' e os dados contidos nestes computadores"[3].

Sua origem está assentada na estrutura ARPANET, *Advanced Research Projec Agency*, desenvolvida pelo Departamento de Defesa dos Estados Unidos, no início dos anos 60 do século XX, em plena Guerra Fria[4].

Além de ter sido uma resposta às disputas tecnológicas entre o Estado norte-americano e a extinta União Soviética, a *ARPANET* foi projetada para ser uma rede militar de comunicação independente, com um único servidor, isto é, sem um comando central, objetivando preservar a operabilidade do sistema mediante ataques nucleares. Posteriormente, sua utilização foi disponibilizada às universidades, sendo difundida paulatinamente nos meios acadêmicos.

Já na década de 80, esse primitivo conjunto de redes virtuais foi substituído oficialmente pela *Internet*, permitindo - com a elaboração do *World Wide Web* (www), pelo inglês Tim Berners Lee - o acesso doméstico[5].

---

[1] BRIGGS, Asa; BURKE, Peter. Uma história social da mídia: de Gutenberg à Internet. Tradução de Maria Carmelita Pádua Dias. Rio de Janeiro: Jorge Zahar, 2006, p. 300-305.

[2] Ibidem, 2006, p. 300-305.

[3] BRASIL, Agência Nacional de Telecomunicações. Norma 004/95: Uso de meios da rede pública de telecomunicações para acesso à internet. Disponível em: <http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=10283&assuntoPublicacao=Norma%20MC%20n%BA%20004/1995&caminhoRel=null&filtro=1&documentoPath=biblioteca/Normas/Normas_MC/norma_004_95.htm>. Acesso em: 03 jul. 2014.

[4] FERREIRA, Érica Lourenço de Lima. Internet: Macrocriminalidade e Jurisdição Internacional. Curitiba: Juruá, 2007, p. 80-81.

[5] BRIGGS; BURKE, op. cit., 2006, p. 300-305.

Com essas tecnologias disponíveis ao uso particular, o computador conectado à grande rede possibilitou a intensificação das relações interpessoais, tornando-se um instrumento imprescindível à vida de uma grande parcela da população mundial e, ao mesmo tempo, revestiu-se como um poderoso gerador de riscos, propício à prática de inúmeros ilícitos.

3 DA SEGURANÇA DA INFORMAÇÃO

Desde o surgimento da escrita e da leitura, a confidencialidade da informação passou a assumir, gradativamente, elevada relevância. Proteger determinado conteúdo informativo começou a refletir não apenas perante o caráter comunicativo, mas também o econômico, o social e o particular de cada indivíduo.

A partir de então, a busca pelo aprimoramento da proteção da informação foi aumentando, visando destiná-la apenas aos legítimos interessados.

Na Grécia Antiga, por exemplo, os generais do exército de Esparta utilizavam mecanismos criptográficos para resguardar o conteúdo de suas mensagens, sendo estas escritas em papiros e enroladas espiralmente em um bastão, chamados de *scytale*, sendo que a informação contida só poderia ser "decifrada" por quem possuísse um *scytale* correspondente[6].

Hodiernamente, o âmbito informático se destaca como um dos principais meios transmissores de informações, e, consequentemente, como um potencial gerador de novos ilícitos, o que exige um constante e sofisticado desenvolvimento de garantias de segurança neste setor.

Com o advento dessas tecnologias, diversos métodos violadores da segurança informática foram criados, em que seus agentes são popularmente conhecidos por *hacker*, *crackers, spammers*, entre outros. Para se prevenir e combater tais ameaças, a segurança da informação se solidificou, sendo definida como:

> Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança

[6] GARFINKEL, S.; SPAFFORD, G. Computer security: practical unix e internet security. 2 ed. 1996. apud ALEXANDRIA, João Carlos Soares de. Gestão da segurança da informação: uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica. 193f. Tese (Doutorado em Ciência na Área de Tecnologia Nuclear) - Instituto de Pesquisas Energéticas e Nucleares - USP, São Paulo, p. 33.

> dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento[7].

Além disso, é caracterizada por três elementos essenciais, denominados por princípios básicos[8], que são: a confidencialidade, a integridade e a disponibilidade.

A confidencialidade é a garantia de que a informação, individualizada e particular, armazenada em determinado aparato informático, seja preservada em sigilo, estando disponível e acessível apenas a quem estiver autorizado e legitimado[9].

Quanto à integridade, trata-se da "incolumidade de dados ou informações na origem, no trânsito ou no destino", ou seja, é a prerrogativa de que os dados criados, transmitidos, recebidos, copiados e armazenados não sejam alterados por terceiros sem autorização[10].

Já a disponibilidade se caracteriza pela viabilização de acesso à informação, possibilitando o usuário legítimo e autorizado a acessar determinado conteúdo[11].

Assim, a segurança informática vai além de meramente proteger informações contra invasões, corrupções de dados ou suas destruições, como também representa a garantia de acessá-las em sua integridade, da forma como foi criada, copiada, armazenada e transmitida.

Dessa forma, a segurança informática está estreitamente associada aos crimes informáticos, especificamente os classificados como próprios, em que são constituídos a partir do descumprimento de um desses três elementos básicos.

4 DO MEIO AMBIENTE FRENTE OS CRIMES INFORMÁTICOS

Ao se aprofundar nos estudos acerca dos crimes informáticos, verificou-se a necessidade de se estabelecer e analisar o ambiente em que estes são praticados, tanto por se tratar de um espaço relativamente recente, como também por ser pouco explorado, especialmente no ordenamento jurídico, com carência de material doutrinário, legislativo e jurídico acerca do tema.

---

[7] Decreto nº. 3.505, de 13 de junho de 2000, art. 2°, § II.

[8] ABNT ISO 17779 NBR.

[9] Decreto nº. 4.553, de 27 de dezembro de 2002, art 4°, §VIII.

[10] Decreto nº. 4.553, de 27 de dezembro de 2002, art 4°, §VIII.

[11] Decreto nº. 4553, de 27 de dezembro de 2002, art 4°, §VIII.

Assim, apesar do ambiente digital, que não é um espaço físico, ser caracterizado como *locus* de exercício de liberdade, de expressão de pensamento, além de viabilizador de inter-relações, inclusive como meio de lazer e entretenimento, as condutas nele realizadas geram resultados materiais e até lesivos, ficando inúmeras vezes à margem do conhecimento e da punibilidade estatal.

Essa criminalidade além de afetar institutos do Direito Penal também interfere no Direito Constitucional, como quando ocorre a violação de direitos fundamentais, como o direito à intimidade e à vida privada, assegurados no art. 5°, inc. X, da Constituição Federal.

Do mesmo modo, atribui-se ao Direito Constitucional, explorado por Paulo Bonavides como a ciência das regras jurídicas encarregadas de estabelecer, transmitir e exercer a autoridade pública[12] o papel de tutelar este novo ambiente.

Para tanto, a concepção do termo meio ambiente, com o avanço dos estudos acadêmicos acerca do tema, modificou-se entre a doutrina jurídica, visando englobar as constantes mutações sociais, culturais e axiológicas.

A legislação, em contrapartida, consagrou um conceito restrito, limitando a possibilidade de bens jurídicos protegidos, em que o descreve como "o conjunto de condições, leis, influências, alterações e interações de ordem física, química e biológica, que permite, abriga e rege a vida em todas as suas formas"[13].

Para sanar essa carência legislativa é essencial adotar posicionamentos doutrinários que ofereçam análises mais extensivas dessa terminologia, como o de José Joaquim Gomes Canotilho, que a descreve como o "conjunto dos elementos que, na complexidade das suas relações, constituem o quadro, o meio e as condições de vida do homem, tal como são, ou tal como são sentidos"[14].

No mesmo raciocínio, José Afonso da Silva leciona que tal é "a interação do conjunto de elementos naturais, artificiais e culturais que propiciem o desenvolvimento equilibrado da vida em todas as suas formas"[15].

De igual modo, Celso Antonio Pacheco Fiorillo entende que a partir do próprio artigo 225, da Constituição Federal, por meio da expressão "sadia qualidade de vida", já há alusão a uma definição jurídica indeterminada e ampla de meio

[12] BONAVIDES, Paulo. Curso de direito constitucional. São Paulo: Malheiros, 2005, p. 21-22.

[13] Art. 3°, I, da Lei nº. 6.938/81.

[14] CANOTILHO, José Joaquim Gomes. Protecção do ambiente e direito de propriedade: (crítica de jurisprudência ambiental). Coimbra: Coimbra, 1995, p. 10.

[15] SILVA, José Afonso da. Direito ambiental constitucional. 4. ed. São Paulo: Malheiros, 2003, p. 19.

ambiente, eis que o ser humano é titular do direito à sadia qualidade de vida do meio genérico em que se envolve, extrapolando, assim, os limites da definição de ambiente natural[16].

Dessa forma, é possível classificar o meio ambiente não apenas por seus elementos naturais, como fauna e flora, como também por toda construção/relação social em que o ser humano é envolvido, isto é, o meio ambiente artificial, cultural, do trabalho e informático.

Embora o meio ambiente seja geralmente classificado em quatro espécies, quais sejam: a natural, a artificial, a cultural e a do trabalho, emergiu uma nova categoria a ser analisada, o ambiente informático.

Assim, conforme os artigos 3°, inciso V, da Lei nº. 6.938/81, e 225, §1°, incisos I, II, III e IV, da Constituição Federal, considera-se como meio ambiente natural os recursos naturais, isto é, "a atmosfera, as águas interiores, superficiais e subterrâneas, os estuários, o mar territorial, o solo, o subsolo, os elementos da biosfera, a fauna e a flora".

Já o meio ambiente artificial se encontra amparado pelos artigos 21, inciso XX, e 182, da Constituição Federal, em que pode ser compreendido por aquele construído pelo homem em substituição dos espaços naturais, como as construções urbanísticas e rurais[17].

O âmbito cultural se destaca por abarcar o patrimônio histórico, arqueológico, artístico, turístico, paleontológico, paisagístico e cultural, sendo caracterizados por bens de natureza material e imaterial, e está previsto expressamente pelos artigos 216, incisos IV e V, e 225, da Lei Maior.

Em se tratando de meio ambiente do trabalho, que está regulamentado pelos artigos 7°, incisos XXII e XXIII, e 200, inciso VIII, da Constituição Federal, Amauri Mascaro Nascimento assinala ser estruturado pelo complexo entre máquina e trabalhador, isto é, constitui-se pelas instalações edificadas, instrumentos de uso individual, condições de salubridade, periculosidade, jornada de trabalho, férias, relação entre empregado e empregador, entre outros fatores[18].

Por fim, o ambiente informático, que é o foco deste capítulo, pode ser elucidado, brevemente, como todo meio que viabilize a interação entre pessoas, compu-

[16] FIORILLO, Celso Antonio Pacheco. Curso de direito ambiental brasileiro. 5.ed. São Paulo: Saraiva, 2004, p. 19-20.

[17] Ibidem, 2004, p. 277.

[18] NASCIMENTO, Amauri Mascaro. Curso de direito do trabalho: história e teoria geral do direito do trabalho: relações individuais e coletivas do trabalho. 26. ed. São Paulo: Saraiva: 2011, p. 846.

tadores e seus elementos, seja conectados à Grande Rede ou não, bem como com os demais instrumentos que se utilizem de processamento automático de dados, como celulares, *tablets, notebooks,* etc.

5 DO MEIO AMBIENTE DIGITAL CONSTITUCIONALIZADO

O primeiro respaldo constitucional atribuído ao meio ambiente se deu através da Constituição Federal de 1988, por meio de seu artigo 225, sendo elencado como um direito fundamental[19].

Com esse posicionamento, o constituinte revestiu a União, os Estados e os Municípios de autonomia tanto administrativa quanto legislativamente para desenvolver suas diretrizes políticas perante o tema.

Em se tratando de lei infraconstitucional, a Lei nº. 6.938/81 estabelece formalmente a Política Nacional do Meio Ambiente e orienta toda sistemática legal acerca das políticas públicas destinadas ao meio ambiente a serem exercitadas pelos entes federativos.

Com os valores constitucionais o fundamentando, uma nova perspectiva de respeito, proteção e promoção passa a irradiar sobre esse bem jurídico, inclusive perante o âmbito da informática, buscando mantê-lo sadio e equilibrado. É o que aduz Celso Fiorillo:

> O direito fundamental ao meio ambiente ecologicamente equilibrado é elemento importante para obtenção de padrões de vida digna e saudável, no que autoriza a superação da oposição entre objetivos econômicos e estratégias de conservação da natureza, estimulando a busca de padrões sustentáveis de desenvolvimento[20].

Nesse sentido, George Marmelstein leciona que o dever de respeito é exercido quando o Estado se posiciona em harmonia com o direito fundamental em questão, não o violando, nem adotando medidas que o ameace, gerando, assim, um comando de auto-abstenção, de inércia[21].

É o que ocorre quando é assegurado o livre exercício da liberdade de expressão em meio digital a todo indivíduo, sem intervenções (censuras) estatais.

[19] FIORILLO, op. cit., 2004, p. 23-24.

[20] Ibidem, 2004, p. 328.

[21] Ibidem, 2004, p. 320.

O dever de proteção é uma obrigação constitucional que se complementa com o dever de respeito, eis que para a efetivação dos direitos fundamentais não basta que o Estado se mantenha inerte, necessitando também de sua atuação positiva, de ação, protegendo-os de qualquer lesão, inclusive de terceiros. Isto é, atribui obrigações aos poderes públicos de assegurarem a devida manutenção do exercício desses direitos.

Nesse sentido, proteger significa destinar aos poderes estatais a criação de leis que regulamentem o ambiente informático, como o caso do Marco Civil da Internet[22]. Além disso, é possível abordar neste ponto também o monitoramento do espaço virtual, por meio de mecanismos de segurança, com o objetivo de afastar potenciais ameaças e riscos a seus usuários.

Já o dever de promoção impõe ao Estado elaborar medidas concretas e capazes de viabilizar a efetivação de direitos fundamentais, seja por meio de políticas públicas, seja por qualquer ação eficaz.

Dessa forma, a promoção se assenta, por exemplo, em políticas públicas destinadas à democratização do acesso à informação através de sistemas computadorizados conectados à *Internet*. É o caso da cidade de Palmital (PR) que, em parceria com o Governo Federal, criou Telecentros Comunitários, que são espaços públicos que oferecem, gratuitamente, computadores conectados à *Internet*, visando que "[...] todos, crianças, jovens e adultos, tenham a oportunidade de aprimorar seus conhecimentos profissionais e educacionais"[23].

Embora o mencionado doutrinador destine esses deveres apenas ao Estado, é possível estendê-los a todo ser humano, uma vez que a Declaração Universal dos Direitos Humanos dispõe que os indivíduos "devem agir para com os outros em espírito de fraternidade"[24].

Assim sendo, tanto o Estado como a sociedade devem respeitar, proteger e promover o direito fundamental aos diversos tipos de meio ambiente, inclusive o informático. Trata-se de uma nova tutela constitucional visando aproximar o Direito às novas necessidades e realidades sociais.

---

[22] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 23 maio 2014.

[23] Parceria entre Prefeitura e Governo Federal disponibiliza internet gratuita à população. Prefeitura de Palmital. Disponível em: <http://www.palmital.pr.gov.br/noticias/parceria-entre-prefeitura-e-governo-federal-disponibiliza-internet-gratuita-a-populacao/>. Acesso em: 23 maio 2014.

[24] Disponível em: <http://portal.mj.gov.br/sedh/ct/legis_intern/ddh_bib_inter_universal.htm>. Acesso em: 23 maio 2014.

6 DOS ASPECTOS JURÍDICO-PENAIS DOS CRIMES INFORMÁTICOS

O Direito Penal é o responsável por proteger os bens jurídicos[25] essenciais à sociedade, em que sua expansão ou modernização[26], isto é, a tutela de novos bens jurídicos, vem para suprir a constante mutação dos interesses e valores socioculturais. Esse fenômeno decorre de realidades antes desconhecidas ao ser humano, seja por inexistirem em determinado momento, seja pela escassez de bens que eram abundantes, ou mesmo por valores que se alteram no desenvolvimento histórico[27].

Com a solidificação da sociedade pós-industrial, também denominada por sociedade de risco, e de suas transformações científico-tecnológicas, houve a abertura para o desenvolvimento de novas criminalidades capazes de produzirem vitimização tanto individual, quanto em massa. Trata-se de um rol de condutas geradoras de resultados lesivos, que evoluíram significativamente com a globalização, como é o caso dos crimes informáticos.

Em um apurado exame da doutrina jurídica brasileira é possível encontrar diferentes nomenclaturas para os mesmos, como *cybercrimes*, crimes do computador, da informática, virtuais, eletrônicos, digitais, entre outros.

Por essa razão, verifica-se a importância em se definir um *nomen juris* que se aproxime dos objetivos que serão analisados nesta pesquisa.

Para Augusto Eduardo de Souza Rossini, a designação mais adequada é a de "delitos informáticos", por abarcar questões envolvendo crimes e contravenções penais executadas não apenas com o uso da *Internet* ou de outro meio telemático, como também de todo e qualquer sistema informático. Aduz que o termo "delitos informáticos" é o gênero, enquanto "delitos telemáticos" é uma espécie[28].

Assim, infere-se que ilícitos cometidos através da *Internet* são espécies dos crimes informáticos, em que estes detêm uma abrangência maior.

Do mesmo modo, Spencer Toth Sydow segue essa lógica, tendo em vista que se trata de

---

[25] Segundo Roxin, o Direito Penal somente será capaz de proteger os bens jurídicos quando o legislador cumprir sua função de proibir "todas as ações que representem um risco não permitido para o bem jurídico protegido e imputando ao autor o resultado típico, que surge como realização de um risco não permitido". ROXIN, Claus. Reflexões sobre a construção sistemática do direito penal. Revista Brasileira de Ciências Criminais, São Paulo, n. 82, a.18, jan./fev. 2010, p. 24-47.

[26] Salienta-se que nem toda expansão é entendida como modernização, esta se refere à constituição de tipos penais que são orientados pelos princípios basilares do Direito Penal.

[27] SÁNCHES, Jesús-Maria Silva. A expansão do direito penal: aspectos da política criminal nas sociedades pós-industriais. Revista dos Tribunais, São Paulo, v. 11, p. 27-28, 2002.

[28] ROSSINI, Augusto Eduardo de Souza. Informática, telemática e direito penal. São Paulo: Memória Jurídica, 2004, p. 110.

> [...] uma criminalidade que não está limitada às tecnologias existentes nem limita à internet ou aos computadores, mas sim àquelas condutas que vão utilizando um novo ferramental conforme evolui o ser humano e a ciência - seja a nanotecnologia, a telefonia, a computação, a robótica ou qualquer outro ramo que crie aparatos facilitadores das tarefas diuturnas[29].

Já Marcelo Xavier de Freitas Crespo prefere utilizar a expressão "crimes digitais", tendo em vista que abarca tanto os elementos da Informática quanto os da Telemática, sendo atribuída maior flexibilidade de uso frente às constantes inovações tecnológicas e seus reflexos penais[30].

No entendimento de Cecílio da Fonseca Vieira Ramalho Terceiro, a nomenclatura "delitos virtuais" se aproxima mais do rol de atividades ilícitas desta seara, uma vez que

> [...] os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas[31].

Em oposição, Túlio Vianna destaca que a denominação "delitos digitais" é equivocada, pois, "ainda que se conceba que os delitos são praticados em um mundo virtual, não haveria qualquer sentido em se falar de um bem jurídico virtual"[32].

Nesse sentido, optou-se por seguir o raciocínio de Vianna, Rossini e Sydow e adotar o termo "crime informático"[33], já que o adjetivo "informático" engloba a informação (dados), o computador e seus elementos, conectados à Grande Rede ou não, bem como os demais instrumentos que se utilizem de processamento automático de dados, como celulares, *tablets*, *notebooks*, etc. Além disso, também se justifica em virtude do bem jurídico protegido, qual seja, a inviolabilidade da informação, destinando ao termo "informação" a sua principal referência.

---

[29] SYDOW, Spencer Toth. Crimes informáticos e suas vítimas. São Paulo: Saraiva, 2013, p. 56.

[30] CRESPO, Marcelo Xavier de Freitas. Crimes digitais. São Paulo: Saraiva, 2011, p. 50.

[31] RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. Jus Navigandi, Teresina, v. 6, n. 58, ago. 2002. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/13024-13025-1-PB.pdf >. Acesso em: 21 jun. 2014.

[32] VIANNA, Túlio Lima. Fundamentos de direito penal informático: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003. p. 20-21.

[33] Ibidem, 2003, p. 10.

A conceituação de crimes informáticos é controversa na doutrina brasileira e embora sua definição seja ampla, defini-la se faz necessário para permitir uma abordagem e classificação científica mais precisa.

Ivette Senise Ferreira esclarece que, respeitando os princípios da legalidade e da reserva legal, os crimes informáticos são "toda ação típica, antijurídica e culpável cometida contra ou pela utilização de procedimentos automático de dados ou sua transmissão"[34].

De igual modo, o Conselho da Europa, a partir da Convenção de Budapeste[35], definiu tais crimes como conduta ilícita, antiética e não autorizada, envolvendo processamento automático de dados e/ou transmissão destes.

Para Augusto Rossini, a principal característica está assentada no rompimento indevido dos elementos da segurança informática, quais sejam: a integridade, a indisponibilidade e/ou a confidencialidade[36].

Tratam-se de delitos conceituados em decorrência, principalmente, da lesão ao bem jurídico da inviolabilidade de informações, corolário do direito fundamental à privacidade e intimidade, previstos no art. 5, inc. X, da Constituição Federal[37]. Ou, ainda, de outros bens jurídicos, quando estes são violados através do uso de máquinas computadorizadas.

Assim, em consonância com o exposto, crime informático é toda ação não autorizada, típica, antijurídica e culpável, cometida contra ou pela utilização de procedimentos automáticos de dados ou sua transmissão, mediante a violação da segurança informática.

7 DA CLASSIFICAÇÃO DOS CRIMES INFORMÁTICOS

Inicialmente, a principal finalidade dos crimes informáticos residia em invadir a intimidade de terceiros, tanto de pessoas físicas quanto jurídicas. Por se trata-

[34] FERREIRA, Ivette Senise. A criminalidade informática. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). Direito & internet: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2008, v. 2. p. 210.

[35] BRASIL. Ministério Público Federal. **Convenção sobre o Cibercrime**. Disponível em: <http://ascji.pgr.mpf.gov.br/informes-e-documentos/documentos/docs_documentos/convencao_cibercrime.pdf>. Acesso em: 19 mar. 2014.

[36] ROSSINI, op. cit., 2004, p. 110.

[37] VIANNA, Túlio Lima; MACHADO, Felipe Daniel Amorim. Crimes informáticos: conforme a Lei n. 12.737/2012. Belo Horizonte: Fórum, 2013, p. 29.

rem de condutas de difícil identificação de seus agentes, praticadas geralmente no anonimato, outras modalidades ganharam espaço, como os ilícitos contra a honra.

Com a evolução da criminalidade em âmbito informático, os contra o patrimônio passaram prevalecer, captando a atenção estatal para o desenvolvimento de medidas preventivas e protetivas.

O Brasil, através de institutos especializados, como a Safernet[38], órgão não governamental destinado a receber denúncias sobre violação de direitos humanos praticados pela *Internet*, destaca-se internacionalmente no combate aos crimes dessa natureza.

É fundamental destacar que, segundo os princípios da anterioridade e da legalidade, previsto no artigo 5º, XXXIX da Constituição Federal, e no artigo 1º do Código Penal, não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Essa é uma garantia constitucional do direito de cada individual do cidadão frente ao poder punitivo do Estado.

Assim, para que uma ação ou omissão seja tida como crime, inclusive de caráter informático, é preciso que a norma seja anterior ao fato.

Para se analisar cientificamente as condutas ilícitas praticadas por meio de computadores, a doutrina tentou estabelecer diversas classificações, e, embora mereça destaque a realizada pelo professor Tulio Vianna, que os divide em quatro categorias: próprios, impróprios, mistos e mediatos ou indiretos, optou-se por abordar apenas as três primeiras classificações, tendo em vista a estreita proximidade conceitual entre os crimes mistos com os mediatos ou indiretos.

Os crimes informáticos próprios surgiram com o advento da tecnologia computadorizada, sendo sua prática exercida exclusivamente contra os sistemas informáticos, em que estes servem como meio e fim almejados pelo agente.

São condutas ilícitas que burlaram algum ou todos os elementos da segurança informática, quais sejam: a integridade, a confidencialidade e a disponibilidade.

Nesse rol, encontram-se os que ofendem o computador ou dados nele armazenados, destacando-se os contra a inviolabilidade de dados, de telecomunicações, além do bom funcionamento dos sistemas operados eletronicamente, como sítios virtuais (*sites*), *hardware*, *software*, dentre outros.

[38] SAFERNET. Disponível em: <http://www.denunciar.org.br/wiki/bin/view/safernet/webhome>. Acesso em: 17 mar. 2014.

É o caso do crime de invasão de dispositivo informático, cujo o bem jurídico protegido é a inviolabilidade de informações e de dados, como dispõe o artigo 154-A, do Código Penal, e será abordado separadamente a seguir.

Quanto aos diversos outros crimes já tipificados e que são exercidos, constantemente, mediante o uso de equipamentos computadorizados, são denominados como impróprio, tendo em vista que a aparelhagem informática serve apenas como meio e não como fim pretendido pelo agente. Trata-se de crimes comuns cujas mudanças residem no *modi operandi*.

Esclarece o professor Tulio Vianna que estes tipos são os mais comuns, sendo executados por meio de equipamentos eletrônicos, inclusive conectados à *Internet*, em que a função da aparelhagem é meramente instrumental, não concretizando ofensa a novos bens jurídicos[39].

Essa categoria abrange a maioria dos ilícitos informáticos, considerando que, para sua execução, não se exige aprofundados conhecimentos técnicos na referida área, basta ter acesso a um computador para executá-los.

Dessa forma, com a intensificação do uso das redes sociais, o mero envio de mensagens em bate-papos, ou até um simples *e-mail*, podem significar a constituição de diversos delitos, como os contra a honra; a liberdade individual; o patrimônio; os costumes; dentre outros.

Por fim, os mistos são "derivados da invasão de dispositivo informático que ganharam *status* de *crimes sui generis*, dada a importância do bem jurídico protegido diverso da inviolabilidade dos dados informáticos"[40]; é o caso do acesso não autorizado ao Sistema de Informação Eleitoral, visando alterar a apuração da contagem dos votos, previsto no art. 72, I, da Lei nº 9.504/97.

Em algumas oportunidades, caracterizam-se como delito-meio que viabiliza um delito-fim não informático.

É o caso da invasão de dispositivo informático de uso particular para extrair dados bancários, como o número e senha de cartões de créditos, com posteriores compras indevidas pela *Internet*. Constitui-se, assim, tanto um delito informático próprio quanto um delito patrimonial, no qual apenas este recebe punição, em virtude do princípio da consunção.

---

[39] VIANNA; MACHADO, op. cit., 2013, p. 37-52.

[40] Ibidem, 2013, p. 34-35.

8 DOS CRIMES INFORMÁTICOS CONTRA A HONRA

A honra se reveste dos elementos morais, físicos e intelectuais do indivíduo, responsáveis por sua auto-estima e reputação, em que esta está relacionada com a honra objetiva e aquela com a subjetiva.

Nesse sentido, aduz Luiz Regis Prado que, do ponto de vista objetivo, "seria a reputação que o indivíduo desfruta em determinado meio social, a estima que lhe é conferida; subjetivamente, a honra seria o sentimento da própria dignidade ou decoro"[41].

Os crimes informáticos contra a honra, na qual se inclui a calúnia, a difamação e a injúria, previstos nos artigos 138, 139 e 140, do Código Penal, respectivamente, são crimes impróprios, que podem se dar por vários meios, incluindo o informático, por serem de forma livre.

A calúnia e a difamação atingem o caráter objetivo, enquanto a injúria atinge o subjetivo. São crimes formais, não necessitando que se obtenha o dano para que a consumação ocorra com o dano à reputação ou auto-estima do ofendido.

A conduta típica da calúnia consiste em imputar uma pessoa certa falsamente a prática de um fato criminoso, na qual a atribuição se faça mediante o conhecimento de sua não-veracidade[42].

Dessa forma, Marcelo Xavier exemplifica um crime de calúnia em meio informático: "dizer em um *chat*, espalhar *e-mails* ou publicar em redes sociais que determinada pessoa abusou sexualmente de outra ou que desviou quantias em dinheiro da empresa configuram a calúnia"[43].

No crime de difamação a conduta típica está em imputar a alguém fato ofensivo e desonroso à sua reputação, em que uma terceira pessoa, obrigatoriamente, toma conhecimento da ofensa[44].

Um famoso caso de difamação ocorreu em Sorocaba (SP), em que depois de descobrir que o marido a traía com a amiga, a esposa expôs, em uma rede social, a intimidade tanto do ex-marido quanto da suposta amante, atribuindo diversas ofensas a ambos. A acusada foi condenada a pagar R$ 67.000,00 (sessenta e sete mil reais) de indenização a esta, conforme decisão do Tribunal de Justiça de São Paulo[45].

---

[41] PRADO, Luiz Regis. Curso de direito penal brasileiro: parte especial: arts. 121 a 249. 7. ed. São Paulo: Revista dos Tribunais, 2008, p. 212-213.

[42] Ibidem, 2008, p. 212-213.

[43] CRESPO, op. cit., 2011, p. 90.

[44] PRADO, op. cit., 2008, p. 224-225.

[45] Mulher que expôs traição na internet é condenada a indenizar amiga em R$ 67 mil. Estadão Conteúdo. Disponível em: <http://noticias.uol.com.br/ultimas-noticias/agencia-estado/2013/02/07/mulher-que-expos-traicao-na-internet-e-condenada.htm>. Acesso em: 13 abr. 2014.

Por fim, quanto ao crime de injúria, Regis Prado leciona como a principal característica "a exteriorização do desprezo e desrespeito, ou seja, consiste em um juízo de valor negativo, apto a ofender o sentimento de dignidade da vítima"[46].

Neste caso, é corriqueiro presenciar em âmbito informático crimes dessa espécie, nos quais um usuário ofende a honra subjetiva de outro por meio de xingamentos, muitas vezes praticados com o envio de mensagens virtuais privadas ou expostas a terceiros.

É o que ocorreu com o aplicativo de celular chamado "*Tubby*", criado para homens avaliarem o comportamento e o desempenho sexual de mulheres, atribuindo-lhes classificações. O uso do aplicativo no Brasil, apesar do pouco tempo que ficou disponível no mercado virtual para *download*, foi proibido pela 15ª Vara Criminal de Belo Horizonte[47].

9 DOS CRIMES INFORMÁTICOS CONTRA O PATRIMÔNIO

Os crimes contra o patrimônio, como já exposto, representam juntamente com os crimes contra a honra, grande parcela das condutas ilícitas cometidas por meio de sistemas computadorizados, sendo os principais o furto e o estelionato, previstos nos artigos 155 e 171, do Código Penal, respectivamente.

Através do anonimato, o meio ambiente informático se tornou um potencial para o exercício dos referidos delitos.

O estelionato, segundo Regis Prado, apresenta elementos como a vantagem ilícita, o emprego de meio fraudulento, o erro causado ou mantido por esse meio, o nexo de causalidade entre o erro e a obtenção da vantagem e a lesão patrimonial[48].

Aliados aos mecanismos de ocultação de identificação, os agentes criminosos, visando a obtenção de vantagem patrimonial, disseminam vírus em *e-mails* e demais meios virtuais, com mensagens falsas para conquistarem dados pessoais e financeiros das vítimas, denominado de *pishing scam*. Os delitos de estelionato cometidos por computadores são da categoria dos crimes impróprios. Exemplificando, Fernando José da Costa leciona que

---

[46] PRADO, op. cit., 2008, p. 232-233.

[47] GOMES, Helton Simões. Justiça proíbe no Brasil app 'Tubby', em que homens avaliam mulheres. G1. Disponível em: <http://g1.globo.com/tecnologia/tem-um-aplicativo/noticia/2013/12/justica-proibe-no-brasil-app-tubby-para-homens-avaliarem-mulheres.html>. Acesso em: 22 jun. 2014.

[48] PRADO, op. cit., 2008, p. 442-443.

> A vítima, no instante em que clica a mensagem fraudulenta, inicia a instalação de um programa malicioso, seguida de uma mensagem de erro. Em seguida são abertas páginas falsas de formulários para a coleta de informações da vítima. No próximo passo, quando o usuário acessar os *sites* bancários, estes serão substituídos para *sites* redirecionados, onde o infrator conhecedor dos dados e senhas pessoais do usuário poderá de qualquer lugar ligado à *internet*, acessar sua conta bancária e efetuar operações financeiras como se fosse usuário. Se, exemplificando, utilizasse um usuário falso ou de outrem ou acessasse a rede através dos denominados sítios de acesso anônimo, as chances de ser identificado seriam mínimas[49].

Assim, é preciso que o usuário confie em determinada informação fraudulenta, acessando-a para, então, em ato contínuo dos agentes criminosos, ter seu patrimônio lesado.

Em relação aos crimes informáticos de furto, geralmente são de caráter misto, em que ocorre a invasão de dispositivo informático para posterior subtração de dados computadorizados ou mesmo informações das vítimas, sendo praticados geralmente por meio de programas maliciosos, como *trojans*[50], popularmente conhecidos por "cavalos de tróia".

10 DO CRIME DE INVASÃO DE DISPOSITIVO INFORMÁTICO ALHEIO

No dia 30 de novembro de 2012, a presidente Dilma Rousseff sancionou as primeiras Leis, nº. 12.737/2012 e nº. 12.735/2012, que incluem modalidades de delitos informáticos próprios, entrando em vigor dia 02 de abril de 2013.

A Lei 12.737/2012, conhecida popularmente como "Lei Carolina Dieckmann", surgiu após fotos íntimas desta atriz terem sido subtraídas, pelo técnico de manutenção de seu computador e, posteriormente, sofrido o delito de extorsão.

Com a referida Lei, acrescentaram-se ao Código Penal os artigos 154-A e 154-B, estipulando um novo tipo penal denominado de "invasão de dispositivo informático". Foram modificados, também, os §§ 1° e 2°, do artigo 266, que estabelecem como crime a conduta de interromper serviço telemático ou de informação de

[49] DA COSTA, Fernando José. Locus Delicti nos Crimes Informáticos. Tese (Doutorado) - Faculdade de Direito da Universidade de São Paulo (USP), São Paulo, p. 100.

[50] Trata-se de um *malware* (programa malicioso) que se instala no dispositivo computadorizado da vítima, captando informações e enviando-as para o agente criminoso.

utilidade pública. Do mesmo modo, o artigo 298 foi destinado a estabelecer como crime a configuração de falsidade de documentos particulares.

O bem jurídico penalmente tutelado foi a inviolabilidade dos dados informáticos, que é corolário do direito à vida privada e à intimidade, previsto no artigo 5, inc. X, da Constituição Federal.

Por essa razão, Vianna destaca que a inviolabilidade abrange tanto o direito à privacidade e intimidade, como à integridade destes contra sua destruição ou alteração[51].

Com efeito, Alexandre de Moraes entende que os direitos à intimidade e à vida privada se distinguem, já que o primeiro está relacionado com as relações subjetivas e de trato íntimo do indivíduo, como suas relações familiares e de amizades, enquanto o segundo constitui os demais relacionamentos humanos, principalmente os de foro objetivo, como as relações comerciais, de trabalho, de estudos, entre outros[52]. Marmelstein esclarece que inseridas nesses valores há inúmeras questões de caráter individual-subjetivo, em que nem o Estado, nem a sociedade podem interferir, como acerca do direito de não ser bisbilhotado, o direito de integridade à vida íntima e familiar, de igual modo, o respeito aos detalhes pessoais, imagem ou nome de cada indivíduo[53].

Assim, proteger o bem jurídico da inviolabilidade dos dados informáticos é efetivar os deveres estatais de respeito e de proteção perante os direitos fundamentais da intimidade e privacidade de cada indivíduo. É, de igual forma, assegurar a integralidade da segurança informática.

Verifica-se que o sujeito ativo deste tipo de delito pode ser qualquer pessoa humana não autorizada a acessar determinados dados, excetuando o proprietário do dispositivo computadorizado, tendo em vista ao redigir a expressão "invadir dispositivo informático alheio" o legislador excluiu a tipicidade das condutas de quem invade dispositivo informático próprio[54].

A partir do artigo 154-A, que estabelece que

> 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.

[51] VIANNA; MACHADO, op. cit., 2013, p. 94.

[52] MORAES, Alexandre de. Direito constitucional. 23. ed. São Paulo: Atlas, 2008, p. 53.

[53] MARMELSTEIN, George. Curso de direitos fundamentais. São Paulo: Atlas, 2011, p. 138-140.

[54] VIANNA; MACHADO, op. cit., 2013, p. 94.

Criar e divulgar programas de computadores com a finalidade de obter, adulterar e destruir dados ou informações, como os vírus e os *trojans*, passaram a se tipificar como um novo delito. Nesse caso, há a violação tanto do elemento da confidencialidade quanto da integralidade, presentes na segurança informática.

Quanto à confidencialidade, ao se invadir um dispositivo informático alheio, sem a autorização do titular do dispositivo, ocorre a quebra da garantia de que a informação, individualizada e particular, armazenada em determinado aparato informático, seja preservada em sigilo.

Já a integralidade, desconstitui-se quando há, com o auxílio da invasão, a alteração ou mesmo a destruição de dados ou informações contidas no computador ou em "nuvens de armazenamento"[55].

Além disso, a modificação nos §§ 1° e 2°, do artigo 266, também incluiu outras condutas ilícitas, como "derrubar"/interromper ou perturbar *sites*, seja de utilidade pública ou mesmo de uso particular, conforme dispõe seu texto:

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa.
>
> §1° Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
>
> §2° Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

Desse modo, para a tipificação do artigo 266 é necessária a lesão ao elemento da disponibilidade da segurança informática, isto é, tornar o serviço indisponível para acesso ou prejudicar o seu regular uso, seja por meio de vírus que deixam o servidor de hospedagem sobrecarregado, seja em decorrência de ataques de "computadores *zoombies*"[56], também conhecidos por "*botnets*"[57].

Logo, a criação da Lei nº 12.737/12 foi uma evolução de nossa legislação pátria, pois visou tornar ainda mais eficaz nosso ordenamento jurídico, que já con-

[55] PRASS, Ronaldo. Tira-dúvidas: conheça serviços para armazenar arquivos na 'nuvem'. G1. Disponível em: <g1.globo.com/tecnologia/noticia/2011/11/tira-duvidas-conheca-servicos-para-armazenar-arquivos-na-nuvem.html>. Acesso em: 28 jul. 2014.

[56] Tratam-se de computadores infectados por *malwares*, nos quais são controlados por algum agente para acessarem simultaneamente determinado sítio eletrônico, sobrecarregando-o e até mesmo interrompendo seus serviços devido à sobrecarga no sistema.

[57] Botnets infectam milhões de máquinas diariamente. Decision Report. Disponível em: <www.decisionreport.com.br/publique/cgi/cgilua.exe/sys/start.htm?infoid=17046&sid=41>. Acesso em: 28 jun. 2014.

templava sua abordagem em âmbito cível, e agora trouxe também para o criminal, no tocante às infrações praticadas em ambiente informático.

11 CONSIDERAÇÕES FINAIS

Ante ao exposto, o computador adveio da necessidade básica do ser humano: potencializar sua capacidade e extensão comunicativa. Os anos 60 foram o berço do marco tecnológico acerca da *Internet*. Embora seu surgimento seja pautado em decorrência de conflitos militares, sua propagação ao meio acadêmico e doméstico modificou as relações sociais, econômicas, culturais, financeiras, ou qualquer outra que envolva a pessoa, seja humana, seja jurídica.

Com o acesso amplamente difundido a qualquer interessado, os computadores conectados à Grande Rede se revestiram como um meio de se exercitar o lazer, o aprendizado, o comércio, o contato interpessoal, e até mesmo a prática de diversos ilícitos, sendo alguns ainda desconhecidos ou pouco explorados pelo ordenamento jurídico.

Para se obter o controle, tanto repressivo quanto preventivo, desenvolveu-se a Segurança da Informação, que é constituída por três conteúdos e que são de fundamental relevância na caracterização dos crimes informáticos, uma vez que violados alguns desses elementos, há a tipificação de um crime dessa espécie.

Conclui-se que, para a abordagem desses ilícitos, primeiramente houve a necessidade de se estabelecer o meio ambiente informático, sendo caracterizado como um direito fundamental, assim como ocorre com o natural, o artificial, o da cultura e do trabalho, merecendo igual respaldo jurídico e constitucional. No que tange ao caráter dos direitos fundamentais, o Estado e a sociedade deverão garantir, por meio de medidas concretas e eficazes, o respeito, a proteção e a promoção do meio ambiente informático.

Para tanto, delimitou-se o *nomen juris* de crimes informáticos, eis que o termo "informático" engloba tanto os aspectos e conteúdos da Informática, Telemática, quanto o bem jurídico dos crimes próprios, que é o foco deste trabalho: a violação de dados computadorizados.

Além disso, estabeleceu-se o conceito dos mesmos como conduta típica, antijurídica, antiética e culpável cometida contra ou pela utilização de procedimentos

automáticos de dados ou sua transmissão, com a lesão às propriedades da Segurança da Informação.

Do mesmo modo, sua classificação se fundamentou, através dos estudos doutrinários em três divisões: os próprios, que ofendem o computador ou dados nele armazenados, destacando-se os contra a inviolabilidade de dados, de telecomunicações, além do bom funcionamento dos sistemas operados eletronicamente, como sítios virtuais (*sites*), *hardware*, *software*, dentre outros; os impróprios, que são crimes já amparados pelo Direito Penal, embora sejam executados por um novo *modi operandi*; e os mistos, nos quais estão presentes tanto as características dos delitos próprios quanto impróprios.

Dessa forma, foi possível destacar os crimes informáticos com maior relevância, como os contra honra, que já são tipificados e ofendem a honra subjetiva e objetiva de algum indivíduo; os patrimoniais, como o furto e o estelionato, nos quais ganharam maior atenção estatal devido à sua parcela nas incidências desses ilícitos; e o de invasão de dispositivo informático alheio, regulamentado pela Lei nº. 12.737/2012, que lesa o bem jurídico da inviolabilidade das informações e dados computadorizados.

Cabe ao legislador penal tipificar os ilícitos decorrentes das tecnologias informáticas, como também selecionar os bens jurídicos emergidos dessa mutável realidade, já que os mesmos também podem ser objeto da tutela cível através da conversão do ato ilícito em perdas e danos.

Assim, apesar da legislação pátria não acompanhar, em mesmo ritmo, as necessidades e realidades sociais, o Direito, por hora, está conseguindo suprir as demandas judiciais, mas há evidente necessidade de se criar novas normas tanto acerca dos crimes informáticos quanto ao ambiente digital.

REFERÊNCIAS

BITENCOURT, Cezar Roberto. **Tratado de direito penal**: parte geral. 16. ed. São Paulo: Saraiva, 2011.

BONAVIDES, Paulo. **Curso de direito constitucional**. 12. ed. São Paulo: Malheiros, 2005.

BRASIL, Agência Nacional de Telecomunicações. **Norma 004/95**: Uso de meios da rede pública de telecomunicações para acesso à internet. Disponível em: <http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=10283&assuntoPublicacao=Norma%20MC%20n%BA%20004/1995&caminhoRel=null&filtro=1&documentoPath=biblioteca/Normas/Normas_MC/norma_004_95.htm>. Acesso em: 03 jul. 2014.

BRASIL. Ministério Público Federal. **Convenção sobre o Cibercrime**. Disponível em: <http://ascji.pgr.mpf.gov.br/informes-e-documentos/documentos/docs_documentos/convencao_cibercrime.pdf>. Acesso em: 19 mar. 2013.

BRIGGS, Asa; BURKE, Peter. **Uma história social da mídia**: de Gutenberg à Internet. Tradução: DIAS, Maria Carmelita Pádua. 2. ed. Rio de Janeiro: Jorge Zahar Editor, 2006.

BRITO, Auriney. **Direito penal informático**. São Paulo: Saraiva, 2013.

CANOTILHO, José Joaquim Gomes. **Protecção do ambiente e direito de propriedade**: (crítica de jurisprudência ambiental). Coimbra: Coimbra, 1995.

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

CRUZ, Danielle da Rocha. **Criminalidade informática**: tipificação penal das condutas ilícitas realizadas com cartões de crédito. Rio de Janeiro: Forense, 2006.

DA COSTA, Fernando José. **Locus delicti nos crimes informáticos**. Tese (Doutorado) - Faculdade de Direito da Universidade de São Paulo (USP), São Paulo.

FERREIRA, Érica Lourenço de Lima. **Internet**: macrocriminalidade e jurisdição internacional. Curitiba: Juruá, 2007.

FERREIRA, Ivette Senise. A criminalidade informática. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). **Direito & internet**: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2008. v. 2.

FIORILLO, Celso Antonio Pacheco. **Curso de direito ambiental brasileiro**. 5.ed. São Paulo: Saraiva, 2004.

GOMES, Helton Simões. Justiça proíbe no Brasil app 'Tubby', em que homens avaliam mulheres. **G1**. Disponível em: <http://g1.globo.com/tecnologia/tem-um-aplicativo/noticia/2013/12/justica-proibe-no-brasil-app-tubby-para-homens-avaliarem-mulheres.html>. Acesso em: 22 jun. 2014.

GOMES, Luiz Flávio; MOLINA, Antonio García-Pablos de. **Criminologia**: introdução a seus fundamentos teóricos - introdução às bases criminológicas da lei 9.099/95, lei dos juizados especiais criminais. São Paulo: Revista dos Tribunais, 2008.

ALEXANDRIA, João Carlos Soares de. **Gestão da segurança da informação:** uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica. 193f. Tese (Doutorado em Ciência na Área de Tecnologia Nuclear) Instituto de Pesquisas Energéticas e Nucleares (USP), São Paulo.

MARMELSTEIN, George. **Curso de direitos fundamentais**. 3. ed. São Paulo: Atlas, 2011.

MORAES, Alexandre de. **Direito constitucional**. 23. ed. São Paulo: Atlas, 2008.

NASCIMENTO, Amauri Mascaro. **Curso de direito do trabalho**: história e teoria geral do direito do trabalho: relações individuais e coletivas do trabalho. 26. ed. São Paulo: Saraiva: 2011.

PRADO, Luiz Regis. **Curso de direito penal brasileiro**: parte geral. 7. ed. São Paulo: Revista dos Tribunais, 2008a. v. 1.

PRADO, Luiz Regis. **Curso de direito penal brasileiro**: parte especial: arts. 121 a 249. 7. ed. São Paulo: Revista dos Tribunais, 2008b. v.2.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. **Jus Navigandi**, Teresina, v. 6, n. 58, ago. 2002. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/13024-13025-1-PB.pdf>. Acesso em: 21 jun. 2014.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

ROXIN, Claus. Reflexões sobre a construção sistemática do direito penal. **Revista Brasileira de Ciências Criminais,** São Paulo, n. 82, a.18, p. 24-47, jan./fev. 2010.

SÁNCHES, Jesús-Maria Silva. **A expansão do direito penal**: aspectos da política criminal nas sociedades pós-industriais. São Paulo: Revista dos Tribunais, 2002. v. 11.

SHECARIA, Sérgio Salomão. **Criminologia**. 2. ed. São Paulo: Revista dos Tribunais, 2008.

SILVA, José Afonso da. **Direito ambiental constitucional**. 4. ed. São Paulo: Malheiros, 2003.

SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**. São Paulo: Revista dos Tribunais, 2003.

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. São Paulo: Saraiva, 2013.

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

VIANNA, Túlio Lima; MACHADO, Felipe Daniel Amorim. **Crimes informáticos**: conforme a Lei n. 12.737/2012. Belo Horizonte: Fórum, 2013.

Recebido em: 16 de setembro de 2014
Aceito em: 09 de dezembro de 2014