FACULDADE DE DIREITO DE CACHOEIRO DE ITAPEMIRIM

SUELEM MARTINS DIOGO

CRIMES DIGITAIS: AS AMEAÇAS VIRTUAIS E O DESAFIO DA LEGISLAÇÃO BRASILEIRA PARA CRIMINALIZAR OS DELITOS DA INTERNET

CACHOEIRO DE ITAPEMIRIM/ES
2017

SUELEM MARTINS DIOGO

CRIMES DIGITAIS: AS AMEAÇAS VIRTUAIS E O DESAFIO DA LEGISLAÇÃO BRASILEIRA PARA CRIMINALIZAR OS DELITOS DA INTERNET

Monografia Jurídica apresentada ao curso de Direito da Faculdade de Direito de Cachoeiro de Itapemirim como requisito parcial para obtenção do titulo de Bacharel em Direito.
Orientador: Izaias C. B. Junior

CACHOEIRO DE ITAPEMIRIM/ES
2017

SUELEM MARTINS DIOGO

CRIMES DIGITAIS: AS AMEAÇAS VIRTUAIS E O DESAFIO DA LEGISLAÇÃO BRASILEIRA PARA CRIMINALIZAR OS DELITOS DA INTERNET

Monografia Jurídica apresentada ao curso de Direito da Faculdade de Direito de Cachoeiro de Itapemirim como requisito parcial para obtenção do titulo de Bacharel em Direito.

Aprovada em _____ de _____ de 2017.

BANCA EXAMINADORA

_____
Prof. Orientador. Izaías Corrêa Barbosa Junior
Faculdade de Direito de Cachoeiro de Itapemirim-FDCI

_____
Prof. Examinador
Instituição de ensino

_____
Prof. Examinador
Instituição de ensino

Aos que, direta ou indiretamente, se dispuseram a me ajudar na realização de mais uma etapa importante de minha qualificação profissional.

A Deus, pela presença constante que me alimentou com a serenidade necessária para compreender, entre as alegrias, tristezas e lutas, que existe a realização de um ideal que nos permite crescer diante da vida. A minha família, em especial aos meus pais, Olívio e Sônia e ao meu namorado Tiago, pelo apoio incessante e compreensão dos dolorosos, mas necessários momentos de ausência.

“A lei é inteligência, e sua função natural é impor o procedimento correto e proibir a má ação”.

Cícero

DIOGO, Suelem Martins. **CRIMES DIGITAIS: AS AMEAÇAS VIRTUAIS E O DESAFIO DA LEGISLAÇÃO BRASILEIRA PARA CRIMINALIZAR OS DELITOS DA INTERNET**. Monografia (Bacharelada em Direito). Faculdade de Direito de Cachoeiro de Itapemirim-FDCI: Cachoeiro de Itapemirim, 2017.

RESUMO

O avanço da tecnologia da informática se deu em um espaço de tempo muito curto. Suas utilidades mais diversas têm sido aproveitadas em praticamente todos os ramos da economia mundial para melhorarem não somente a comodidade das pessoas, mas, também, as relações comerciais entre elas e as empresas, potencializando a níveis muito grandes o mercado globalizado. Devido ao avanço da tecnologia digital, a realização de compras, pagamentos, transferências e, inclusive, a transmissão de um volume de dados muito grande, e em tempo real, através do chamado cyber espaço. Entretanto, junto com todo esse avanço tecnológico e toda a comodidade que esses fatores podem nos trazer, veio também o perigo dos crimes digitais. Pessoas que se valem do espaço digital da rede mundial de computadores (internet) para materializarem no universo da informática, os crimes já dispostos no Código Penal Brasileiro e outros que a legislação ainda encontra dificuldade de tipificação. Assim este trabalho monográfico vem analisar aspectos históricos e conceitos do mundo virtual, assim como das ameaças que lhe são inerentes, e ainda trazer a tona a atual legislação brasileira acerca dos crimes virtuais e os desafios enfrentados no universo jurídico brasileiro diante da necessidade de se criar normas eficazes para coibição dessas práticas delituosas, como, por exemplo, faz as leis 12.735/2012 e 12.737/2012. Diante disso, se faz necessário uma revisão na metodologia utilizada para prevenir, combater e até mesmo punir esses delitos digitais que aí estão e, infelizmente, vieram para ficar.

Palavras-Chave: crimes digitais. Espaço digital. legislação brasileira. tipificação.

DIOGO, Suelem Martins. **CRIMES DIGITAIS: AS AMEAÇAS VIRTUAIS E O DESAFIO DA LEGISLAÇÃO BRASILEIRA PARA CRIMINALIZAR OS DELITOS DA INTERNET**. Monografia (Bacharelada em Direito). Faculdade de Direito de Cachoeiro de Itapemirim-FDCI: Cachoeiro de Itapemirim, 2017.

RESUMO EM LINGUA ESTRANGEIRA

The advancement of computer technology took place in a very short space of time. Its most diverse uses have been used in almost every branch of the world economy to improve not only the comfort of people, but also the commercial relations between them and companies, boosting the globalized market to a very great extent. Due to the advancement of digital technology, the making of purchases, payments, transfers and even the transmission of a very large volume of data, and in real time, through the so-called cyber space. However, along with all this technological advancement and all the comfort that these factors can bring us, also came the danger of digital crimes. People who use the digital space of the world wide web to materialize in the universe of computer science, crimes already disposed in the Brazilian Penal Code and others that the legislation still finds difficulty in typing. Thus, this monographic work examines historical aspects and concepts of the virtual world, as well as the threats that are inherent to it, and also to bring to light the current Brazilian legislation on virtual crimes and the challenges faced in the Brazilian legal universe in view of the need to create Effective rules to curb these criminal practices, such as Law 12,735 / 2012 and Law 12,737 / 2012. Given this, it is necessary to review the methodology used to prevent, combat and even punish these digital crimes that are there and, unfortunately, have come to stay.

Keywords: digital crimes. Digital space. Brazilian legislation. Typification.

SUMÁRIO

1 INTRODUÇÃO

O início da década de 90 foi marcado, dentre outras coisas, pela popularização do uso do computador, o que trouxe ao mercado mundial uma nova realidade e a necessidade de se conviver com esse elemento que invadia nossas casas, bancos, escolas, lojas, shoppings, etc.

O desenvolvimento abrupto da internet fez com que uma nova realidade se desenvolvesse: o comércio digital. Um volume imenso de dinheiro tem sido direcionado para as negociações na esfera digital que cresceu assustadoramente tornando-se um campo mais do que promissor, básico, nas relações econômicas e sociais. Entretanto, juntamente com essa nova era mundial também surgiram indivíduos oportunistas e criminosos que se valem da facilidade de interação proporcionada pela internet para o cometimento de delitos ainda não previstos na legislação e que envolvem o mundo virtual.

O sucesso das relações comerciais realizadas tem atraído a atenção de criminosos que se valem da tecnologia para cometer ações desonestas no intuito de lesar o patrimônio alheio. Através da captura de dados pessoais, de anúncios mentirosos, milhares de usuários, empresas, provedores, bancos e investidores seriam enganados e lesados por pessoas com atitudes criminosas que usariam a tecnologia da informática para cometerem crimes comuns.

Isso nos remete a preocupação com a segurança contra esse tipo de crime que passou a ser uma realidade que precisa ser encarada com seriedade, pois, atualmente, é praticamente impossível ter um computador sem estar conectado à internet, pelo fato dela já ter se tornado um dos maiores meios de divulgação e fonte de pesquisas e auxílio do homem na busca por informações e troca, transmissão e aquisição de informações e dados em tempo real.

Nesse ínterim, programas têm surgido como uma ameaça real no intuito de sabotar programas e arquivos, além de sequestrar formações sigilosas de pessoas físicas e jurídicas, se enquadrando na maioria das vezes em alguma espécie de crime digital. Basta um simples e-mail falso de um Banco, onde o usuário deve entrar com o número da sua conta e suas senhas com promessas de se ganhar uma viagem, por exemplo, para que seus dados sejam enviados para um *cyber-criminoso* e o estrago estará feito.

A evolução do mundo virtual é uma realidade e traz inúmeros benefícios para a humanidade, envolvendo pessoas de todas as classes sociais, além dos setores público e privado. Contudo, é preciso que estejamos sempre alerta e jamais deixemos de lado a questão da segurança, pois, embora a evolução e os avanços tecnológicos da informática tenham sido

muito grandes, ainda assim, não se conseguiu impedir os crescentes aumentos dos índices de crimes digitais.

Nesse sentido, um dos maiores desafios da legislação brasileira é justamente a criação de tipos penais que ainda não estejam previstos na legislação e envolvam o mundo virtual, uma vez que não é permitida pela legislação, no Direito Penal, a utilização de analogia em relação às tipificações já existentes.

2 AS TRAMAS DA PESQUISA

2.1 A delimitação do marco teórico

Em seus registros Wendt & Jorge (2012) lembram a primeira conexão internacional da ARPANET realizada em 1973 que interligou a Inglaterra e a Noruega e acabou por substituir seu protocolo de comutação de pacotes (Protocolo de Controle de Rede - *Network Control Protocol* - NCP) para o Protocolo de Controle de Transmissão/Protocolo de Interconexão (*Transmission Control Protocol/Internet Protocol* - TCP/IP), uma linguagem básica de comunicação ou protocolo da rede mundial de computadores, que tardiamente se tornaria o protocolo de transmissão de dados pela internet atual. Tratava-se de um conjunto de camadas responsáveis por determinadas tarefas como, por exemplo, a comunicação entre o servidor de internet e computador local, baseada na configuração TCP/IP.

Uma década a frente a ARPANET passa a ser chamada de internet com a criação da rede mundial (*World Wide Web* - WWW) um conjunto de documentos em hipermídia da Linguagem de Marcação de Hipertexto (*HyperText Markup Language* - HTML), uma linguagem para a produção de páginas de internet, visualizados através de programas de computador chamados *browsers* (para navegação pela internet, como o *Internet Explorer* ou o *Firefox*). Tal evolução trouxe como grande vantagem à melhoria na interface gráfica tornando-se bem mais atraente aos usuários e permitindo a interação com figuras e sons (POLEGATTI & KAZMIERCZAK, 2012).

A partir de então, a Internet passa a ser composta de aproximadamente 50.000 redes internacionais, sendo que mais ou menos a metade delas nos Estados Unidos. Monteiro Neto (2008) lembra ressalta que a partir de julho de 1995, havia mais de 6 milhões de computadores permanentemente conectados à Internet, além de muitos sistemas portáteis e de desktop que ficavam on-line por apenas alguns momentos. Trata-se já do início da chamada revolução tecnológica que evidenciou a importância e o papel da informação no meio virtual que passa a categoria de bem jurídico importante nos meios informáticos.

Monteiro Neto (2008) destaca que a sociedade da informação – que se destaca a partir da facilitação no desempenho de atividades cotidianas proporcionadas pelo uso de ferramentas informatizadas – possui a mecanismos eletrônicos para guardar e proteger bens jurídicos de suma importância para o ser humano como, por exemplo, a saúde, intimidade,

segurança, liberdade entre muitos outros numa sociedade, agora, vinculada às tecnologias da informação.

No entanto, disserta Oliveira (2013) a criminalidade também acompanha essa evolução social e avança sobre tais bens jurídicos com seus crimes virtuais, que passa a depender da ordem constitucional para sua proteção na esfera penal, de forma que, tais condutas criminosas não permaneçam sem regulamentação e o mundo virtual se afaste da designação de mundo sem leis que ainda possui.

Não há o que se questionar acerca da eficácia da internet como um dos meios mais eficazes para celebração de contratos, destaca Vedovate (2005). Hoje são milhares de contratos fechados por essa via, de forma que obedecem aos princípios da publicidade, vinculação, veracidade, não-abusividade, dentre outros. A inexistência de normatização especifica no ordenamento jurídico brasileiro sobre os contratos realizados sob essa égide, ainda é uma realidade embora o Código Civil e o Código de Defesa do Consumidor sanam, pelo menos em parte, os conflitos atinentes a respeito desse tema, faltando uma norma específica que assegure os asseios da comunidade virtual (VEDOVATE, 2005).

2.2 O objeto e o problema da pesquisa

Como objetivo deste trabalho monográfico, temos a oportunidade de analisar aspectos históricos e conceitos ligados à internet e suas ameaças, além do desafio da atual legislação brasileira em relação aos crimes virtuais.

No caso do problema de pesquisa, tratam-se os crimes digitais e suas ameaças virtuais um grande desafio para o ordenamento jurídico brasileiro que ainda persegue o objetivo de criminalizar os delitos ocorridos na internet, cujas condutas ainda se encontram sem a devida regulamentação, pelo menos em sua grande maioria, o que da margem a autores como Basso & Almeida (2007) a usarem a expressão “mundo sem leis" para o universo digital por entenderem que em vários casos uma nova regulamentação ainda é necessária para se ter mais segurança no emprego das ferramentas eletrônicas e maior certeza quanto a validade e eficácia das transações celebradas por meio eletrônico.

Para Monteiro Neto (2008) as condutas ilícitas cada vez mais numerosas praticadas através do ambiente informático vem prejudicando a manutenção dos níveis mínimos de segurança e credibilidade necessários a qualquer negócio jurídico. E mais, elas acabam por

interferir diretamente no cotidiano de muitas pessoas tornando inapto o ambiente virtual para o estabelecimento ou manutenção de relações sociais.

Dessa forma até onde vai a eficácia do conjunto reduzido de normas existentes no ordenamento jurídico brasileiro, para fiscalizar e punir as condutas ilícitas que ocorrem no mundo virtual e que são cometidos no universo brasileiro dentro da rede mundial de computadores?

2.3 A base metodológica

A metodologia dedica-se a reconstruir teorias, conceitos, idéias, ideologias, polêmicas, tendo em vista aprimorar fundamentos teóricos no sentido de reconstruir teorias, quadros de referência, condições explicativas da realidade, polêmicas e discussões pertinentes ao assunto abordado (DEMO, 2000).

Realizou-se neste estudo uma revisão integrativa da literatura, ou seja, aquela em que as pesquisas já publicadas são sintetizadas e geram conclusões sobre o tema em estudo, cuja elaboração compreende as etapas de seleção das hipóteses ou questões, definição dos critérios para seleção da amostra, definição das características da pesquisa original, análise de dados, interpretação dos resultados e apresentação da referência.

A questão condutora desta pesquisa foi dissertar sobre o universo dos crimes digitais, as ameaças virtuais e o desafio da legislação brasileira para criminalizar os delitos da internet, onde, para a construção do conteúdo desenvolvido neste trabalho, foram realizadas pesquisas bibliográficas, de cunho qualitativo, tendo como fonte principal livros com autores do porte de Monteiro Neto (2008), Oliveira (2013) e Polegatti & Kazmierczak (2012) dentre outros grandes nomes da área que me oportunizaram os conceito, caminhos e a busca pela qualificação dentro dessa área.

3 OS CRIMES DIGITAIS: TIPOS E CARACTERÍSTICAS

Crime digital engloba todo o sistema de informática e não apenas a internet. É o crime no qual computadores é instrumento direto e expressivo na prática do mesmo. É a conduta ofensiva e danosa que pode violar ou prejudicar tanto a sociedade, quanto a uma pessoa.

Segundo Aras (2001), para a OECD – *Organization for Economic Cooperation and Development*, o crime de computador é "qualquer comportamento ilegal, antiético ou não autorizado envolvendo processamento automático de dados e, ou transmissão de dados", podendo implicar a manipulação de dados ou informações, a falsificação de programas, a sabotagem eletrônica, a espionagem virtual, a pirataria de programas, o acesso e/ou o uso não autorizado de computadores e redes.

Na visão de Wend & Jorge (2012) práticas criminosas cometidas através do computador se dividem em crimes virtuais e ações prejudiciais consideradas atípicas - por causarem algum tipo de transtorno para a vítima, embora para esta não exista uma previsão legal e o causador possa ser responsabilizado no âmbito civil somente, como nos casos de acesso não autorizado a redes de computadores. Já aqueles são subdivididos em abertos e exclusivamente cibernéticos:

> [...] os primeiros são os praticados tradicionalmente ou através de computadores (p. ex., os casos de crime contra a honra). Os segundos se dão somente por intermédio do computador ou qualquer outro recurso que permita o acesso à internet, como, por exemplo, casos de *carding* (clonagem de cartão) por meio de sistema de informática. (WENDT & JORGE, 2012, p. 18).

Rosa (2002) também disserta a respeito e partilha seu conceito de crime digital como sendo:

> [...] a conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. o 'Crime de Informática' é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o 'Crime de Informática' pressupõe does elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se *software* e *hardware*, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade

> individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc. (ROSA, 2002; p.52).

No entanto, independentemente do conceito que lhe é instituído, devido aos pontos de vista diferentes que vem tipificar o crime digital, a relevância se encontra no fato de que o instrumento utilizado será sempre o mesmo, o computador e o meio pelo qual o ato é praticado é a internet.

Os crimes digitais vêm se aperfeiçoando na velocidade que evolui a tecnologia. Organizações são invadidas e põem a confiabilidade das empresas em risco, causando, além de enormes prejuízos, ameaças tamanhas que são capazes de comprometer a estabilidade das organizações, podendo ser divididos em duas subclasses ou duas categorias, de crimes cibernéticos: o próprio e o impróprio.

Para Castro (2003), o próprio é aquele que não pode ser cometido fora do espaço cibernético, sem a utilização de computadores e sistema de informática para a disseminação de, por exemplo, códigos maliciosos e o acesso indevido (sem autorização) a dados pessoais ou do governo, aqueles que somente podem ser efetivados por intermédio de computadores ou sistemas de informática, sendo impraticável a realização da conduta por outros meios.

Em relação aos impróprios, Castro (2003) destaca que, nestes, sua prática é realizada seja com o uso de sistemas de informática e computadores ou mesmo por outros meios para a prática de, por exemplo, difamação, calúnia, dano mortal e racismo. O autor ainda cita ainda outra divisão, chamada de tripartida onde ressalta os seguintes conceitos:

> a) os crimes de informática puros, onde o agente objetiva atingir o computador, o sistema de informática ou os dados e as informações neles utilizadas; b) os crimes de informática mistos, onde o agente não visa o sistema de informática e seus componentes, mas a informática é instrumento indispensável para consumação da ação criminosa e c) os crimes de informática comuns, onde o agente não visa o sistema de informática e seus componentes, mas usa a informática como instrumento (não essencial, poderia ser outro o meio) de realização da ação (CASTRO, 2003; p.04).

No entanto essas classificações de conceitos acabam não tendo muita eficácia no ordenamento jurídico, pelo contrário, são utilizadas de forma didática uma vez que a dinâmica dos computadores, da rede mundial e dos delitos digitais cometidos evolui de forma tão rápida que tais definições acabam gradativamente se tornando obsoletas na esfera judicial, um ponto bem ressaltado por Crespo (2011) pela relevância que possui no âmbito social:

> Face à ausência de norma específica, impõe-se a aplicação da legislação existente, ou seja, o Código Penal e as Leis. Alguns fatos, porém, não se enquadram perfeitamente nos tipos penais em vigor, o que provoca a atipicidade e, consequentemente, a impunidade. Daí porque a sociedade aguarda, ansiosamente, a

> elaboração de lei tratando sobre a Informática e a Internet, não só no campo do Direito Penal, mas também na área do Direito Civil, Comercial, Tributário, etc. (CRESPO, 2011; p. 47).

Os avanços da tecnologia e o surgimento da internet propiciariam o aparecimento de novos tipos penais, como também novas fórmulas de praticar crimes já conhecidos. A informática passou a ser utilizada como instrumento para execução de antigos tipos penais. Nasceram, assim, os crimes de informática, conceituados como sendo aqueles praticados contra o sistema de informática ou através deste, incluindo-se o perpetrado através da internet, pois pressuposto para acessar a rede é a utilização de um computador.

> Por mais que pareça óbvio, é preciso afirmar que o Direito Penal e a Internet possuem interação, mesmo porque, o chamado cyberespaço e toda a sua cultura afetam de forma significativa as relações no mundo real, devendo, portanto, sujeitar-se ao Direito para disciplinar as condutas ali praticadas que, ao final, são mesmo relações entre os indivíduos (LIMA, 2005; p. 155).

Segundo Lima (2005), impõe-se a aplicação de direito nestes casos, embora a legislação sobre a informática seja bem escassa. Temos a Lei nº. 9.609/98, que dispõe sobre a proteção da propriedade intelectual de programa de computador e sua comercialização, e a Lei nº. 9.983/2000 que acrescentou alguns tipos ao Código Penal (arts. 153, § 1ºA; 313-A e 313-B). Na área do Direito Processual, a Lei nº. 9.800/99 permite às partes a utilização de sistema de transmissão de dados para a prática de atos processuais. , ainda, a Lei nº. 9.296/96, que prevê a interceptação de comunicações telefônicas e telemáticas.

Greco Filho (2000) defende que nos crimes praticados através da informática, ou seja, tipos antigos, nos quais o agente utiliza a informática como meio de execução, como instrumento de sua empreitada, não há dificuldades. O crime é o mesmo previsto em sua origem, a forma de sua execução é que se inovou, por exemplo, uma ameaça feita pessoalmente não se distingue na tipicidade de uma ameaça virtual.

No entanto, lembra Lima (2005), problemas surgem em relação aos crimes cometidos contra o sistema de informática, atingindo bens não tutelados pelo legislador, como dados, informações, hardware, sites, home pages, e-mails, etc., são condutas novas que se desenvolveram junto com a nossa sociedade, razão pela qual o legislador de 1940, época do Código Penal, não pode prever tais tipos penais.

> Com o advento da computação e, por conseguinte, o começo da era informática, produziu-se uma transformação profunda que, por suas características, em face da importância das mudanças socioculturais que a acompanha, o vertiginoso de seu desenvolvimento e sua significação econômica mundial, merece urgentemente um tratamento legislativo que contemple as novas problemáticas que se apresentam com esse fenômeno (LIMA, 2005, p. 156)

Para Lima (2005), encontramos solução quando o agente atinge os bens não descritos pelo Código Penal, destruindo-os total ou parcialmente, e com isso provoca prejuízos econômicos, podendo ser aplicado o tipo penal do dano (artigo 163 do Código Penal). Em relação à correspondência eletrônica (e-mail), a questão já passa a ser resolvida pela Lei nº. 9.296/96. Todavia, diversas condutas não se amoldam à legislação existente e, diante do princípio da reserva legal, não podem ser punidas. São exemplos: criação de vírus, sabotagem virtual, vandalismo virtual, acesso não autorizado, uso desautorizado de hardware, dentre muitas outras ações imorais e lesivas à informática, porém atípicas.

> Assim, devemos modificar a estrutura normativa vigente, que resulta incapaz de dar resposta aos novos desafios, sendo assim necessário incorporar a esse os elementos indispensáveis de informática e cibernética, permitindo-nos obter a segurança jurídica necessária para seguirmos realizando avanços significativos no novo contexto global, surto a partir desta verdadeira revolução tecnológica (LIMA, 2005, p. 157).

Em suas dissertações Lima (2005) cita a Carta Magna em seu art. 5º, XXXIX cujo conteúdo lembra-nos que "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal". Dessa forma, destaca o autor, fato é que se faz imperativo que, para se punir os crimes praticados no meio digital, é preciso que o tipo penal se adeque as normas já existentes, preenchendo, inclusive, as lacunas que por ventura ainda existam, devem ser preenchidas e ter incorporados os conceitos de informática à legislação vigente.

Rosa (2002) lembra que na década de 80 nosso legislativo deu inicio a construção de algumas providências sobre os crimes cometidos na esfera digital com instituição do Plano Nacional de Informática e Automação (Conin) - Lei nº 7.232/84 – que versa sobre as diretrizes no âmbito da informática em solo Brasileiro. Seguido a isso veio a Lei nº 7.646/87, revogada mais tarde pela Lei n. 9.609/98, considerada o primeiro ordenamento a tipificar as infrações de informática, em cujo artigo 12 elenca-se os seguintes delitos:

> Art. 12. Violar direitos de autor de programa de computador: Pena – Detenção de seis meses a dois anos ou multa. § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: Pena – Reclusão de um a quatro anos e multa. § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral. § 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo: I – quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público; II – quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo. § 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou

> contribuição social e qualquer acessório, processar-se-á independentemente de representação.

Dessa forma, é preciso que se acelerem os trabalhos legislativos com o intuito de se ver disciplinado não só novos tipos penais, como também outras áreas do Direito que sofreram impacto com a evolução digital.

> A internet é um caminho eficaz para diversos tipos de estelionato, lavagem de dinheiro, pornografia infantil, violações a direitos autorais, divulgações de informações sobre preparo de drogas, confecção de armas, propagandas ou comportamentos ilegais ou que violem direitos fundamentais, entre outras modalidades de crimes. Cabe, pois, criar mecanismos que assegurem uma investigação eficaz destes casos. O rastreamento das mensagens na internet, recurso importante para o esclarecimento de tais ocorrências seria facilitado se os computadores destinados a prover acesso e a trafegar mensagens da rede mantivessem registro regular e sistemático das suas atividades. A autoridade policial conseguiria, então, detectar, com maior frequência, a origem da mensagem relacionada à infração ou do programa causador de danos (CRESPO, 2011; p.204)

É certo também que a legislação existente pode ser aproveitada em muitos casos, não sendo necessário um novo código para tratar dos crimes de informática, o que é preciso é que sejam preenchidas as lacunas que atualmente existem, como afirma Lima (2005):

> Também assim, se incorporarmos a nosso ordenamento os conceitos em forma clara e ordenada, evitando modificar pontualmente a legislação na matéria, estaremos trabalhando com o compromisso e a habilidade necessários para esse novo empreendimento. A necessidade de incorporação dos conceitos de informática à legislação vigente não implica que devemos esquecer todo o nosso sistema e, fazendo rasa, começar desde o zero. Muito pelo contrário, nosso sistema legal se encontra atualmente desenhado para suportar sem maiores contratempos as modificações aludidas (LIMA, 2005, p. 157).

Dizem que as lacunas vêm prevalecendo nas decisões judiciais, o que pode até ocorrer em um ou outro caso concreto, mas os recursos e as ações de impugnações existem para socorrer e sanar tais situações. Greco Filho (2000) reforça que o Poder Judiciário precisa enfrentar estas questões com sabedoria e equidade, usando a modificação da legislação penal como arma para sancionara as condutas que atentam contra a segurança do sistema informático que hoje invade todas as áreas, e assim se solucionar os conflitos referentes à informática e Internet, fazendo prevalecer, por fim, a Justiça, pela qual todos nós lutamos.

4 A LEGISLAÇÃO MUNDIAL

A informática vem se desenvolvendo em todo o mundo e com ela multiplicam-se os crimes praticados com o auxílio do computador e da internet. Alguns países já possuem legislação específica sobre o tema, outros inseriram nos diplomas legais existentes modificações a fim de disciplinar esta nova modalidade de delitos.

Portugal, por exemplo, se encontra bem à frente de nosso país em matéria de legislação sobre crimes de informática. Em 1991, foi publicada a Lei nº. 109, dispondo sobre a criminalidade na informática. O Código Penal Português, Decreto Lei nº. 48/95, de 15 de março, também cuidou d assunto ao prever dois tipos penais relacionados à informática. O primeiro está inserido no capítulo reservado aos crimes contra a reserva da vida privada e refere-se à devassa por meio da informática. Já o segundo delito, incluído no capítulo destinado aos crimes contra o patrimônio em geral, dispões sobre a burla informática e nas comunicações.

> Art. 193º Devassa por meio de informática.
> Quem criar, mantiver ou utilizar ficheiro automatizado de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou à origem étnica, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.
> 1. A tentativa é punível.

Este tipo penal tutela os dados, mas não qualquer um. A lei protege apenas os referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada e à origem étnica. O crime é publico, não dependendo de queixa o participação do ofendido (art. 198 do Código Penal Português).

A Lei da criminalidade informática – Lei nº. 109/91, de 17 de agosto, além de definir alguns conceitos utilizados na informática como, por exemplo, o que seja rede de informática e sistema informático, tipifica alguns crimes.

Os conceitos de rede informática, sistema informático, programa informático, topografia, produto semicondutor, interceptação, valor elevado e valor consideravelmente elevado vêm expostos no artigo 2º deste diploma legal. Andou bem o legislador português ao traçar estas definições, pois a maioria dos profissionais de Direito não está acostumada com a nomenclatura específica da ciência da informática.

Aspecto que merece ressalva é o da responsabilidade penal das pessoas coletivas e equiparadas, sendo que esta só ocorrerá quando o crime for praticado e nome ou interesse da pessoa coletiva (art. 3º). As penas principais aplicáveis aos entes coletivos são: Admoestação,

Multa e Dissolução (artigo 10º) e as acessórias: Perda de bens, Caução de boa conduta, Interdição temporária do exercício de certas atividades ou profissões. Enceramento temporário do estabelecimento. Encerramento definitivo do estabelecimento e Publicidade da decisão condenatória (artigo 11º).

> Quanto aos delitos, previu o legislador português seis tipos penais: falsidade informática, danos relativos a dados ou programas informáticos, sabotagem informática, acesso ilegítimo, interceptação ilegítima e reprodução ilegítima de programa protegido (CASTRO, 2003; p. 158).

No caso da Itália, o Código Pena Italiano, tal qual o português, sofreu alterações nos últimos anos. A lei nº. 547, de 23 de dezembro de 1993, acrescentou quinze preceitos, incriminadores na área dos crimes de informática, com seis figuras essenciais: sabotagem, acesso ilegal, violação de segredo informático e do sigilo, falsificações, fraude informática e violação dos direitos do autor concernentes ao software.

> A sabotagem como ataque à funcionalidade do sistema informático é prevista em duas figuras distintas de crime de gravidade diversa, levando-se em conta o tipo de sistema atacado, se de utilidade pública, ou simplesmente de outrem. Em ambos os casos, o bem jurídico tutelado é a integridade física do sistema informático, sendo que, quando a ofensa se dirige ais sistemas de utilidade pública, aplica-se o artigo 420 e quando pertence a qualquer outra pessoa impõe-se a regra de um a quatro anos, no primeiro caso, e três meses a três anos, no último (CASTRO, 2003; p. 159).

E continua Castro (2003)

> O envio de vírus também é previsto na legislação italiana. Pune-se a conduta do agente que difunde, comunica ou entrega um programa informático com o intuito de provocar danos aos dados, programas informáticos ou telemáticos de computadores alheios ou interrompa, total ou parcialmente, seu funcionamento (artigo 615 do Código Penal Italiano).

A conduta dos *hackers* vem disciplinada no crime de acesso ilegal a um sistema informático ou telemático (artigo 615, 1º§ do Código Penal Italiano). Pune-se da mesma forma a conduta de quem difunde, ilegalmente, os códigos de acessos, palavras chaves ou outros meios idôneos de acessar um sistema e informática protegido por medida de segurança (artigo 615, 1º§ do Código Penal Italiano).

Nos Estados Unidos, existem várias leis sobre a informática. A lei nº. 18 U.S.C. 1030 disciplina a fraude e atividades relacionadas a computadores, tipificando algumas condutas e conceituando computador, dentre outras expressões, prevendo penas de multas e encarceramento. É tendência nas leis atuas conceituar os termos técnicos nelas inseridos, assim ocorre na Lei americana, na portuguesa e na brasileira.

Para os efeitos desta lei, constitui crime a conduta de quem acesse computador sem autorização ou excedendo autorização e com isso obtenha informação de registro financeiro, de instituição financeira ou informações do departamento e agências dos Estados Unidos. Também é crime a conduta de acessar um computador, sem autorização ou excedendo autorização, e uso exclusivo do governo dos Estados Unidos ou computador não exclusivo, mas utilizado pelo governo.

Também é punida a conduta de quem causar transmissão de um programa, informação, código ou comando, e provoque dano para computador protegido ou quem, com o intuito de extorquir dinheiro ou outra coisa de valor, ameace de causar danos a computador protegido de pessoa, firma, associação, instituição educacional, financeira, entidade de governo ou outra entidade legal.

Outras leis existem sobre o assunto: Lei nº. 18 U.S.C. 1362 protegendo as linhas de comunicações, estações e sistemas. A Lei 18 U.S.C. 2511 tutela as comunicações tipificando como criem a conduta de quem intercepta ou revela comunicação, oral ou eletrônica, proibida. A lei 18 U.S.C. 2701 tipifica o acesso ilícito de comunicações armazenadas. E a lei 18 U.S.C. 2702 dispõe sobre a revelação de conteúdo.

Quanto à Inglaterra, ouve uma apresentação do governo britânico ao seu parlamento de um projeto que prevê o rastreamento do tráfico de informações na internet pelos serviços de segurança do país, onde os provedores de acesso à internet seriam obrigados a permitir acesso irrestrito da polícia a uma grande quantidade de informações sobre os seus usuários. O *Computer Minuse Act*, de 1990, disciplinou várias condutas criminosas ligadas à informática, como, por exemplo, a obtenção de acesso não autorizado a programa ou informação. Dispôs a excludente de responsabilidade criminal sempre que o agente, sem saber, obtém a informação, ou seja, não houve a intenção de violar o sistema alheio.

O acesso também é punível quando for meio para execução de outro delito. Desta forma, puniu o legislador inglês os atos preparatórios de crimes mais graves que, por circunstâncias diversas, não chegam a se consumar. Trata-se de tio subsidiário, conhecido em nossa legislação (vide LCP). Modificar informações armazenadas em computadores também é punível, excluindo-se, no entanto, a modalidade culposa.

Na Argentina temos o Decreto 427/98, de 16 de abril de 1998, iniciou um programa de uso de assinaturas digitais no âmbito da Administração Pública, para internos que não produzam efeitos jurídicos. Enquanto no Canadá, a RCMP (*Royal Mounted Police*) considera

como principais tipos de crimes as seguintes condutas: acesso não autorizado, danos a dados, furto de telecomunicação e violação de direito autoral de software.

Já na Alemanha, a lei federal de 1997, IuKDG (*Informations – und Kommunikationsdienste – Gesetzt*), alterou várias leis existentes e introduziu novas determinações. Vejamos: disciplinou o uso de serviços de comunicações, a segurança e proteção de dados nos serviços de comunicações, a assinatura digital, modificou o CP e LCP, alterou a lei sobre difusão de publicações atentatórias à juventude e alterou a lei dos direitos autorais.

> A nova legislação define a responsabilidade por transmissão de material pornográfico e prevê a responsabilidade pela veiculação de material ilegal, fazendo distinção entre provedores de acesso e provedores de conteúdo. Os primeiros só podem ser responsabilizados pelo material a que dão acesso caso tenham conhecimento de sua natureza e tenham falhado em utilizar todos os meios razoáveis e tecnicamente possíveis para bloqueá-lo (CASTRO, 2003; p. 163).

Mas, não é só, pois outras leis existem protegendo os meios eletrônicos, como a TK6 (*Telekommunikationsgesetz*), Lei de Telecomunicações, e a TD6 (*Teledienstgezets*), Lei de Tele-serviços.

No caso da China, o governo distribuiu normas de controle do conteúdo da internet sob a alegação de que a rede é utilizada para filtrar segredos de Estado e difundir informações danosas. A regulamentação prevê multas aos infratores e foi aprovada no dia 12/12/1998.

5 OS DESAFIOS DA ATUAL LEGISLAÇÃO BRASILEIRA FRENTE AOS CRIMES DIGITAIS E A ATUAL LEGISLAÇÃO

As discussões têm se intensificado nos últimos tempos quanto a essas inúmeras condutas cometidas pelos usuários da internet e pelos operadores dos sistemas de informática. O principal objeto desses debates é a utilização desses sistemas eletrônicos de forma ilícita, com o intuito de obtenção de vantagem ilícita ou qualquer outro fim nocivo ou prejudicial à sociedade conforme discorre de forma clara Polegatti & Kazmierczak (2012):

> O fator criminógeno virtual cresce de forma a fazer surgirem crimes novos, além de potencializar alguns dos já existentes. Muitos desses crimes são cometidos através da internet ou com o uso do computador. Desse modo, é criada uma nova esfera de atuação delituosa, a saber, os chamados crimes virtuais ou cibercrimes (como são chamados os crimes praticados com o uso do computador ou crimes praticados pela internet). De certo, a informática proporciona uma fácil interação entre as pessoas e, caso não seja utilizada de forma correta, acaba por ser uma meio eficaz na prática de delitos (POLEGATTI & KAZMIERCZAK, 2012; p. 02).

Porém, o fato é que o nosso atual Direito Penal de Informática é quase inexistente, sendo certo afirmar que muito pouco existe no âmbito legislativo no que se refere ao campo da informática. No que tange, então, às condutas criminais que de qualquer forma mantenham relação ao meio informático, pouco se tem em termos de norma legal repressora de condutas atentatórias a bens jurídicos plenamente relevantes, fatos vistos com preocupação por Polegatti & Kazmierczak (2012) quando destacam:

> [...] é imprescindível a atuação do Estado no sentido de coibir esse tipo de conduta, sendo necessária a criação de tipos penais ainda não previstos na legislação e que envolvam o mundo virtual, uma vez que não é permitido, em Direito Penal, utilizar analogia em relação às tipificações já existentes (POLEGATTI & KAZMIERCZAK, 2012; p. 08).

Em suas dissertações Medeiros (2010) destaca que nosso Código Penal Brasileiro, apesar das inúmeras atualizações que recebeu, sua estrutura e redação originais ainda datam de 1940 – quase meio século mais velho que a Lei Magna deste país (a Constituição Federal), e pelo menos cinco décadas antes da Revolução Digital. No momento em que se destaca que a sociedade passou por incontáveis e aceleradas mudanças sociais, econômicas e tecnológicas desde a década de 1980, a desatualização acaba sendo gritante e impossível de não ser posta em foco.

Laflouva (2011) ressalta o fato de que esse quadro não fica restrito unicamente à legislação brasileira, uma vez que, segundo a autora, o mundo digital não possui fronteiras – um dos seus maiores problemas.

> [...] enquanto a legislação é aplicada de acordo com a localidade de realização do suposto crime cibernético, os hackers de todo de todo o mundo têm aprendido a burlar as leis hospedando seus sites em países de legislação mais flexível, como a Eslovênia ou a Suíça, e usando artimanhas digitais para que seus acessos via IP apontem para regiões onde a punição judicial a *cibercrimes* seja mais difícil, com o uso de *proxys*, sites da web que permitem a navegação de forma supostamente anônima, ao trocar o IP que identifica o computador que realiza determinado acesso (LAFLOUVA, 2011, p.02).

E como em nosso ordenamento jurídico a Constituição Federal estabelece em seu art. 5º, XXXIX que "[...] não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal", reserva-se legalmente nesse momento devido o dispositivo constitucional citado, a tipificação adotada pelo sistema jurídico romano-germânico (*civil law*) aderido pela legislação brasileira. Dessa forma, a constatação do delito nas atividades que regem a esfera virtual (p.ex., invadir sistemas e acessar dados restritos) carece de forma direta de uma legislação específica, contrário, por exemplo, ao sistema utilizado no direito anglo-saxão (*common law*) que opta pelo julgamento por analogia.

A opinião de Medeiros (2010) vem ressaltar essa linha de pensamento no momento em que destaca que para alguém ser punido e responsabilizado penalmente, existe a necessidade de que a lei descreva, de forma prévia e minuciosa, todos os elementos do ato considerado ilícito e praticado pelo agente - nesse caso em questão faz-se menção a condutas criminosas ocorridas mediante a utilização de sistema informatizado, dispositivo de comunicação ou rede de computadores - e que devem, igualmente, estar expressamente definidas em lei.

Na visão de Castro (2001), as primeiras iniciativas legislativas ocorreram como advento do Plano Nacional de Informática e Automação (Conin), através da Lei nº. 7.232/84, que veio a delimitar as principais diretrizes no âmbito da informática em solo brasileiro, e também com a Lei nº. 7.646/87 (revogada pela Lei nº. 9.609/98), que foi o primeiro instrumento legal a descrever condutas ou infrações de informática. O principal defeito de tal norma era o fato de que essa somente cuidou de proteger a propriedade intelectual dos programas de computador e sua comercialização.

> Por fim, vale ressaltar que o Direito Penal não vem acompanhando as mudanças ditadas pela explosão tecnológica, operada desde a última metade do Século XX. Tais mudanças já estão preconizadas na Constituição da República do Brasil, de forma que se buscou proteger os interesses envolvidos contra os avanços da utilização dos meios informáticos em práticas que ferem a dignidade da pessoa humana, assimilando os nuances da nova realidade social. Assim, a tutela penal de tais interesses faz-se extremamente necessária, vez que a falta de regulamentação que reprima atos que vão de encontro à nova ordem social torna instável a sustentação desse novo modelo (SOUZA NETO, 2009; p. 134).

Em suas dissertações Carvalho (2014) traz à luz da discussão o fato de que as casas legislativas de nosso país brasileiras não vêm acompanhando o desejado e necessário progresso e evolução social - em especial no que se refere aos crimes praticados pela via digital fazendo-se uso da tecnologia. Há que ser destacado, no entanto, comenta Carvalho (2014), que mudanças significativas foram realizadas em textos legais no sentido de permitirem responsabilizar o indivíduo que comete delitos na esfera virtual, como, por exemplo:

> [...] o art. 20, §2º da Lei n.º 7.716/89 que define como qualificadora utilizar-se de meio eletrônico para incitar e discriminar, permitindo que o magistrado interdite mensagens ou páginas na rede mundial de computadores; tipificar no art. 241-A da Lei n.º 8.069/90 como crime contra a criança e adolescente oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio de vídeo ou outro registro com cena de sexo explícito ou pornografia que envolva criança ou adolescente; equiparar meios eletrônicos aos convencionais para corromper menores, conforme o art.244-B da Lei n.º 8.069/90; utilizar ou divulgar programa de processamento de dados em crimes contra a ordem tributária, no art. 2º, V da Lei n.º 8.137/90 bem como em outras áreas como interceptação telefônica, violação de dados eleitorais e violação de direitos autorais de programa de computador (CARVALHO, 2014, p.01).

Nesse momento Carvalho (2014) nos mostra que, mesmo tímidas, as iniciativas legislativas tomadas já constituem o que ele chama de pequeno rol de aparato normativo a ser utilizado pelo Estado para combater as ações que compõem as condutas delitivas digitais. No entanto, questiona o autor em sua dissertação frente às evoluções na previsão legal de alguns crimes digitais: são os remédios legais existentes na atual legislação suficientes para se coibir tais ações cometidas dentro do universo cibernético?

Pela importância que possui no seio da atual sociedade moderna, Carneiro (2012) destaca a via digital como sendo um dos veículos mais importantes de celebração de contratos onde nosso país, por exemplo, não tem legislação específica sobre os delitos cometidos através dos meios cibernéticos – o que acaba levando a utilização do princípio da analogia como único meio hábil para que o criminoso cibernético não escape impune. No entanto, salienta:

> [...] tal princípio não é aplicável no Direito Penal, por ferir do princípio da taxatividade, sendo necessária a criação de leis mais específicas. São exemplos de normas aplicadas, com a utilização da analogia, aos crimes virtuais: Calúnia (art. 138 do Código Penal); Difamação (art. 139 do Código Penal); Injúria (art. 140 do Código Penal); Ameaça (art. 147 do Código Penal); Furto (art. 155 do Código Penal); Dano (art. 163 do Código Penal); Apropriação indébita (art. 168 do Código Penal); Estelionato (art. 171 do Código Penal); Violação ao direito autoral (art. 184 do Código Penal); Pedofilia (art. 247 da Lei nº 8.069/90 - Estatuto da Criança e do Adolescente); Crime contra a propriedade industrial (art. 183 e ss. da Lei nº 9.279/96); Interceptação de comunicações de informática (art. 10 da Lei nº

> 9.296/96); Interceptação de E-mail Comercial ou Pessoal (art. 10 da Lei nº 9.296/96); Crimes contra software - "Pirataria" (art. 12 da Lei nº 9.609/98). (CARNEIRO, 2012, p. 01).

Assim, destaca Wanderlei (2012), houve a tramitação de Projetos de Lei que dissertam sobre crimes virtuais e que hoje já convertidos em Leis Ordinárias como, por exemplo, o PL n° 84/1999 (transformado na lei ordinária 12.735/2012) e o PL n° 2.793/2011 (transformado posteriormente na Lei Ordinária 12.737/2012 – vulgo Lei Carolina Dieckman).

Quanto à Lei 12.735/12, Oliveira (2013) lembra que, inicialmente projetada para ser extravagante, alterou apenas os diplomas legais já existentes, com a seguinte ementa:

> Ela altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. A criação de tal norma teve como principal influência a impossibilidade de proteção aos bens da vida, maculados pelos crimes virtuais, através de uma legislação da década de 1940, ano da criação do Código Penal (OLIVEIRA, 2013; p. 34).

No caso da Lei Ordinária 12.737/2012 – vulgo Lei Carolina Dieckman, a aprovação deste projeto de Lei se deu depois do escândalo envolvendo a atriz de mesmo nome que teve seu computador invadido por criminosos digitais e viu fotos íntimas suas vazadas nas redes sociais. Esse projeto veio então com o intuito de tipificar condutas criminosas como essas desde que com o intuito de obter, mudar ou destruir dados ou informações, instalar vulnerabilidades entre outros (WANDERLEI, 2012).

> Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.
> Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
> "Invasão de dispositivo informático
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal" (LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012).

Além da questão conotativa, Oliveira (2013) destaca ainda a discussão que se sucedeu devido a necessidade de se impor limites penais às condutas praticadas no campo virtual, em especial devido ao fato de que o a época PL 84/1999 (que posteriormente tornou-se a Lei nº 12.737/2012) recebeu o apelido de AI-5 digital em decorrência da acusação de estar promovendo a censura e a obrigação de retenção de *logs* ou IPs (endereço do computador na internet) por três anos pelos provedores.

Entretanto, o fator final que foi realmente decisivo na aprovação de tais institutos teve origem mesmo no vazamento das fotos íntimas da atriz Carolina Dieckmann, um momento em que, destaca Oliveira (2013) a atriz viu sua conta de e-mail *hackeada* de forma *que* os criminosos tivessem acesso aos dados da vítima culminando na publicação de suas imagens em sites de pornografia.

Para Oliveira (2013), a produção legislativa no Brasil recebe indiscutível e forte influência da mídia, o que da a impressão de que a privacidade de uns poucos famosos seja mais importante que a segurança de informações contidas em sites oficiais do governo.

Porém Maciel (2012) destaca que, embora tal projeto tenha dimensão exclusivamente civil, sua aprovação não causará apenas reflexos na respectiva área, mas também efeitos na esfera criminal. E para Wanderlei (2012):

> [...] tais dispositivos serão vistos com mais peculiaridades mais adiante. Todas essas ações não são suficientes para coibir as práticas do infrator cibernético. Há a necessidade de regulamentação da internet, o que está sendo discutido pela sociedade atualmente, através do chamado Marco Civil da Internet. Tal instituto consiste em uma espécie de constituição da internet contendo princípios que nortearão o correto uso da internet no Brasil, além de projetar diretrizes para o Poder Público no sentido de buscar o desenvolvimento saudável da internet no Brasil. (WANDERLEI, 2012; p. 38).

No entanto, Oliveira (2013) dispara que ambas as leis 12.735/2012 e 12.737/2012 tiveram o objetivo de preencher lacunas legislativas que impediam a tipificação de atos ilícitos praticados pelos meios digitais – desejando-se cumprir os princípios que norteiam o Direito Penal, a saber, o da legalidade e a proibição da analogia.

Já Monteiro Neto (2008) destaca que ambas tiveram como foco a proteção da informação, embora devam ser criados mecanismos específicos no combate aos crimes virtuais. Para o autor, o mundo virtual ainda é vítima de um imenso vazio de normas para o regulamentar, fato este que contribui de forma direta para a ausência de punição da pare do Estado que supostamente deve coibir os delitos que nele se materializarem.

5.1 Alguns exemplos de crimes digitais e a postura da legislação penal brasileira diante deles

Com o advento da internet e o forte crescimento tecnológico no universo da informática, muitos dos recursos e instrumentos digitais que já fazem parte da vida e do cotidiano de bilhões de pessoas ao redor do mundo, passaram a ter seus prós e contras no nosso cotidiano, pois, da mesma forma que nos permite uma enorme comodidade entretendo, e ajudando-nos a realizar importantes trabalhos como, por exemplo, pagamento de despesas e transferência de valores, também, pela falta de segurança em muitos sistemas, nos deixam a mercê de criminosos que lançam mão de seus recursos para acessar dados e senhas para praticar crimes que vão desde a pornografia, pedofilia, desvio de recursos de contas bancárias, divulgação de informações de cunho pessoal de pessoas físicas até informações sigilosas de pessoas jurídicas.

Alguns desses crimes, que já são antigos, passaram a ser praticados no universo digital da rede mundial, da mesma forma que outros delitos novos também surgiram estando alguns já tipificados pelo ordenamento jurídico brasileiro como, por exemplo, o furto, estelionato, etc., que serão a seguir detalhados.

- **Inserção de dados falsos em sistemas de informações:** essa modalidade de crime foi tipificada no nosso Código Penal (2007), no seu artigo 313-A, no capítulo que trata dos crimes praticados por funcionário público contra a administração em Geral, ou seja, é um crime próprio, ficando os demais criminosos fora dessa tipificação.
- **Modificação ou alteração não autorizada de sistema de informações:** assim como a inserção de dados falsos em sistemas de informações, esta modalidade de crime também foi normatizada no art. 313-B, do CPB.
- **Divulgação de segredo - espionagem:** é a divulgação, transferência, sem autorização, de informações sigilosas ou reservadas, no intuito de causar prejuízo econômico ao legítimo dono do segredo, visando obter vantagem econômica para si ou para outrem.

Este tipo de crime, também já está tipificado no Código Penal Brasileiro, no seu artigo 153, § 1º-A, no capítulo dos crimes contra a liberdade individual.

- **Pornografia infantil:** a tipificação inicial do artigo 241, do Estatuto da Criança e do Adolescente – ECA (Lei 8.069/90) previa que somente as condutas de fotografar ou publicar cena de sexo explícito ou pornografia envolvendo criança ou adolescente era considerada crime. Em 12/11/2003, a Lei 10.764, alterou o tipo penal, prevendo expressamente, pela primeira vez, a prática criminosa utilizando-se, inclusive, a rede mundial de computadores ou Internet. Obs. Posteriormente, como resultado da CPI da Pedofilia, realizada no Senado Federal, a Lei nº 11.829, de 25/11/2008, alterou profundamente referido tipo penal, aprimorando o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizando a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na Internet, adequando-se a nossa realidade.
- **Pirataria ou Violação de Direitos Autorais:** é a cópia, venda ou distribuição de material sem autorização nem pagamento dos direitos autorais, envolvendo diversos tipos de produtos, desde roupas, livros, CDs, *softwares*. A pirataria, também já se encontra tipificada no artigo 12, da Lei 9.609/98.
- **Utilização indevida de acesso restrito e permitir acesso de pessoas não autorizadas a sistemas de informações:** este crime diz respeitos ao funcionário público que permite ou facilita que um estranho tenha acesso aos sistemas de informações ou banco de dados da Administração pública, assim como venha acessar sistemas restritos sem autorização ou permissão, conforme disposto no artigo 325, incisos I e II, do Código Penal Brasileiro (2007).

Pires Neto (2009) esclarece que a rede mundial de computadores (internet) tornou-se há tempos uma terra sem fronteiras onde se consegue por intermédio de computadores e da própria rede se ter o autor de um crime em um país e uma vítima em outro. Pelo fato de cada país possuir legislação própria acaba sendo difícil de chegar a uma competência específica para a apuração do delito ou mesmo obtenção dos dados necessários à investigação.

Segurado et al (2014) enfatiza a complexidade deste tema no momento em que precisa reunir setores da mais alta relevância social como o governo, sociedade civil, empresas e comunidades para se discutir os rumos e objetivos que devem ter as leis a serem criadas para legislar sobre o mundo e os delitos que dele se originam de forma proteger o individuo que tem a perder com a ação de criminosos cibernéticos espalhados ao redor do mundo.

Para Neto (2009) os demais crimes cometidos com a utilização dos meios de informática e da Internet, ainda não foram normatizados especificamente, no entanto, não significa dizer que quem cometer esses crimes não será punido, pois o enquadramento da conduta é realizado pelas leis já existentes, por exemplo:

> A falsificação, que com o advento das novas impressoras de alta resolução facilitou a falsificação de documentos oficiais, papel-moeda, entretanto o crime ainda é de falsificação de papéis e documentos públicos (arts. 293 e 297, CPB) e falsificação de moeda (art. 289, CPB).
> A utilização dos *Cavalos de Tróia* e *Sniffers* para conseguirem as senhas dos cartões de crédito e os números das contas, para em seguida sacarem todo o dinheiro e efetuarem compras com os cartões. Neste caso, a conduta é enquadrada como estelionato (art. 171, do CPC), mas outros doutrinadores enquadram como furto (art. 155, do CPB).
> O crime de dano que é previsto no artigo 163 do Código Penal, que ocorre quando um *cracker* invade uma página da "Internet" danificando-a, destrói banco de dados, arquivos e demais informações constantes no disco rígido.
> O crime de estelionato (art. 171, CPB), também pode ser aplicado a outras formas de condutas criminosas, como fraudar vendas com a utilização de *sites* e dados falsos, onde a vítima adquire uma mercadoria e paga com cartão de crédito e essa mercadoria nunca chega, nem a pessoa consegue mais contatar com o estelionatário, uma vez que seus dados não são verídicos.
> Existe ainda, o tráfico de drogas, onde os traficantes se utilizam dos correios eletrônicos para negociarem a venda de drogas, sendo enquadrados no art. 33, da Lei 11.343/06, bem como o incentivo ao consumo, onde normalmente são publicados na "Internet".
> Entre diversas outras modalidades de crimes, podemos ainda mencionar os crimes de ameaça (art. 147, CPB), injúria (art. 140, CPB), calúnia (art. 138, CPB), difamação (art. 139, CPB), racismo (art. 20, da Lei 7.716/89), apologia ao crime (art. 287, CPB), incitação ao crime (art. 286, CPB), lavagem de dinheiro (Lei 9.613/98), e quadrilha ou bando - art. 288, CPB (NETO, 2009; p.15).

Cabe ao Estado agora vencer o que chamamos de competência jurisdicional para se avançar ainda mais sobre os crimes cibernéticos, pois já destaca Colares (2006) que o Estado tem o exercício de seu poder jurisdicional limitado ao território onde exerce sua soberania, entretanto, as novas tecnologias da informação, ao contrário, proporcionam um ambiente virtual que não reproduz quaisquer fronteiras, inexistindo, portanto, o pressuposto geográfico necessário ao exercício da jurisdição.

6 CONCLUSÃO

O infindável número de indivíduos que, de alguma forma são virtualmente lesados, ofendidos, agredidos ou expostos publicamente em sua privacidade cresce assustadoramente a cada dia e, pelo volume de casos de condutas que podem ser tipificadas criminalmente na internet, faz-se necessária à intervenção estatal para que sejam coibidas e assim se preserve a liberdade garantia pela própria Constituição Federal.

No entanto, um dos maiores empecilhos à ação do Estado nessa esfera digital se dá pelo fato de que tais condutas ainda não estejam tipificadas pela nossa legislação, pois, apesar do ordenamento jurídico brasileiro já atuar por analogia nas ações punitivas contra os infratores com base na legislação vigente, é preciso se criar uma lei específica contra os crimes digitais e assim se esquivar dessa limitada "adaptação" de novos delitos às leis antigas, abrindo-se verdadeiras brechas ao processo de impunidade.

O meio digital é usado por criminosos para praticarem crimes que, na maioria das vezes, não se configuram como crimes digitais, pelo contrario, são crimes comuns e, pior, já devidamente previstos no ordenamento jurídico brasileiro – em bora se deem por intermédio de computadores, dentre os quais se destacam o estelionato, ameaça, crimes do Estatuto da Criança e do Adolescente (ECA).

Essas condutas dizem respeito aos crimes denominados virtuais, de informática, ou crimes de internet, ou seja, os que são praticados através de computadores, contra os próprios computadores ou seus usuários. Como exemplo podemos citar as condutas delitivas para se acessar, de forma não autorizada, os sistemas de informação de pessoas físicas ou jurídicas, interceptando comunicações, obtendo e modificando ilicitamente dados, incitando o ódio e a violência e difundindo sentimentos como a intolerância, pornografia infantil e o terrorismo.

Nesse sentido, apesar da importância de leis como a 12.735/12 e a 12.737/12, é preciso admitir que ainda sejam insuficientes, pois vieram apenas alterar dispositivo que não previa, à época de sua elaboração, tais condutas, por ser o Código Penal datado de 1940.

Soma-se a isso a Lei 12.965/2014 que, apesar de sua base cível, tornou-se uma forte aliada contra as ações delitivas digitais ajudando no procedimento de investigação de crimes virtuais para transformar a rede mundial de computadores em um ambiente menos árido à atuação do Estado para assegurar princípios, garantias e direitos dos seus usuários que são feridos por crimes realizados por meios eletrônicos como *download* de *spy* (programas

espiões), copiadores de senha, e-mails e mensagens, que expõem o usuário ao tornar público o que deveria ser privado.

Há que se falar ainda dos crimes de cunho sexual e das mais diversas formas de pornografia e pedofilia em âmbito digital num país onde a legislação relacionada aos crimes digitais é tímida – assim como as iniciativas do legislativo para acompanhar as transformações tecnológicas ocorridas e coibir esses delitos – o que nos leva ao ponto de que os debates e as discussões que buscam combater as modalidades de crimes virtuais ainda estejam longe do fim.

O chamado Marco Civil da Internet defende a confidencialidade e a isenção do provedor embora também determine em seu art. 22 que ele deve fornecer os registros quando judicialmente solicitados destacando que "[...] a parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet".

No entanto, o seu parágrafo único impõe que "sem prejuízo dos demais requisitos legais" o requerimento que busca e ordena os mesmos registros deve conter, sob pena de inadmissibilidade, fundados indícios da ocorrência do ilícito; uma justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória, e, finalmente, o período ao qual se referem os registros, ficando a cargo do juiz a iniciativa das providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro, listados no art. 23 do referido instrumento jurídico.

No momento da finalização deste trabalho há que ser ressaltada a necessidade de se trazer a luz da discussão um tema com tamanha repercussão social - até mesmo pelos avanços que nos atingiram nas últimas décadas com a revolução tecnológica que não para de superar limites com o processo de interação nas redes sociais e a comodidade de se acessar a vários serviços através da rede mundial de computadores, deixando-nos vulneráveis aos criminosos cibernéticos e seus delitos na seara digital.

Obviamente que essa nova realidade cobra uma rápida e eficaz intervenção estatal no ordenamento jurídico vigente no intuito de se criar ferramentas jurídicas que possam resguardar os direitos dos cidadãos com uma legislação específica que faça frente às violações

diárias dos direitos de dezenas de milhões de pessoas em nosso país diminuindo a sensação de impotência diante da insegurança virtual que vivemos.

REFERÊNCIAS

ARAS, Vladimir. **Crimes de informática. Uma nova criminalidade**. Jus Navigandi, Teresina, ano 5, n. 51, out. 2001. Disponível em: <http://jus2.uol.com.br/doutrina/t>. Acesso em 2017.

BASSO, M; ALMEIDA, G. A. **É preciso difundir mentalidade digital nas empresas.** In: KAMISNSKI, Omar (Org.), op. cit., 2007.

CARNEIRO, A. G. Crimes Virtuais: Elementos Para uma Reflexão Sobre o Problema na Tipificação. In: **Âmbito Jurídico**, Rio Grande, 15, n. 99, abr. 2012. Disponível em: <http://www.ambito-uridico.com.br/site/index.php>. Acesso em 2017.

CARVALHO, Paulo Roberto de Lima. **Crimes cibernéticos: uma nova roupagem para a criminalidade.** 2014. Disponível em: https://jus.com.br/artigos/31282/crimes-ciberneticos-uma-nova-roupagem-paraacriminalidade. Acesso em 2017.

CASTRO, Aldemario Araújo. **Internet e os Tipos Penais que Reclamam Ação Criminosa em Público.** 2003. Disponível em <http://www.webly.com.br/forum>. Acesso em 2017.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.48.

DEMO, Pedro. **Pesquisa e construção do conhecimento: metodologia científica no caminho de Habermas**. Rio de Janeiro: Tempo Brasileiro, 2000.

GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet**. Boletim do ibccrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.

LAFLOUFA, Jacqueline. **Hackativismo: crime cibernético ou legítima manifestação digital?** 2011. Disponível em: http://comciencia.scielo.br/scielo=sci. Acesso em 2017.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. Campinas, SP: Ed. Millennium, 2005.

MEDEIROS, Cláudia Lucio de. **Deficiências da legislação penal brasileira frente aos crimes cibernéticos.** 2010. Disponível em: http://www.mpce.mp.br/esmp/publicacoes. Acesso em 2017.

MONTEIRO NETO, J. A. **Aspectos Constitucionais e Legais do Crime Eletrônico.** Fortaleza, 2008.

NETO, L. P. **Crimes cibernéticos: necessidade de uma legislação específica no Brasil**. Dissertação monográfica apresentada no Curso de Graduação em Direito da FESP. 2009.

OLIVEIRA, J. C. de. **O Cibercrime e as Leis 12.735 e 12.737/2012.** São Cristóvão, 2013.
POLEGATTI, B. C; KAZMIERCZAK, L. F. **Crimes Cibernéticos: O Desafio do Direito Penal na Era Digital.** Ourinhos, 2012.

ROSA, Fabrízio. **Crimes de Informática.** Campinas: Bookseller, 2002.

SEGURADO, Rosemary; LIMA, Carolina Silva Mandú; AMENI, Cauê S. **Regulamentação da internet: perspectiva comparada entre Brasil, Chile, Espanha, EUA e França.** 2014. Disponível em: http://www.scielo.br/pdf/hcsm/pdf. Acesso em 2017.

SOUZA NETO, P. A. de. **Crimes de Informática.** Itajaí, 2009.

VEDOVATE, L. L. V. Contratos Eletrônicos. **Intertemas.** v. 10, n. 10. Presidente Prudente, 2005.

WANDERLEI, F. P. **Crimes Cibernéticos: Obstáculos para Punibilidade do Infrator.** Araguaína, 2012.

WENDT, E; JORGE, H. V. N. **Crimes Cibernéticos**. São Paulo: BRASPORT, 2012.

ANEXO

SUBSTITUTIVO AOS PLS 76/2000, PLS 137/2000 E PLC 89/2003 – SENADOR AZEREDO ALVES.

Altera o Decreto-Lei nº 2.848, de 07 de dezembro de 1940 (Código Penal) e o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), para tipificar condutas realizadas mediante uso de rede de computadores ou internet, ou que sejam praticadas contra sistemas informatizados e similares, e dá outras providências.

O CONGRESSO NACIONAL decreta:

Art. 1º O Capítulo IV do Título II da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do art. 163-A, assim redigido:

Dano por difusão de vírus eletrônico

Art. 163-A. Criar, inserir ou difundir vírus em dispositivo de comunicação ou sistema informatizado, com a finalidade de destruí-lo, inutilizá-lo ou dificultar-lhe o funcionamento.
Pena: reclusão, de 1 (um) a 3 (três) anos, e multa.
Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso.” (NR)
Art. 2º O Título I da Parte Especial do Código Penal fica acrescido do Capítulo VII-A, assim redigido:

Capítulo VII-A: DA VIOLAÇÃO DE DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO.

Acesso indevido a dispositivo de comunicação

Art. 154-A. Acessar indevidamente, ou sem autorização, dispositivo de comunicação ou sistema informatizado:
Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 1º Nas mesmas penas incorre quem fornece a terceiro meio indevido ou não autorizado de acesso a dispositivo de comunicação ou sistema informatizado.
§ 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias.
§ 3º A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso.

Manipulação indevida de informação eletrônica

Art. 154-B. Manter consigo, transportar ou fornecer indevidamente ou sem autorização, dado ou informação obtida em dispositivo de comunicação ou sistema informatizado:
Pena – detenção, de 2 (dois) a 4 (quatro) anos, e multa.
Parágrafo único - Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias.
Dispositivo de comunicação, sistema informatizado, identificação de usuário e autenticação de usuário.
Art. 154-C. Para os efeitos penais, considera-se:
I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados digitais, ou qualquer outro meio capaz de processar, armazenar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia digital.
II – sistema informatizado: a rede de computadores, o equipamento ativo da rede de comunicação de dados com ou sem fio, a rede de telefonia fixa ou móvel, a rede de televisão, a base de dados, o programa de computador ou qualquer outro sistema capaz de processar, armazenar ou transmitir dados eletronicamente.
III – identificação de usuário: os dados de nome de acesso, senha criteriosa, nome completo, filiação, endereço completo, data de nascimento, numero da carteira de identidade ou equivalente legal, que sejam requeridos no momento do cadastramento de um novo usuário de dispositivo de comunicação ou sistema informatizado.

IV – autenticação de usuário: procedimentos de validação e conferência da identificação do usuário, quando este tem acesso ao dispositivo de comunicação ou sistema informatizado, realizados por quem os torna disponíveis ao usuário.

Divulgação de informações depositadas em banco de dados

Art. 154-D. Divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas físicas ou jurídicas, ou a dados de pessoas físicas referentes à raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, salvo por decisão da autoridade competente, ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.
Pena – detenção, de um a dois anos, e multa.
Parágrafo único: A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de divulgação.

Dados de conexões e comunicações realizadas

Art. 154-E. Deixar de manter, aquele que torna disponível o acesso à rede de computadores, os dados de conexões e comunicações realizadas por seus equipamentos, aptas à identificação do usuário, endereços eletrônicos de origem e destino no transporte dos registros de dados e informações, data e horário de início e término da conexão, incluindo protocolo de internet ou mecanismo de identificação equivalente, pelo prazo de cinco anos.
Pena – detenção, de dois a seis meses, e multa.

Permitir acesso por usuário não identificado e não autenticado

Art. 154-F. Permitir, aquele que torna disponível o acesso à rede de computadores, a usuário, em a devida identificação e autenticação, qualquer tipo de acesso ou uso pela rede de computadores.
Pena – detenção, de um a dois anos, e multa.

Parágrafo único. Na mesma pena incorre, o responsável por provedor de acesso à rede de computadores, que deixa de exigir, como condição de acesso à rede, a necessária, identificação e regular cadastramento do usuário.

Art. 3º O Código Penal passa a vigorar acrescido do seguinte art. 183A:

Art. 183-A. Equiparam-se à coisa o dado ou informação em meio eletrônico, a base de dados armazenada em dispositivo de comunicação e o sistema informatizado, a senha ou qualquer meio que proporcione acesso aos mesmos.

Art. 4º Os arts. 265 e 266 do Código Penal passam a vigorar com as seguintes redações:

Atentado contra a segurança de serviço de utilidade pública

Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública:

Interrupção ou perturbação de serviço telegráfico ou telefônico

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático ou de telecomunicação, impedir ou dificultar-lhe o restabelecimento:

Art. 5º O Capitulo II do Título VIII do Código Penal passa a vigorar acrescido do seguinte artigo:

Difusão Maliciosa de Código

Art. 266-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por quaisquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:

Pena – detenção de um a dois anos.

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso. (NR)

Art. 6º O art. 298 do Código Penal passa a vigorar acrescido do seguinte parágrafo único:

Art. 298. ...

Falsificação de cartão de crédito ou débito ou qualquer dispositivo eletrônico portátil de armazenamento e processamento de informações.

Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito ou qualquer dispositivo eletrônico portátil de armazenamento ou processamento de informações. (NR).
Art. 7º O Código Penal passa a vigorar acrescido do seguinte art. 298A:

Falsificação de telefone celular ou meio de acesso a sistema eletrônico.

Art. 298-A. Criar ou copiar, indevidamente ou sem autorização, ou falsificar código; sequência alfanumérica; cartão inteligente; transmissor ou receptor de rádio frequência ou telefonia celular; ou qualquer instrumento que permita o acesso a dispositivo de comunicação ou sistema informatizado:
Pena – reclusão, de um a cinco anos, e multa.”(NR)
Art. 8º O Código Penal passa a vigorar acrescido do seguinte art. 141A:
Art. 141-A. As penas neste Capítulo aumentam-se de dois terços caso os crimes sejam cometidos por intermédio de dispositivo de comunicação ou sistema informatizado.
Art. 9º O Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar) fica acrescido do art. 262-A, assim redigido:

Dano por difusão de vírus eletrônico

Art. 262-A. Criar, inserir ou difundir vírus em dispositivo de comunicação ou sistema informatizado, com a finalidade de destruí-lo, inutilizá-lo ou dificultar-lhe o funcionamento.
Pena: reclusão, de 1 (um) a 3 (três) anos, e multa.
Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso. (NR)

Art. 10 O Título VII da Parte Especial do Livro I do Código Penal Militar, Decreto-Lei, nº 1.001, de 21 de outubro de 1969, fica acrescido do Capítulo VII-A, assim redigido:

Capítulo VII - DA VIOLAÇÃO DE DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

Acesso indevido a dispositivo de comunicação

Art. 339-A. Acessar indevidamente, ou sem autorização, dispositivo de comunicação ou sistema informatizado:
Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
§ 1º Nas mesmas penas incorre quem fornece a terceiro meio indevido ou não autorizado de acesso a dispositivo de comunicação ou sistema informatizado.
§ 2º A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso.

Manipulação indevida de informação eletrônica

Art. 339-B. Manter consigo, transportar ou fornecer indevidamente ou sem autorização, dado ou informação obtida em dispositivo de comunicação ou sistema informatizado:
Pena – detenção, de 2 (dois) a 4 (quatro) anos, e multa.

Dispositivo de comunicação, sistema informatizado, identificação de usuário e autenticação de usuário.

Art. 339-C. Para os efeitos penais, considera-se:
I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados digitais, ou qualquer outro meio capaz de processar, armazenar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia digital.
II – sistema informatizado: a rede de computadores, o equipamento ativo da rede de comunicação de dados com ou sem fio, a rede de telefonia fixa ou móvel, a rede de televisão, a base de dados, o programa de computador ou qualquer outro sistema capaz de processar, armazenar ou transmitir dados eletronicamente.
III – identificação de usuário: os dados de nome de acesso, senha criteriosa, nome completo, filiação, endereço completo, data de nascimento, numero da carteira de identidade ou equivalente legal, que sejam requeridos no momento do cadastramento de um novo usuário de dispositivo de comunicação ou sistema informatizado.

IV – autenticação de usuário: procedimentos de validação e conferência da identificação do usuário, quando este tem acesso ao dispositivo de comunicação ou sistema informatizado, realizados por quem os torna disponíveis ao usuário.

Divulgação de informações depositadas em banco de dados

Art. 339-D. Divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas físicas ou jurídicas, ou a dados de pessoas físicas referentes à raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, salvo por decisão da autoridade competente, ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.
Pena – detenção, de um a dois anos, e multa.
Parágrafo único: A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de divulgação.

Dados de conexões e comunicações realizadas

Art. 339-E. Deixar de manter, aquele que torna disponível o acesso à rede de computadores, os dados de conexões e comunicações realizadas por seus equipamentos, aptas à identificação do usuário, endereços eletrônicos de origem e destino no transporte dos registros de dados e informações, data e horário de início e término da conexão, incluindo protocolo de internet ou mecanismo de identificação equivalente, pelo prazo de cinco anos.
Pena – detenção, de dois a seis meses, e multa.

Permitir acesso por usuário não identificado e não autenticado

Art. 339-F. Permitir, aquele que torna disponível o acesso à rede de computadores, a usuário, sem a devida identificação e autenticação, qualquer tipo de acesso ou uso pela rede de computadores.
Pena – detenção, de um a dois anos, e multa.

Parágrafo único. Na mesma pena incorre, o responsável por provedor de acesso à rede de computadores, que deixa de exigir, como condição de acesso à rede, a necessária, identificação e regular cadastramento do usuário.(NR)

Art. 11 O Capítulo I do Título VI da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar) fica acrescido do art. 281-A, assim redigido:

Difusão maliciosa de código

Art. 281-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:

Pena – detenção de um a dois anos.

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso. (NR)"

Art. 12 O Título V da Parte Especial do Livro I do Código Penal

Militar, Decreto-Lei, nº 1.001, de 21 de outubro de 1969, fica acrescido do Capítulo VIII-A, assim redigido:

Capítulo VIII – A. DISPOSIÇÕES GERAIS

Art. 267-A. Equiparam-se à coisa o dado ou informação em meio eletrônico, a base de dados armazenada em dispositivo de comunicação e o sistema informatizado, a senha ou qualquer meio que proporcione acesso aos mesmos. (NR)

Art. 13 Todo aquele que desejar acessar uma rede de computadores, local, regional, nacional ou mundial, deverá identificar-se e cadastrar-se naquele que torne disponível este acesso.

Parágrafo único. Os atuais usuários terão prazo de cento e vinte dias após a entrada em vigor desta Lei para providenciarem ou revisarem sua identificação e cadastro junto a quem, de sua preferência, torne disponível o acesso aqui definido.

Art. 14 Todo aquele que torna disponível o acesso a uma rede de computadores somente admitirá como usuário pessoa ou dispositivo de comunicação ou sistema informatizado que for autenticado conforme validação positiva dos dados cadastrais previamente fornecidos pelo

contratante de serviços. A contratação dar-se-á exclusivamente por meio formal, vedado o ajuste meramente consensual.

§1º O cadastro mantido por aquele que torna disponível o acesso a uma rede de computadores conterá obrigatoriamente as seguintes informações prestadas por meio presencial e com apresentação de documentação original: nome de acesso; senha de acesso ou mecanismo similar; nome completo; endereço completo com logradouro, número, complemento, código de endereçamento postal, cidade e estado da federação; número de registro junto aos serviços ou institutos de identificação das Secretarias de Segurança Pública Estaduais ou conselhos de registro profissional; número de inscrição no Cadastro de Pessoas Físicas (CPF), mantido pelo Ministério da Fazenda ou o Número de Identificação do Trabalhador (NIT), mantido pelo Ministério da Previdência Social.

§ 2º O cadastro somente poderá ser fornecido a terceiros mediante expressa autorização da autoridade competente ou em casos que a Lei venha a determinar.

§ 3º A senha e o cadastro de identificação, a critério daquele que torna disponível o acesso, poderão ser substituídos por certificado digital emitido dentro das normas da Infraestrutura de Chaves Públicas Brasileira (ICP–Brasil), conforme determina a MP 2.200-2 de 24 de agosto de 2001.

§ 4º O cadastro de identificação, a critério daquele que torna disponível o acesso, poderá ser obtido mediante instrumento público de convênio de cooperação ou colaboração com aqueles que já o tenham constituído na forma deste artigo.

§ 5º Para assegurar a identidade e a privacidade do usuário à senha de acesso poderá ser armazenada criptografada por algoritmo não reversível.

Art. 15 O art. 2º da Lei nº 9.296, de 24 de julho de 1996, passa a vigorar acrescido do seguinte § 2º, renumerando-se o parágrafo único para § 1º:

§ 2º O disposto no inciso III do caput não se aplica quando se tratar de interceptação do fluxo de comunicações em dispositivo de comunicação ou sistema informatizado.

(NR)

Art. 16 Esta Lei entra em vigor sessenta dias após a data de sua publicação.

Sala da Comissão, Presidente, Relator.