FACULDADES INTEGRADAS
"ANTÔNIO EUFRÁSIO DE TOLEDO"

FACULDADE DE DIREITO DE PRESIDENTE PRUDENTE

OS NOVOS CRIMES DE INFORMÁTICA CRIADOS COM O ADVENTO DAS LEIS 12.735/2012 E 12.737/2012

Danielly Maia dos Santos

Presidente Prudente/SP

2014

FACULDADES INTEGRADAS
"ANTÔNIO EUFRÁSIO DE TOLEDO"

FACULDADE DE DIREITO DE PRESIDENTE PRUDENTE

OS NOVOS CRIMES DE INFORMÁTICA CRIADOS COM O ADVENTO DAS LEIS 12.735/2012 E 12.737/2012

Danielly Maia dos Santos

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do Grau de Bacharel em Direito, sob a orientação do Professor Francisco José Dias Gomes.

Presidente Prudente/SP

2014

OS NOVOS CRIMES DE INFORMÁTICA CRIADOS COM O ADVENTO DAS LEIS 12.735/2012 E 12.737/2012

Trabalho de Conclusão de Curso aprovado como requisito parcial para obtenção do Grau de Bacharel em Direito

_____

FRANCISCO JOSÉ DIAS GOMES

_____

GISELE CAVERSAN BELTRAMI MARCATO

_____

PAULA AKEMI KIKUSHI

Presidente Prudente, 04 junho de 2014

“Technological progress is like an axe in the hands of a pathological criminal".

“O progresso tecnológico é como um machado nas mãos de um criminoso patológico”.

Albert Einstein

AGRADECIMENTOS

A Deus, o que seria de mim sem o poder de sua criação.

Aos meus amados pais, Valter dos Santos e Fátima Maia dos Santos, por me educarem e criarem com dignidade, respeito e amor, sempre respeitando minhas escolhas e opiniões. O mérito da pessoa que hoje me tornei é de vocês. Obrigada por tudo, o meu amor por vocês é eterno e sem restrições.

Igualmente e, não menos importante, agradeço a minha irmã querida pelo incentivo e conselhos que contribuíram para o meu crescimento e maturidade. Devoto minha sincera gratidão e meu amor a você.

Meu agradecimento também aos meus familiares, que de um modo ou outro sempre estiveram presentes na minha vida e na minha formação.

A meu estimado e querido orientador, prof. Francisco José Dias Gomes, exemplo de pessoa e profissional, competente e dedicado em tudo o que se propõe. Obrigada pela paciência, apoio e amizade durante essa longa jornada.

A profª. Gisele Caversan Beltrami Marcato e a Paula Akemi Kikushi, meu sincero agradecimento, por aceitarem compor a banca examinadora deste trabalho.

Aos amigos, que fizeram ou fazem parte da minha vida de alguma forma, obrigada pelo apoio, incentivo, e até mesmo distrações; sem vocês eu não seria nada. Devoto meu amor e carinho a vocês, que me ajudaram a construir minha história.

Danielly Maia dos Santos

RESUMO

Com a evolução tecnológica e o uso de dispositivos eletrônicos cada vez mais modernos, que podem trocar informações de qualquer parte do mundo em tempo real, a internet tornou-se parte do cotidiano do brasileiro. Essa troca de informações ou mesmo seu armazenamento tornaram-se alvo de criminosos, que passaram a se aproveitar da facilidade de acesso e falta de proteção de alguns sistemas, para invadi-los e cometer “crimes”, que, muitas vezes, ficavam impunes frente à falta de legislação específica. Para sanar tal problema, foram criadas e sancionadas novas leis que modificaram e criaram alguns dispositivos no Código Penal e Código de Processo Penal. Estas modificações foram trazidas pelas Leis 12.735/2012 e 12.737/2012, que trouxeram tipificações para algumas condutas relacionadas à informática, que antes eram atípicas.

Palavras-chave: Internet. Crime. Código Penal. Código de Processo Penal. Lei 12.735/2012. Lei 12.737/2012.

ABSTRACT

With the technological development and the use of electronic devices increasingly modern, which can exchange information from anywhere in the world in real time, the internet has become part of everyday life of Brazilians. This exchange of information or even your store became the target of criminals, who have to take advantage of the ease of access and lack of protection of some systems, to invade them and committing "crimes", which often went unpunished front the lack of specific legislation. To remedy the problem, were created and enacted new laws that modified and created some devices in the Penal Code and Criminal Procedure Code. These modifications were introduced by Laws 12.735/2012 and 12.737/2012, which brought typifications for some behaviors related to information technology, that were atypical.

Keywords: Internet. Crime. Criminal Code. Code of Criminal Procedure. Law 12.735/2012. Law 12.737/2012.

LISTA DE ABREVIATURAS E SIGLAS

ARPA	Advance Research Projects Agency
ARPANET	Advance Research Projects Agency Network
CD	Compact Disc
DDoS	Distributed Denial of Service
DVD	Digital Versatile Disc
EDSAC	Eletronic Delay Storage Automatic Calculator
EDVAC	Eletronic Discrete Variable Computer
ENIAC	Eletronic Numerical Integrator and Computer
FAPESP	Fundação de Amparo à Pesquisa do Estado de São Paulo
IBGE	Instituto Brasileiro de Geografia e Estatística
LNCC	Laboratório Nacional de Computação Científica
NSF	National Science Foundation
NSFNET	National Science Foundation Network
PNAD	Pesquisa Nacional por Amostra em Domicílios
UFRJ	Universidade Federal do Rio de Janeiro
UNIVAC	Universal Automatic Computer
WWW	World Wide Web

LISTA DE FIGURAS

FIGURAS

SUMÁRIO

INTRODUÇÃO

O avanço da tecnologia ocorre de forma extremamente rápida. A internet é uma das ferramentas mais utilizadas pelos brasileiros, seja no trabalho, em casa, nos momentos de lazer ou descontração. Através dela, informações e dados podem ser trocados de maneira ágil e instantânea, de forma muito eficiente.

Conjuntamente com toda essa facilidade, surgem indivíduos que fazem mau uso dessa ferramenta, utilizando-a para praticar atos ilícitos, ferindo bens jurídicos que devem e são tutelados pelo direito material penal.

Algumas dessas condutas já são tipificadas por meio dos dispositivos existentes no Código Penal. Ocorre que outras ainda não eram tipificadas, tornando esses criminosos impunes por falta de legislação específica para determinados casos.

Ganhou grande repercussão na mídia, a existência de inúmeros casos reais, nos quais ocorreram práticas de condutas danosas, até então atípicas, via internet ou meios informáticos, de modo que o legislador viu-se na obrigação de criar novos dispositivos para, então, proteger os bens jurídicos que estavam sendo feridos e, assim, tutelá-los de forma a garantir a paz social e também a manutenção, de forma eficaz, do Estado Democrático de Direito.

Com isso, foram sancionadas as leis 12.735/2012 e 12.737/2012, que serão melhor explanadas nos seguintes tópicos.

No capítulo I será abordado um pequeno histórico sobre computadores e internet, para melhor compreensão do ambiente onde os crimes são cometidos e conseqüente entendimento do porque estes meios são utilizados.

A partir do capítulo II, será trazido uma explanação sobre os cibercrimes, seu conceito, evolução histórica e os meios utilizados pelos criminosos para sua prática.

Já no capítulo III, far-se-á uma análise da legislação vigente atualmente para os crimes de informática, levando em consideração quais são os direitos fundamentais constitucionais tutelados por estas leis.

Nos capítulos IV e V, realizar-se-á uma análise detalhada das leis 12.735/2012 e 12.737/2012, respectivamente, as chamadas Lei Azeredo e Lei Carolina Dieckmann, mostrando e explicando todos os tipos penais trazidos com essas inovações legislativas.

No capítulo VI, breves comentários sobre o recente aprovado Marco Civil da Internet serão feitos.

Finalmente no capítulo VI, será realizado uma análise da eficácia das leis supracitadas, mostrando se as mesmas preenchem ou não as lacunas antes existentes na legislação pátria para os cibercrimes.

1 CONSIDERAÇÕES INICIAIS SOBRE COMPUTADOR E INTERNET

Neste capítulo serão trazidas algumas breves considerações sobre a origem histórica dos computadores e da internet, em busca de uma melhor compreensão futura dos temas que serão abordados.

1.1 Breve Histórico Sobre Computador e Internet

Quando o homem notou que para contar tudo aquilo que aspirava já não era mais suficiente utilizar os meios então disponíveis, viu-se diante da necessidade de criar uma máquina capaz de fazê-lo.

Esta máquina é o computador. Computador vem do latim "computadore", que segundo o dicionário Aurélio Online[1], tem como acepção:

> Que ou aquele que computa. / Cibern. Máquina composta de um número variável de unidades especializadas, comandadas por um mesmo programa gravado, que, sem intervenção humana direta, permite efetuar complexas operações aritméticas e lógicas com fins estatísticos, administrativos, contabilísticos etc. (Diz-se também computador eletrônico para processamento de dados.); Um computador compreende uma parte material, dita hardware e constituída de circuitos eletrônicos integrados, e um software. O hardware compõe-se de um ou vários processadores, uma memória, unidades de entrada/saída e unidades de comunicação. O processador executa, instrução por instrução, o(s) programa(s) contido(s) na memória. As unidades de entrada/saída compreendem teclado, monitor, unidades de memória, meios de armazenamento secundário (discos, fitas magnéticas), impressoras etc. Elas permitem a introdução de dados e a saída dos resultados. As unidades de comunicação possibilitam a relação do computador com os terminais ou com outros computadores organizados em rede. Os softwares são escritos numa linguagem que o computador é capaz de traduzir numa série limitada de instruções elementares

[1] Dicionário Aurélio Online. Disponível em: <http://www.dicionariodoaurelio.com>. Acesso em 20 ago. 2013.

> diretamente executáveis pelos circuitos eletrônicos. O encadeamento das instruções é suscetível de ser alterado pelos próprios resultados das operações efetuadas ou pela chegada de novas informações vindas do exterior. A função de um computador limita-se a ordenar, classificar, calcular, escolher, procurar, editar ou representar informações antes codificadas segundo uma representação binária.

Em suma, computador pode ser conceituado como um instrumento capaz de receber comandos e executá-los sobre dados fornecidos de forma muito ágil.

Para se analisar a origem do computador, deve-se voltar no tempo para o ano de 2500 a.C., onde, no Oriente Médio, já existia o primeiro modelo primitivo de Ábaco, que era uma máquina de calcular mecânica. Com ela, romanos e egípcios computavam transações através do *calculi*[2].

Já no século XVII, por volta do ano de 1642, Blaise Pascal inventou a primeira máquina de calcular automática, que possibilitava realizar operações de soma e subtração com números de até oito algarismos.

Em 1964, a máquina de Pascal serviu de base para Gottfried Wilhelm von Leibniz criar uma calculadora que, além de somar e subtrair, podia também multiplicar, dividir e até mesmo extrair a raiz quadrada dos números. Contudo, estes equipamentos ainda eram meras utensílios de realizar cálculos.

Enquanto o Ábaco de Leibniz realizava diversas operações matemáticas, o computador tão-somente podia realizar operações não muito complexas. Surgiu então a necessidade de se apurar os computadores então existentes, criando mais funções, além da soma e subtração.

Charles Babbage, nos dias de hoje considerado como o pai do computador, com o intuito de trazer mais funções aos computadores, no século XIX, aos redores do ano de 1822, criou o projeto Máquina das Diferenças, que servia para calcular tabelas. Alguns anos depois, em 1833, criou o projeto Máquina Analítica, que trazia a inovação de poder ser programada para realizar os cálculos.

Em 1880, Herman Hollerith, utilizando máquinas especificadamente projetadas, inventou o sistema de perfuração dos cartões para as operações estatísticas.

---

[2] *Calculis* eram pedras de calcário que representavam os números.

Durante a Segunda Guerra Mundial, surgiu a necessidade de realizar os cálculos com maior exatidão visto que era preciso organizar enorme quantidade de armamentos e, também, fazer todo cálculo das tabelas de artilharia. Com isso, John Mauchly e John Eckert, criaram o primeiro computador integralmente eletrônico, chamado de ENIAC (*Eletronic Numerical Integrator and* Computer).

Tratava-se de um computador de grande porte e segundo Fabrízio Rosa (2002, p. 26), “consumia cerca de 150 KW de potência, ocupava 140 m² aproximadamente e pesava cerca de 30 toneladas”.

Depois do ENIAC, que possuía válvulas mecânicas, John Neumann inventou o EDVAC (*Eletronic Discrete Variable Computer*) e, posteriormente, o EDSAC (*Eletronic Delay Storage Automatic Calculator*) e o UNIVAC (*Universal Automatic Computer*), que faziam parte da primeira geração de computadores com válvulas eletrônicas.

Em 1950, substituindo as válvulas eletrônicas por transistores, surge então a segunda geração de computadores.

Nesta mesma geração, o computador, que era essencialmente utilizado para cálculos e operações de guerra anteriormente, passou a ser vendido para civis. Também apareceram as linguagens computacionais de alto nível, o Fortran e Cobol, os softwares e os primeiros sistemas operacionais.

A terceira geração surge em 1958, trazendo como inovação os circuitos integrados, a multiprogramação (sistema operacional executando diversos processos ao mesmo tempo) e o teleprocessamento (processamento à distância).

Na quarta geração os circuitos integrados tornaram-se mais modernos, possuindo maior capacidade de armazenamento e maior agilidade. Apareceram também os microprocessadores e o mainframe (computador de grande porte).

Já na quinta geração, surgiram os computadores menores que apresentavam grandes inovações de software, hardware e também telecomunicações.

De geração em geração, com todo esse desenvolvimento tecnológico, na qual surgiram inúmeras inovações, não se imaginava a dimensão que os computadores tomariam.

Em sua origem e início da evolução, os computadores eram utilizados apenas por pesquisadores, de modo que não se concebia, ainda, a sua aplicação em práticas delituosas, porém, a partir do momento que passaram a ser disseminados, de uso comum, tanto civis quanto pesquisadores, a possibilidade do uso do computador como instrumento para prática de crimes se tornou mais consistente. Com isso, diante de toda essa evolução, começou-se a pensar também na proteção dos direitos que eram atingidos com essas práticas delituosas.

Com a evolução dos meios de comunicação e não muito posterior ao advento do computador, surge a Internet.

Segundo Carla Rodrigues Araújo de Castro (2003, p. 2),

> Internet é uma grande rede de comunicação mundial, onde estão interligados milhões de computadores, sejam eles universitários, militares, comerciais, científicos ou pessoais, todos interconectados. É uma rede de redes, que pode ser conectada por linhas telefônicas, satélites, ligações por micro-ondas ou por fibra ótica.

A origem histórica da internet se dá em 1969, com a ARPA (*Advance Research Projects Agency*), que foi uma experiência do governo norte americano que tinha como objetivo conectar de forma segura e flexível computadores, possibilitando assim que seus pesquisadores pudessem compartilhar recursos de hardware e software. Criou-se então a ARPANET (*Advance Research Projects Agency Network*), que era uma rede capaz de conectar computadores de pesquisadores de quatro universidades norte americanas.

Em 1985, surgiu a NSFNET (*National Science Foundation Network*), que conectava os computadores da NSF (*National Science Foundation*).

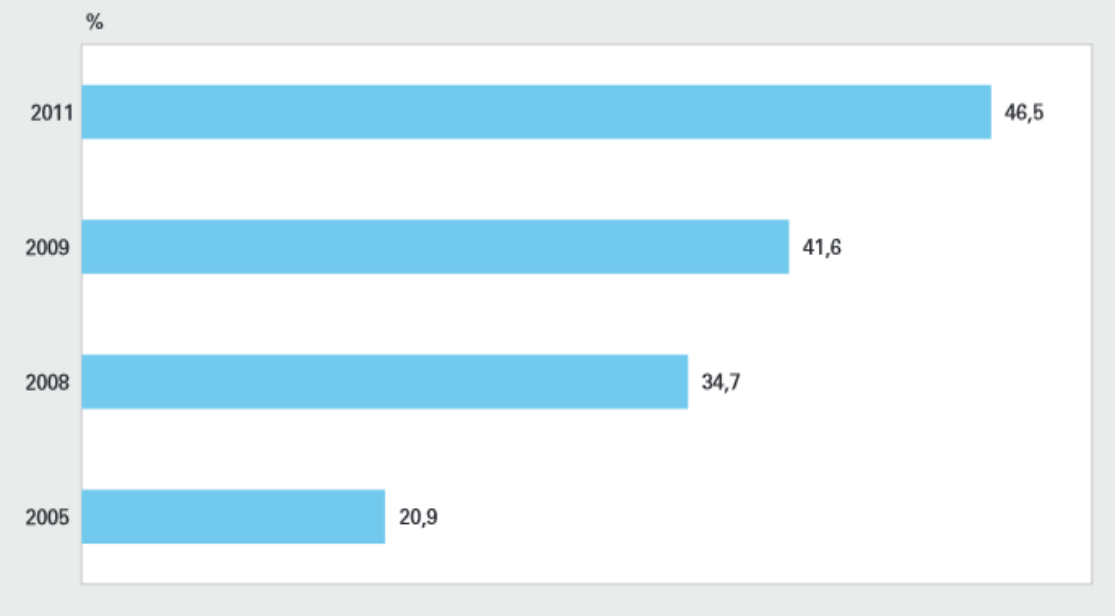
Posteriormente, em 1986, foram interligados os computadores e redes da ARPANET com a NSFNET, formando-se a espinha dorsal da rede, conhecida como *backbone,* e com essa união, toda esta estrutura passou a ser denominada Internet.

Em 1989 é então criada em Genebra a WWW (*World Wide* Web), transformando então a Internet em meio a ser utilizado como objeto de comunicação em massa.

No Brasil, ela foi implementada em 1988, por ação de diversas universidades paulistas e cariocas, como a FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo), a UFRJ (Universidade Federal do Rio de Janeiro) e o LNCC (Laboratório Nacional de Computação Científica).

Um estudo realizado pela PNAD (Pesquisa Nacional por Amostra em Domicílios) realizada durante os anos de 2005, 2008, 2009 e 2011 mostrou um aumento gradativo do número de usuários de Internet.

Figura 1 - Percentual de pessoas que utilizaram a Internet, no período de referência dos últimos três meses, na população de 10 anos ou mais de idade - 2005/2011



Fonte: IBGE, Diretoria de Pesquisas, Coordenação de Trabalho e Rendimento, Pesquisa Nacional por Amostra de Domicílios, 2005/2011

Os resultados da pesquisa mostram que, em 2011, 77,7 milhões de pessoas de 10 anos ou mais de idade acessaram a Internet no período de referência nos últimos três meses. Este contingente equivalia a 46,5% do total da população de 10 anos ou mais de idade. Em 2009, o número de internautas foi estimado em 67,7 milhões, representando 41,6% da população-alvo. Nos anos de 2008 e 2005, estes totais foram estimados em 55,7 milhões (ou 34,7% da população-alvo) e 31,9 milhões (ou 20,9% da população-alvo), respectivamente. De 2005 para 2011, a população de 10 anos ou mais de idade (população em idade ativa) cresceu 9,7%,

enquanto o contingente de pessoas que utilizaram a Internet aumentou 143,8%, ou seja, em seis anos o número de internautas no País cresceu 45,8 milhões.

Avalia-se que aproximadamente 70% de todos estes computadores com acesso à internet no Brasil estão desprotegidos totalmente ou não protegidos de forma suficiente e, sendo tão vulneráveis, tornam-se alvo de fácil invasão.

A Internet é uma grande rede mundial de computadores que conecta bilhões de pessoas, que a utilizam da forma que desejarem, licita ou ilicitamente. E, é nesse ponto que há uma preocupação dos operadores do Direito, diante do grande poder lesivo das condutas realizadas por meio dela.

Assim, a existência e crescimento de uma imensa gama de internautas conectados, com muitos deles totalmente desprotegidos contra possíveis invasões virtuais, evidencia a necessidade premente da criação de mecanismos jurídicos de proteção das informações e dos computadores, para evitar maiores lesões à paz social.

1.2 Relação do direito com a informática

Com o avanço contínuo no mundo informático nota-se, ainda uma enorme revolução nas relações entre os internautas.

Todas as comodidades e facilidades trazidas pela utilização do computador e também da internet modificaram a vida dos brasileiros e de todas as pessoas ao redor do mundo.

Como o uso dos computadores e da internet abrangem diversas áreas, acabam também por alcançar todos ramos do Direito.

Na esfera do direito civil, podem ser destacadas a compra, troca e venda através de leilões, o *e-commerce* (comércio eletrônico), entre outros, sendo que a transação de bens pela internet aumenta cada vez mais e, consequentemente, multiplicam-se os consumidores na rede.

Ainda nesta esfera estão todos os anúncios veiculados por meio da internet, oferecendo serviços de profissionais liberais, como advogados e médicos, fazendo com que tudo seja contratado online.

Na esfera do direito empresarial, podem ser citados o *Home Broker* e o pregão eletrônico, que são formas de compra e venda de ações em tempo real negociadas online.

No ramo do direito do trabalho, com toda essas novas tecnologias, tornou-se comum a contratação de pessoas pela internet, sem nenhuma entrevista entre empregador e empregado. É feita a contratação online e o empregado trabalha diretamente da sua casa, realizando determinadas tarefas utilizando um computador conectado à Internet.

Já no ramo do direito tributário, há muita discussão sobre a incidência ou não de determinados impostos sobre algumas transações realizadas por meio da Internet, já que os fatos geradores àqueles realizados por meio físico.

Como observado, é visível é que toda essa revolução tecnológica atinge os mais diversos ramos do direito, o que possibilita que o “mundo virtual” se torne alvo de criminosos, propiciando o surgimento de novos tipos de crime ou novos meios de praticar os crimes já existentes no Código Penal Brasileiro.

Logo, é precisamente no âmbito do direito penal que o desenvolvimento da informática acabou por gerar situações inusitadas, criando desafios para o legislador, no sentido de prevenir e reprimir a violação de bens jurídicos tutelados pelo direito penal.

É necessário então a aplicação do Direito na Informática, sobretudo na comunicação via Internet, tanto nas relações de direito privado quanto no direito público, e por tais razões é possível notar a crescente criação de legislação específica para este tema, visando preencher as lacunas anteriormente existentes pela ausência de qualquer previsão legal sobre o assunto.

2 CIBERCRIMES

A expressão "cibercrimes" passou a ser utilizada genericamente para designar os delitos cometidos através do uso de aparelhos eletrônicos ou internet.

Para uma melhor compreensão sobre o tema, se faz conveniente a abordagem dos conceitos e classificações dos crimes de informática e também dos meios utilizados para sua prática.

2.1 Conceito

Os crimes virtuais, também chamados de crimes de informática, cibercrimes ou crimes eletrônicos, dentre outras denominações, têm diversos conceitos e também muitas divergências doutrinárias sobre o conteúdo, visto que não há legislação que os definam.

Fabrízio Rosa (2002, p. 53), trata da definição de crime de informática, como:

> [...] a conduta que 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;

Ainda segundo o ilustre autor,

> [...] 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. 54)

Já para Sergio Marcos Roque (2007, p. 25), o conceito de crime de informática é “toda conduta, definida em lei como crime, em que o computador tiver

sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material.”

Outro conceito é o apresentado por João Marcelo de Araújo Junior (1988, p. 460), que diz que ocorre o crime de informática quando há:

> [...] uma conduta lesiva, dolosa, a qual não precisa, necessariamente, corresponder à obtenção de uma vantagem ilícita, porém praticada, sempre, com a utilização de dispositivos habitualmente empregados nas atividades de Informática.

Mais um conceito de destaque é o dado por Augusto Eduardo de Souza Rossini (2004, p. 110), que define o delito informático como:

> Aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.

É notável a grande variedade de conceitos dados pelos doutrinadores, não havendo uma unanimidade sobre qual seria o mais correto.

De forma geral, um conceito simplório para o crime de informática seria a prática de uma conduta, segundo a Teoria Tripartite de Crime, que seja típica, ilícita e culpável, e que atente contra informações ou dados que estejam guardados, compilados, em transmissão ou transmissíveis em computadores, celulares, tablets, dentre outros.

2.2 Classificação

As classificações dos crimes de informática são importantes para a diferenciação dos diversos tipos de crime que podem ser cometidos, e para a verificação de quais já possuem ou não legislação que pode ser aplicada no caso concreto.

Existem muitas possibilidades quanto à classificação dos crimes virtuais. Segundo os ensinamentos de Carlos Maximiliano, especialista em hermenêutica jurídica, não existe classificação boa ou ruim, o que há é uma classificação útil ou inútil. Com isso, viu-se ser mais apropriada a classificação dos crimes de informática em crimes próprios e impróprios.

2.2.1 Crimes virtuais impróprios e próprios

Os crimes virtuais impróprios ou impuros são aqueles em que o computador é utilizado como meio para execução do crime, mas não há afronta ao bem jurídico correspondente à inviolabilidade dos dados ou informações.

A maior parte desses crimes já se encontra tipificada no Código Penal, pois se diferenciam dos demais apenas porque são praticados por meio da informática, sendo que poderiam ser praticados da mesma forma, utilizando-se de outro meio.

Um exemplo de crime virtual impróprio acontece no caso de crime contra a honra cometido por meio da internet, que é tipificado pelo artigo 138, do Código Penal.

Os crimes virtuais próprios ou virtuais puros são os que atingem o bem jurídico inviolabilidade dos dados ou informações, sendo que em tais crimes o único modo para praticá-los é por meio da informática, ou seja, não podem ser praticados por outras formas, como os crimes virtuais impróprios.

Grande parte desses crimes era considerada atípica e apenas com as modificações recentes na legislação penal é que as condutas vêm sendo tipificadas, com a possibilidade de punição.

Um exemplo de crime virtual próprio acontece no caso do recente artigo 313-A, do Código Penal, que preconiza:

> Art. 313-A - Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:
>
> Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa.

2.3 Meios utilizados para prática dos cibercrimes

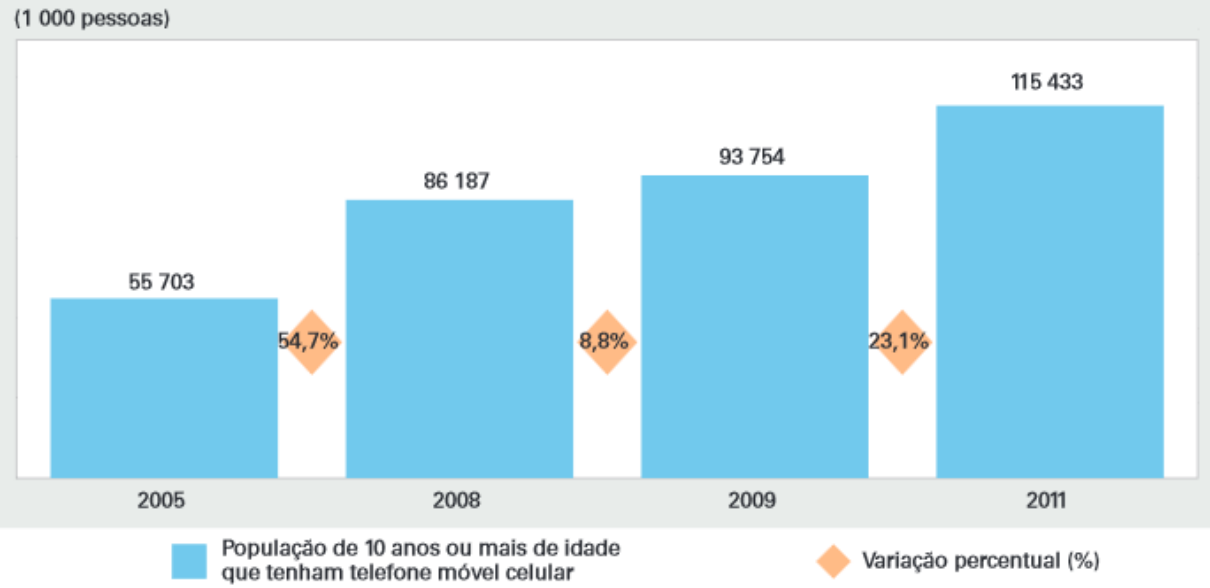
Até o presente momento foi trazido ao trabalho que apenas os computadores e a internet seriam os meios utilizados pelos criminosos para a prática dos cibercrimes.

Atualmente não só os computadores são capazes de armazenar dados e informações, mas também outros diversos dispositivos eletrônicos.

Então, além dos computadores, também podem ser incluídos ao meio utilizado para prática dos delitos informáticos, os tablets e telefones celulares, que não deixam de ser “computadores” e possuem vários dados e informações pessoais que podem ser alvo de condutas criminosas.

As estimativas da PNAD (Pesquisa Nacional por Amostra em Domicílios) realizada pelo IBGE (Instituto Brasileiro de Geografia e Estatística) nos anos de 2005, 2008, 2009 e 2011 mostraram que, neste último ano, o contingente de pessoas de dez anos ou mais de idade que tinham telefone móvel celular para uso pessoal foi estimado em 115,4 milhões, o que correspondia a 69,1% da população. Frente a 2005, quando havia 55,7 milhões de pessoas que possuíam esse aparelho, ou 36,6% da população, o crescimento foi de 107,2%. No mesmo período, a população de 10 anos ou mais de idade do País cresceu 9,7%: de 152,3 milhões de pessoas em 2005 para 167,0 milhões de pessoas em 2011.

Figura 2 - Pessoas e variação do número de pessoas de dez anos ou mais de idade que tinham telefone móvel celular para uso pessoal - Brasil - 2005/2011



Fonte: IBGE, Diretoria de Pesquisas, Coordenação de Trabalho e Rendimento, Pesquisa Nacional por Amostra de Domicílios, 2005/2011

Como o número de brasileiros com celulares também cresceu absurdamente nos últimos anos, é presumível que a prática dos cibercrimes utilizando-os como meio cresceu de forma proporcional.

3 NOVA LEGISLAÇÃO APLICÁVEL AOS CIBERCRIMES

3.1 Considerações gerais

Inicialmente, antes da evolução tecnológica, apenas eram tipificados criminalmente os chamados delitos de informática impuros ou impróprios, que, como explanado no capítulo anterior, são aqueles que são cometidos com ou sem a utilização de um dispositivo informático, ou seja, este é apenas um dos meios possíveis para prática do crime, de modo que a conduta criminosa pode ser abarcada pelo Código Penal Brasileiro, como é o caso do crime de estelionato na Internet, que se enquadra no previsto no artigo 171 do diploma supracitado.

O grande problema encontra-se nos chamados delitos de informática puros ou próprios, que são aqueles que só podem ser praticados por meio do dispositivo informático.

Até mesmo pela revolução tecnológica ocorrida nos últimos tempos, muitas condutas que ofendem bens jurídicos tutelados penalmente, cometidas por meios eletrônicos, são consideradas atípicas. Isto porque, no nosso Direito Penal vigora o princípio da legalidade, ou seja, não haverá crime sem lei anterior que o defina, conforme o art. 5º, XXXIX da Constituição Federal.

Bem por isso que o nosso ordenamento jurídico penal passou a incorporar novas leis, com intuito de tipificar as condutas que caracterizam os crimes virtuais próprios.

Neste contexto ocorreu o advento das leis 12.535/2012 e 12.537/2012, tipificando penalmente condutas ligadas à informática, trazendo agora uma maior proteção para a sociedade brasileira.

3.2 Princípios e direitos constitucionais tutelados

A Constituição Federal do Brasil traz um emaranhado de direitos e garantias fundamentais humanas que formam um conjunto de princípios que, na esfera criminal, são imprescindíveis para o correto funcionamento do poder de punir do Estado.

Primeiramente, quanto aos princípios relacionados com a criação das novas leis pode-se citar o princípio da legalidade e da segurança jurídica.

Na seara penal, o princípio da legalidade, ou também, "nullum crimen nulla poena sine previa lege", é de tamanha importância que além de estar previsto no artigo 1º do Código Penal, também está contido na Constituição Federal, como um de seus direitos fundamentais:

> Art. 1º - Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal.
>
> Art. 5º - Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> [...]
>
> XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal;

Para Guilherme de Souza Nucci (2012, p. 414), o princípio da legalidade “é o princípio central do sistema de direito codificado, guarnecendo a indispensável segurança jurídica no âmbito das figuras típicas incriminadoras, bem como no contexto dos instrumento processuais de persecução penal.”

Este importante princípio relaciona-se com os novos crimes criados porque, anteriormente, como eram condutas antes não tipificadas, não podiam ser punidas pois não havia ilícito penal sem legislação prévia que os definissem. Assim sendo, por força do princípio da legalidade, era necessária lei para que a impunidade deixasse de existir em determinados casos de crimes de informática.

Outros princípios que devem ser considerados neste aspecto são os princípios constitucionais da inviolabilidade da privacidade, intimidade, vida privada e à imagem das pessoas.

Estes princípios constam em nossa Lei Maior como forma de proteção aos direitos fundamentais:

> Art. 5º - Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> [...]
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

Além disso, para Pablo Stolze Gagliano e Rodolfo Pamplona Filho (2010, p. 217):

> O elemento fundamental do direito à intimidade, manifestação primordial do direito à vida privada, é a exigibilidade de respeito ao isolamento de cada ser humano, que não pretende que certos aspectos de sua vida cheguem ao conhecimento de terceiros.

Ao definir os novos crimes cibernéticos, o legislador almejou a proteção do direito à intimidade das pessoas, em manter seus dados e poder dispor dos mesmos da maneira que melhor desejarem.

Outros princípios importantes são da igualdade e da dignidade da pessoa humana que também estão interligados com as inovações legislativas aqui tratadas.

O princípio da igualdade está previsto no caput do artigo 5º da Constituição Federal:

> Art. 5º - Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

Já o princípio da dignidade da pessoa humana encontra-se espalhado por vários dispositivos da Constituição Federal, um desses é o inciso III do artigo 1º:

> Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
>
> [...]
>
> III - a dignidade da pessoa humana;

Tanto o princípio da igualdade quanto o da dignidade da pessoa humana também relacionam-se com a nova legislação informática.

Enfim, demonstra-se que foi de extrema importância a criação dos novos crimes de informática posto que muitos princípios e direitos fundamentais garantidos pela Constituição Federal vinham sendo desrespeitados e violados e nada podia ser feito. Agora há a possibilidade de punição, trazendo uma maior segurança jurídica aos cidadãos brasileiros.

4 LEI 12.535/2012: LEI AZEREDO

4.1 Considerações Iniciais

A lei 12.735/12, a Lei Azeredo, surgiu com a aprovação do projeto de lei 84/99.

O projeto da Lei Azeredo nasceu em 1999 e tinha como objetivo inicial definir vários crimes de informática em seus vinte e três artigos. Surgiram várias emendas a este, inclusive com o conteúdo de alguns projetos de lei incorporados em seu teor, sendo que, após quatro anos, em 2003, foi aprovado pela Câmara dos Deputados.

Após essa primeira aprovação, o projeto de lei, agora no Senado, sofreu algumas reformulações até sua versão final, sendo aprovado definitivamente apenas no ano de 2008.

Posteriormente, mesmo com todas reformas realizadas por ambas as Casas, ainda pairavam diversas polêmicas acerca das inovações trazidas pelo projeto de lei, pois, se fosse aprovado, resultaria em graves consequências para a sociedade, uma vez que criminalizaria atos corriqueiros, como, por exemplo, ser o simples desbloqueio de um celular tipificado como ilícito penal. Por isso, em 2012, após muita discussão, muitos de seus artigos foram retirados, restando apenas poucos deles, que hoje fazem parte da denominada Lei Azeredo.

4.2 Inovações Trazidas

A Lei Azeredo, trouxe modificações na tipificação dos crimes de informática e entrou em vigor no dia 2 de abril de 2013.

O objetivo desta lei é punir indivíduos que cometam crimes de informática próprios ou puros, ou seja, punir àqueles que pratiquem condutas por meio de dispositivos eletrônicos ou informáticos.

Além disso, visa dirimir a atual inconsistência jurídica que os crimes cometidos em ambientes virtuais têm provocado, regulamentando, por exemplo, a questão dos crimes raciais praticados neste ambiente.

Segundo o artigo 1º da lei supracitada,

> Art. 1o Esta Lei 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.

Visível que com a aprovação da Lei Azeredo foram modificados tanto o Código Penal, quanto o Código Penal Militar, em se tratando dos crimes cometidos mediante uso de sistema eletrônico, digital ou similares.

Uma das novidades trazidas pelo legislador foi que agora deve haver uma mobilização, antes não existente, para a criação de setores especializados dentro da polícia e, também, a contratação de pessoal habilitado tecnicamente para apuração dos crimes de informática.

Essencial este ponto trazido pelo 4º artigo da lei. Havendo setores especializados dentro da própria polícia para apuração dos crimes virtuais, todo sistema será mais eficaz, podendo oferecer agilidade na apuração destes crimes e individualizando a conduta do internauta criminoso, diminuindo os índices de impunidade que antes imperavam em se tratando dos crimes virtuais.

Outro importante ponto criado pela lei foi nos casos de crime contra raça ou discriminatórios cometidos por meios informatizados.

Sabe-se que a Lei 7.716 de 5 de janeiro de 1989 é responsável pela tipificação dos crimes raciais praticados no Brasil. Como esta lei é do ano de 1989, época em que a realidade era outra e nem se cogitava da utilização dos computadores e outros meios eletrônicos para cometimento de delitos, seu texto, em muitos pontos, deixava a desejar se comparado com a sociedade que hoje vive-se. Diante da necessidade de adequar os meios utilizados para se cometer o crime de racismo ao contexto atual, foi acrescentado o inciso II do parágrafo 3º do artigo 20 da lei supracitada, que agora vigora com a seguinte redação:

> Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.
>
> [...]
>
> § 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza:
>
> Pena: reclusão de dois a cinco anos e multa.
>
> § 3º No caso do parágrafo anterior, o juiz poderá determinar, ouvido o Ministério Público ou a pedido deste, ainda antes do inquérito policial, sob pena de desobediência:
>
> I - o recolhimento imediato ou a busca e apreensão dos exemplares do material respectivo;
>
> II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio; (grifo da autora)
>
> [...]

Com intuito de ampliar a proteção nos casos de crimes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, o juiz pode determinar que seja retirado o conteúdo ofensivo do respectivo meio no qual foi publicado, inclusive a internet.

Abordando de maneira especifica, vale expor que a novidade quanto aos crimes raciais não instituiu novo ilícito penal, somente constituiu um novo meio pelo qual o crime, já anteriormente previsto, poderá ser cometido.

Se não o mais importante ponto criado com a Lei Azeredo, esta previsão faz com que muitos crimes raciais cometidos pela internet agora passem a ser punidos, sendo tratados de forma mais clara, resguardando os princípios constitucionais da dignidade da pessoa humana e da igualdade.

Comparada ao seu projeto inicial, a Lei Azeredo mostra-se bem sucinta, porém foi o modo encontrado para que sua aprovação ocorresse de forma mais rápida, retirando-se os artigos que eram excessivos, muito amplos e poderiam trazer problemas futuros, como a tipificação de ações corriqueiras dos internautas e que não poderiam ser consideradas como crimes.

Sua complexidade era tão grande que foi alvo de muita discussão, tanto no plenário quanto da população brasileira, que divergiam muito sobre o assunto. Para o criador do projeto, o ex-Senador Eduardo Azeredo, para parte da população que usa o computador de forma “normal” não haveria nenhum impacto.

Já os internautas sentiram que, caso o projeto fosse aprovado, seriam extremamente prejudicados e por isso iniciaram uma petição online para angariar assinaturas e vetar o projeto de lei em questão.

A verdade é que, analisando de forma esmiuçada tudo que o projeto de lei 84/99 trazia, era evidente que não havia como saber quem estava sendo protegido pela lei e quais eram os sujeitos ativos dos crimes, mostrando, assim, falta de segurança jurídica caso o projeto fosse aprovado, pois poderiam ocorrer diversas interpretações para o mesmo texto, abrindo a possibilidade para o abuso de poder e insegurança jurídica em casos determinados.

Mesmo sendo retalhada, ainda assim, a Lei Azeredo tem sua relevância para o mundo jurídico e trouxe inovações muito esperadas pela sociedade brasileira.

5 LEI 12.537/2012: LEI CAROLINA DIECKMANN

5.1 Considerações Iniciais

A lei 12.737/12, também conhecida como Lei Carolina Dieckmann, surgiu com a aprovação do projeto de lei 2793/11.

Em 2011, em paralelo ao projeto da Lei Azeredo, tramitava o Projeto de Lei 2793/11, que trazia uma versão mais enxuta do Projeto de Lei 84/99. Coincidentemente quando aquele projeto de lei foi aprovado, a atriz Carolina Dieckmann teve fotos íntimas subtraídas de seu laptop e foi chantageada para recuperá-las. Como ela não cedeu à chantagem imposta, suas imagens foram publicadas na internet, tornando-se inevitável associar esse evento, que envolvia uma conduta lesiva que utilizava um meio informatizado, ao projeto de lei, que passou então a ser conhecido, após sua aprovação, como Lei Carolina Dieckmann.

Ocorrido esse evento, que gerou grande repercussão na mídia nacional, o legislador deparou-se numa situação em que não podia mais adiar a aprovação dos projetos de lei que estavam em trâmite e versavam sobre os crimes de informática.

Com isso, foram aprovadas e sancionadas as Leis 12.735 e 12.737, ambas editadas em 30 de novembro de 2012.

5.2 Inovações trazidas

A Lei Carolina Dieckmann, trouxe, conforme seus artigos 1º e 2º, modificações ao Código Penal, criando os artigos 154-A e 154-B e alterando os artigos 266 e 298, todos pertencentes ao referido diploma. Esta lei entrou em vigor no dia 2 de abril de 2013.

5.2.1 Análise do artigo 154-A do Código Penal

O artigo 154-A do Código Penal tipifica o crime de “invasão de dispositivo informático” e foi o que trouxe maior modificação dentre todos os criados, tanto pela Lei Azeredo, quanto pela Lei Carolina Dieckmann, possuindo a seguinte redação:

> 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..

Num primeiro exame do artigo supracitado, verifica-se que devem estar presentes elementos do tipo penal para caracterização do delito supracitado:

i. O núcleo invadir;

ii. Dispositivo informático alheio;

iii. Conectado ou não à rede de computadores;

iv. Mediante violação indevida de mecanismo de segurança;

v. Com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo;

vi. Ou instalar vulnerabilidades para obter vantagem ilícita.

Assim, para a exata compreensão deste novo tipo penal, é necessária uma análise pormenorizada de cada um dos elementos mencionados.

5.2.1.1 Classificação Doutrinária

O crime de invasão de dispositivo informático tem as seguintes classificações doutrinárias:

a) Crime comum;

b) Crime plurissubsistente;

c) Crime comissivo, excepcionalmente, comissivo por omissão;

d) Crime formal;

e) Crime instantâneo;

f) Crime monossubjetivo;

g) Crime simples.

É crime comum porque qualquer um do povo pode praticá-lo, não sendo necessária nenhuma característica especial para seu exercício.

É crime plurissubsistente porque são necessários vários atos para sua prática.

É crime comissivo porque deve ser praticado através de uma ação positiva do agente, quais sejam os núcleos do tipo invadir ou instalar. Como exceção pode ser também um crime comissivo por omissão, que são aqueles que seus resultados deveriam ser impedidos pelos seus garantes mas não o foram devido à sua omissão, conforme o artigo 13, §2º do Código Penal.

É crime formal, se consumando sem a necessidade da produção de qualquer resultado naturalístico, contudo este pode acontecer.

É crime instantâneo visto que sua consumação não se prolonga no tempo.

É crime unissubjetivo podendo ser praticado apenas por um agente, não sendo necessárias mais pessoas para configurá-lo. Também é admitido o concurso de pessoas para este crime.

E, por fim, é crime simples porque atenta apenas contra o bem jurídico da inviolabilidade da intimidade da vítima.

5.2.1.2 Objetos jurídico e material

No crime de invasão de dispositivo informático, o objeto jurídico é a inviolabilidade da intimidade e da vida privada que, como discutido em capítulo anterior, é um direito fundamental garantido pela Constituição Federal em seu artigo 5º, inciso X, que preleciona que:

> Art. 5º
>
> [...]
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

Já o objeto material é o “dispositivo informático alheio, conectado ou não à rede de computadores”, conforme o *caput* do artigo 154-A do Código Penal.

Quanto ao núcleo do tipo “invadir”, seus objetos materiais são os dados e as informações guardadas, armazenadas no dispositivo informático da vítima e que tenham sido conseguidas, modificadas ou mesmo excluídas por consequência do ato ilícito do agente.

Em relação ao núcleo do tipo “instalar”, seu objeto material é o próprio dispositivo informático da vítima, pois é neste que o agente instala alguma vulnerabilidade para obter vantagem ilícita.

Aqui deve ser feita uma ressalva quanto às expressões utilizadas pelo legislador pátrio, quais sejam, “dados ou informações”. Estas devem ser interpretadas de forma ampla pois esta foi a intenção do legislador, sendo que, desta forma estendida, podem ser definidas como tudo que a vítima do crime de invasão de dispositivos informáticos possa armazenar nestes, ou seja, senha de contas bancárias, senha de cartões de crédito, fotos, correspondências, vídeos, dentre outros.

Também os dispositivos informáticos, relembrando aqui, visto que já discutidos em capítulo anterior, devem ser interpretados de forma abrangente, incluindo então qualquer hardware que seja adequado para armazenar dados e informações.

Importante aqui salientar sobre os dispositivos informáticos. Estes podem ser desmembrados em quatro grupos diversos:

A) Dispositivos informáticos de processamento: fazem análise dos dados fornecendo informações com o intuito de processar algum dado que é inserido por um dispositivo de entrada e enviado a um outro de saída ou de armazenamento. São exemplos deste tipo de dispositivo os processadores de computadores e smarthphones, as placas de vídeo, entre outros.

B) Dispositivos informáticos de entrada: fazem a inserção de dados no sistema ao qual pertencem. São exemplos deste tipo de dispositivo os microfones, webcams e teclados.

C) Dispositivos informáticos de saída: fazem a exibição de todos os dados e também informações processadas pelo computador. São exemplos deste tipo de dispositivo as impressoras e os monitores de vídeo.

D) Dispositivos informáticos de armazenamento: como o próprio armazenamento de dados e também informações para uso futuro. São exemplos deste tipo de dispositivo os pendrives, os hard disks, os CD's e os DVD's.

Além de todas essas informações, deve-se atentar que o legislador claramente previu que o dispositivo informático tem que ser de outra pessoa, ou seja, se este for próprio e estiver sob a posse de outra pessoa a conduta será atípica.

Outro ponto a ser destacado aqui é que não importa se o dispositivo informático alheio está conectado ou não à internet ou outra rede.

5.2.1.3 Sujeitos do delito

Como já comentado no começo da análise do art. 154-A do Código Penal, o crime de invasão de dispositivo informático é comum, ou seja, seu sujeito ativo pode ser qualquer pessoa, não sendo necessária nenhuma característica especial para que seja praticado.

Mesmo sendo crime comum, na maioria dos casos os crimes são praticados por crakers[3].

Já o sujeito passivo também pode ser qualquer pessoa que, como consequência da conduta ilícita praticada pelo sujeito ativo, sofra o dano moral ou material de ter seus dados ou informações obtidos de forma indevida, modificados ou excluídos ou também se forem instaladas vulnerabilidades para obter vantagem ilícita.

5.2.1.4 Conduta típica

O verbo invadir tem como definições “entrar violentamente em”, “espalhar-se”, “apoderar-se de”, entre outros.

No mundo jurídico, em específico no *caput* do art. 154-A do Código Penal, o núcleo do tipo invadir tem o sentido de adentrar sem prévia autorização do proprietário do dispositivo informático, conectado ou não à internet.

Ainda analisando o *caput*, a expressão “mediante violação indevida de mecanismo de segurança” traz dois importantes pontos a serem enfatizados para configuração do crime em questão.

Primeiramente a violação do dispositivo informático deve ser indevida, ou seja, sem motivo ou sem legitimidade, pois se a invasão for devida, como ocorre nos casos de agentes da Polícia que possuem autorização judicial para realizar esta medida, a conduta será atípica.

O segundo ponto é que o sistema do dispositivo informático alheio deve conter algum mecanismo de segurança instalado, ou seja, indicando que o sistema tem que estar protegido anteriormente, para ocorrer então a sua violação e,

[3] *Crackers* são elementos mal intencionados, que estudam e decodificam programas e linguagens a fim de causar danos a computadores alheios. A intenção é invadir e sabotar sistemas, quase sempre objetivando a captação de dados passíveis de render cifras. Ou seja, roubo eletrônico, estelionato ou o que quer que seja. A intenção é definitivamente ruim. Disponível em: <http://www.sisnema.com.br/Materias/idmat014717.htm>. Acesso em 29 set. 2013.

assim, configurar o crime do artigo 154-A do Código Penal. Caso o sistema esteja desprotegido, a invasão não poderá ser punida, nos termos desse dispositivo.

5.2.1.5 Elemento subjetivo

Aqui estão presentes tanto o dolo genérico quanto o dolo específico.

O dolo genérico repousa no fato de que o agente quer cometer o crime com vontade livre e consciente de que está invadindo dispositivo informático alheio protegido por dispositivo de segurança indevidamente ou quer instalar vulnerabilidades para torná-lo totalmente sem proteção.

E por fim, ponderando as expressões “com o fim de” e “para obter vantagem ilícita”, verifica-se a presença do elemento subjetivo específico, ou seja, o criminoso, para configurar o crime, deve praticá-lo com as finalidades de adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Para este crime não é prevista a modalidade culposa.

5.2.1.6 Consumação e tentativa

Como o crime em tela tem consumação antecipada, ou seja, trata-se de um crime formal, não é imperativa a produção de nenhum resultado naturalístico para que se consume, mesmo que, eventualmente, este venha a ocorrer.

Assim sendo, há a consumação deste crime quando ocorre a invasão do dispositivo informático alheio ou a instalação de qualquer vulnerabilidade, não tendo a mínima importância se o objetivo do agente foi ou não alcançado.

Já quanto a tentativa, tratando-se de crime plurissubsistente, como já explicado anteriormente, é possível visto que como possuem diversos atos, fracionando o *iter criminis*, de sorte que é possível que o agente seja impedido de

consumar o crime em um destes atos e que ocorra então sua prática apenas na forma tentada.

5.2.1.7 Figura típica equiparada

O parágrafo 1º do art. 154-A do Código Penal traz a forma equiparada ao crime de invasão de dispositivo informático. Diz que “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.”

São núcleos da forma equiparada:

A) Produzir: efetuar, elaborar, executar, fabricar, fazer, manufaturar, montar, realizar;

B) Oferecer: exibir, expor, mostrar, ostentar;

C) Distribuir: dar, transmitir, entregar;

D) Vender: alienar, ceder, transferir;

E) Difundir: alastrar, despargir, desparzir, disseminar, espargir, esparzir, grassar.

O agente que pratica qualquer desses núcleos, ou seja, produção, oferecimento, distribuição, venda ou difusão de dispositivo ou programa de computador que ajude na invasão de dispositivos informáticos alheios, comete o crime do parágrafo primeiro do art. 154-A do Código Penal.

Além disso, para configurar este crime deve estar presente o elemento subjetivo específico, que é o intuito de ajudar na prática da conduta prevista pelo *caput* do artigo supracitado.

Esta é uma exceção à Teoria Monista prevista no *caput* do artigo 29 do Código Penal, haja vista que quem invade o dispositivo alheio responde por um

crime, já quem o ajuda, disponibilizando dispositivo ou programa de computador, responde por outro crime diferente.

5.2.1.8 Figuras típicas qualificadas

O parágrafo 3º do artigo 154-A do Código Penal traz a forma qualificada do crime de invasão de dispositivo informático, da seguinte forma,

> § 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.

Trata-se de crime qualificado porque, devido a presença de certas circunstâncias não previstas no *caput* do artigo, torna o crime mais grave e, portanto, tem também uma pena mais elevada, alterando os mínimo e máximo da pena abstrata prevista para o tipo simples.

Diferentemente do *caput* do artigo, no parágrafo 3º exige-se o resultado naturalístico para que ocorra a consumação do crime, ou seja, o crime aqui não é formal e é necessária “a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas”.

Só será imposto este crime qualificado se não existir outro crime mais gravoso em que se encaixe a conduta, ou seja, sua aplicação é subsidiária e está expressamente descrita no tipo penal.

Esta qualificadora tem a intenção de punir àqueles que, além de invadirem dispositivos informáticos alheios, conseguiram conteúdo de comunicações eletrônicas privadas, tais como e-mails, mensagens particulares das redes sociais; segredos comerciais ou industriais, tais como uma estratégia para lançamento de um novo produto no mercado; ou informações sigilosas definidas em lei e, como ainda não há lei nesse sentido, trata-se de norma penal em branco.

Também será aplicada qualificadora no caso de acesso remoto não autorizado do dispositivo alheio, ou seja, através de algum programa que o agente possa acessar de qualquer ambiente o aparelho informático da vítima, controlando-o sem o consentimento desta. Se o acesso for permitido, não há que se pensar no crime disposto neste tipo penal, já que se trataria de conduta atípica.

5.2.1.9 Causas de aumento de pena

As causas de aumento de pena estão previstas nos parágrafos 2º, 4º e 5º do art. 154-A do Código Penal.

O acréscimo de pena trazido pelo parágrafo 2º será aplicado quando houver qualquer tipo de prejuízo econômico à vítima do crime de invasão de dispositivo informático.

Prejuízo econômico é aquele no qual há prejuízo material, uma perda financeira, de algum valor econômico. Não está inserido então neste aumento de pena quando só há prejuízo moral à vítima.

Já o parágrafo 4º trata exclusivamente de um aumento de pena para a forma qualificada do crime de invasão de aparelho informático de outra pessoa, ou seja, havendo o agente praticado o crime previsto no art. 154-A, § 3º, do Código Penal, este terá sua pena aumentada “se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos”.

Vale ressaltar que, como o legislador trouxe a expressão “a qualquer título”, mesmo que se já realizada divulgação, comercialização ou transmissão de forma gratuita (sem contraprestação) o crime restará configurado com aumento de pena.

E, finalmente, o parágrafo 5º trata de causa de aumento de pena imposta se os sujeitos passivos do crime forem determinadas pessoas.

São elas:

> 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..

Sanção mais rigorosa imposta neste caso por se tratarem de pessoas ligadas à gestão pública e que muitas vezes em seus dispositivos informáticos possuem informações e dados de extrema importância pública.

Aplicam-se aos crimes previstos no art. 154-A do Código Penal, tanto nas formas simples, equiparada ou qualificada o disposto na Lei 9.099/1995 – Lei do Juizado Especial Criminal.

Isto porque, como as penas cominadas não ultrapassam dois anos, ou seja, por se tratarem de infrações de menor potencial ofensivo, estas condutas são compatíveis com a lei do JECRIM.

5.2.2 Análise do artigo 154-B do Código Penal

Outro artigo criado pela Lei 12.737/2012 foi o 154-B, que trata sobre o tipo de ação penal do crime previsto no artigo 154-A, que preconiza que:

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

Em suma este dispositivo traz que nos casos dos crimes do artigo 154-A, a ação penal procede apenas mediante representação, ou seja, ação penal pública condicionada. Exceção se faz nos casos em que o crime é praticado contra a administração pública de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra concessionárias de serviços públicos, onde a ação penal será pública incondicionada.

Uma crítica que deve ser feita tanto ao artigo 154-A e 154-B é que é utilizada no texto dos referidos artigos a expressão “invasão”, sendo também exigida que essa invasão se dê mediante infração de máquina de segurança, o que torna mais difícil o enquadramento nos crimes, pois em muitas das vezes o ingresso indevido a aparelhos eletrônicos, de celular e computadores não exige nenhuma superação de barreiras para se consumar, ou seja, não há mecanismos de segurança instalados em determinados dispositivos informáticos.

Além desta crítica, vale ressaltar que no texto dos artigos supra é trazido que os crimes devem ser cometidos com o fim de obtenção, adulteração ou destruição de dados ou informações, o que não abrange, embora carecesse, o simples acesso para outros fins que não os listados.

Outro ponto, também já comentado e agora criticado, trazido pelo caput do artigo 154-A, é que as vulnerabilidades instaladas têm que ter o fim de obter vantagem ilícita, ou seja, não abarca aqueles indivíduos que façam esta instalação sem interesses contrários a lei.

E por último, o parágrafo primeiro do artigo 154-A diz que “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”. Existem questionamentos quanto aos limites de eficácia deste parágrafo, pois os programadores e fornecedores de equipamentos e de softwares de segurança eletrônica poderiam se enquadrar nesta conduta descrita. Contudo, não parece ser o caso, visto que a caracterização do delito depende do preenchimento de todos os elementos contidos no referido tipo penal.

5.2.3 Análise do artigo 266 do Código Penal

Além da concepção do novo tipo penal, a aludida lei ainda modificou o artigo 266 do mesmo diploma, que trata da interrupção do serviço telegráfico ou telefônico, incluindo o serviço telemático ou de informação de utilidade pública.

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
>
> Pena - detenção, de 1 (um) a 3 (três) anos, e multa.
>
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. (grifo meu)
>
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

O intuito do legislador, ao criar este dispositivo, foi proteger os usuários da rede mundial de computadores contra ataques *DDoS*[4], o que vem sendo um problema principalmente para empresários que oferecem serviços de utilidade pública pela internet, visto que com esses ataques estes serviços podem se tornar indisponíveis, acarretando grandes prejuízos, tanto para os fornecedores de serviços quanto para os usuários dos mesmos.

Neste ponto vale salientar que o legislador já havia previsto no artigo 265 do Código Penal que atentar contra segurança ou funcionamento de serviço de utilidade pública constituía crime, porém a criação do parágrafo 1º do artigo 266 do Código Penal serviu para cobrir qualquer situação não abarcada pelo artigo 265 e prevenir contra qualquer alegação de conduta atípica.

A crítica a ser feita quanto ao artigo 266, em seu parágrafo primeiro, é que apenas trouxe previsão quanto aos serviços de utilidade pública, mostrando-se insuficiente, pois excluem a tipificação criminal de todos aqueles serviços de informação que não tenham esta finalidade pública.

5.2.4 Análise do artigo 298 do Código Penal

Finalmente, o artigo 298 do Código Penal, que agora conta com o seguinte texto:

---

[4] *DDoS (Distributed Denial of Service)* constitui um ataque de negação de serviço distribuído, ou seja, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet. Normalmente estes ataques procuram ocupar toda a banda disponível para o acesso a um computador ou rede, causando grande lentidão ou até mesmo indisponibilizando qualquer comunicação com este computador ou rede. Disponível em: <http://www.terra.com.br/informatica/especial/cartilha/conceitos_11_1.htm>. Acesso em: 25 set. 2013.

> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
>
> Pena - reclusão, de 1 (um) a 5 (cinco) anos, e multa.
>
> Falsificação de Cartão
>
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. (grifo meu)

Este artigo também alterado com o advento da lei em tela e foi modificado com o intuito de sanar qualquer dúvida sobre o conceito de documento particular, trazendo para o rol desses documentos os cartões de crédito, que é um meio pelo qual ocorrem muitos crimes de informática.

6 O MARCO CIVIL DA INTERNET

Após a análise pormenorizada das leis 12.735/12 e 12.737/12, é perceptível que, mesmo com a edição destas é previsível que a impunidade por meio da Internet ainda continuará acontecendo, posto que é difícil provar e apurar a autoria dos crimes virtuais em determinados casos.

No decorrer do desenvolvimento e finalização do presente trabalho, foi aprovada e sancionada a Lei 12.965 de 23 de abril de 2014.

Esta nada mais é que a lei que derivou do projeto de lei 2126/11 e que ficou conhecida como o Marco Civil da Internet.

Com a aprovação desta lei, que tem *vacacio legis* de 60 dias, ou seja, passará a vigorar no final de junho deste ano, foram estabelecidas diversas premissas, dentre elas, direitos e obrigações aos usuários, tanto internautas quanto provedores de serviços da rede mundial de computadores no Brasil.

Ficando conhecida como “constituição dos internautas e provedores”, esta lei veio para complementar as leis Carolina Dieckmann e Azeredo, pois em muitos pontos abarca situações não tratadas por estas últimas.

Como já comentado, o projeto lei esteve em trâmite deste 2011, e devido as invasões norte americanas das informações veiculadas pela rede brasileira, sua aprovação foi acelerada, sendo isso fator determinante para que a aprovação ocorresse.

O projeto da lei surgiu no ano de 2009, sendo que sua ideia original apareceu em 2007, após intensa discussão acerca de uma das leis objeto do presente estudo, a Lei Azeredo.

Após árduo debate por toda a rede brasileira, em 2011, o projeto de lei finalmente surgiu, sendo aprovado pela Câmara dos Deputados em 25 de março de 2014, no Senado Federal em 23 de abril de 2014, ocorrendo a sanção imediatamente pela presidente Dilma Rousseff na mesma data.

Sendo uma lei recente e que ainda não vigora em nosso sistema jurídico, não há ainda como saber quais serão as consequências jurídicas de seu uso.

Já em seu 1º artigo, a lei determina que:

> Art. 1o Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Logo após, nos artigos seguintes, traz todos os princípios, garantias e direitos fundamentais que disciplinam o uso da internet no Brasil.

Em suma, os pontos de maior relevância trazidos no Marco Civil da Internet são:

a) Princípio da neutralidade na rede: a rede precisa ser idêntica para todos, sem distinção quanto ao tipo de uso, quer dizer, o internauta poderá acessar o que desejar, não importando o conteúdo e, pagará conforme o volume e velocidade de acesso especificados no contrato.

b) Princípio da privacidade na rede: a privacidade deve ser garantida para todos os usuários, e apenas mediante ordens judiciais no processo de investigação de crimes será admissível ter acesso a estas informações veiculadas pelos usuários. Além disso, as empresas fornecedoras de serviços da internet devem garantir que os conteúdos veiculados só sejam acessados por quem os emitiu e para quem os mesmos foram destinados, cabendo inclusive sanções administrativas, penais e cíveis caso haja quebra de sigilo dessas informações.

c) Logs ou registros de acessos: os provedores de serviços de internet devem manter os registros de acesso armazenados pelo período de

> um ano, podendo este prazo ser prorrogado. Estes logs podem ser requeridos por meio de autorização judicial pedida pelo requerente. Esta previsão trouxe uma benesse na apuração dos crimes de informática, pois com o log de acesso torna-se possível a inquirição do provável autor do crime de informática de maneira mais rápida e simples.

De forma geral, esta lei só veio a acrescentar e melhorar a apuração dos crimes virtuais, delimitando de maneira mais clara o que pode ser feito e o que não pode ser feito no ambiente virtual brasileiro.

7 CONCLUSÃO

As modificações trazidas pelas leis 12.735/2012 e 12.737/2012 eram necessárias para diminuição da impunidade frente aos crimes de informática.

A Lei 12.735/2012 derivou de um projeto de lei que tramitava desde 1999 na Câmara dos Deputados e no Senado Federal, que após diversas reformas, sendo retirados inúmeros artigos, resultou na enxuta Lei Azeredo, que traz como principais previsões a criação de delegacias especializadas e o combate aos crimes de racismo cometidos pela internet.

A Lei 12.737/2012 acarretou uma novidade ao panorama legal penal, acolhendo à vontade da comunidade jurídica e de toda a coletividade que presenciavam algumas condutas na internet, tidas como danosas aos indivíduos, contudo, permaneciam silentes quanto ao combate destas em virtude da carência de previsão no Código Penal.

É evidente que estas modificações não são suficientes para abranger todos os crimes de informática, visto que a tecnologia da informação marcha em passos largos e o direito em passos curtos.

Mesmo assim, a criação dessas leis foi significativa e, embora essa inovação ainda não seja suficiente para proteger integralmente os bens jurídicos que podem ser atingidos pela via eletrônica, já foi um primeiro passo para criação e aprovação de novas leis tratando dos crimes de informática, como o Marco Civil da Internet.

É necessário, todavia, lembrar que as leis em estudo não têm o teor de extinguir os crimes de informática. Isto porque, convivemos num mundo em contínuo progresso tecnológico, de tal modo que a legislação penalista tende a não acompanhar o advento de novas condutas danosas a bens considerados importantes para a sociedade brasileira.

Os novos crimes de informática, frutos da evolução tecnológica, demandam bem mais que um texto de lei regulamentando comportamentos delituosos. Tais ilícitos carecem ainda serem afrontados por um processo de investigação mais cuidadoso, pois a maior parte das condutas delituosas praticadas por meio da rede mundial abarca a ação de um indivíduo com amplos conhecimentos de computadores e internet e, com isso, não importa se há diversos tipos penais incriminadores, se o judiciário, os membros do Ministério Público e as policias não se encontram comprometidos, dispostos e prontos tecnicamente na precaução e contenção destes delitos.

Conclui-se, finalmente, que a mera edição de novas leis não será eficaz para o combate aos crimes de informática, já que também é necessário investimento na criação de novos meios de apuração dos crimes, ou seja, na criação de delegacias especializadas e também no treinamento de todos os envolvidos no processo de investigação dos crimes de informática, restabelecendo assim a segurança jurídica, garantindo a paz social e a manutenção do Estado Democrático de Direito.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Wesley Almeida. **Crimes na internet**: uma realidade na sociedade de informação. Presidente Prudente, 2006. 57 f. Monografia (Graduação) - Faculdades Integradas 'Antônio Eufrásio de Toledo', Faculdade de Direito de Presidente Prudente, 2006.

BARRETTO, Ana Carolina Horta. **O direito e a internet**. 1. ed. Rio de Janeiro: Forense Universitária, 2002.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília: Senado, 1988.

BRASIL. Decreto Lei nº 2.848, de 07 de dezembro de 1940. **Código Penal**. Brasília. Disponível em: <www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 22 abr. 2013.

BRASIL. **Lei nº 7.716, de 05 de janeiro de 1989**. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l7716.htm>. Acesso em: 22 abr. 2013.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 22 abr. 2013.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acesso em: 22 abr. 2013.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Brasília. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm>. Acesso em: 24 abr. 2014.

BRASIL. Câmara dos Deputados. **Projeto de Lei Nº 84, de 1999**. Brasília. Disponível em: <http://imagem.camara.gov.br/Imagem/d/pdf/DCD11MAI1999.pdf#page=59> . Acesso em: 22 abr. 2013.

BRASIL. Câmara dos Deputados. **Projeto de Lei Nº 2793, de 2011**. Brasília. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=944218&filename=PL+2793/2011>. Acesso em: 22 abr. 2013.

BRASIL. Câmara dos Deputados. **Projeto de Lei Nº 2126, de 2011**. Brasília. Disponível em: < http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=912989&filename=PL+2126/2011>. Acesso em: 24 abr. 2014.

CABETTE, Eduardo Luiz Santos. Primeiras impressões sobre a Lei nº 12.737/12 e o crime de invasão de dispositivo informático. **Jus Navigandi**. Disponível em: <http://jus.com.br/revista/texto/23522/primeiras-impressoes-sobre-a-lei-no-12-737-12-e-o-crime-de-invasao-de-dispositivo-informatico>. Acesso em: 22 abr. 2013.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**. 2. ed., rev., ampl. e atual. Rio de Janeiro: Lumen Juris, 2003.

CAVALCANTE, Márcio André Lopes. Primeiros comentários à Lei n.° 12.737/2012, que tipifica a invasão de dispositivo informático. **Dizer Direito.** Disponível em: <http://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html>. Acesso em: 22 abr. 2013.

COELHO, Ana Carolina Assis Coelho. **Crimes virtuais**: análise da prova. 2008. 48 f. Monografia (Graduação) - Faculdades Integradas 'Antônio Eufrásio de Toledo', Faculdade de Direito de Presidente Prudente, 2008.

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

DERECHO de internet. Buenos Aires: Heliasta, 2004.

DIREITO & internet: aspectos jurídicos relevantes . Bauru, SP: EDIPRO, 2001.

DIREITO, sociedade e informática: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000.

FACULDADES INTEGRADAS “ANTONIO EUFRÁSIO DE TOLEDO”. **Normalização de apresentação de monografias e trabalhos de conclusão de curso.** 2007 – Presidente Prudente, 2007, 110p.

FERREIRA, Lóren Pinto. Os “crimes de informática” no direito penal brasileiro. **OAB**. Disponível em: <http://www.oab.org.br/editora/revista/revista_08/anexos/crimes_de_informatica.pdf>. Acesso em: 22 abr. 2013.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo Mário. **Novo curso de direito civil**: abrangendo os códigos civis de 1916 e 2002. 12. ed., rev. e atual. São Paulo: Saraiva, 2010-2011.

GRECO, Marco Aurelio; MARTINS, Ives Gandra da Silva; WALD, Arnoldo. **Direito e internet**: relações jurídicas na sociedade informatizada. São Paulo: Revista dos Tribunais, 2001.

GRECO, Rogério. **Curso de direito penal**. 12. ed., rev., ampl. e atual. Niterói: Impetus, 2010.

IBGE, Instituto Brasileiro de Geografia e Estatística. **Acesso à Internet e posse de telefone móvel celular para uso pessoal 2011 – PNAD**. Disponível em: <http://www.ibge.gov.br/home/estatistica/populacao/acessoainternet2011/default.shtm>. Acesso em: 29 ago. 2013.

IBGE, Instituto Brasileiro de Geografia e Estatística. **Acesso à Internet e posse de celular.** Disponível em: <ftp://ftp.ibge.gov.br/Acesso_a_internet_e_posse_celular/2011/PNAD_Inter_2011.pdf>. Acesso em: 29 ago. 2013.

ISHIDA, Válter Kenji. **As modificações promovidas pela Lei Carolina Dieckmann no Código Penal**. Disponível em: <http://www.cartaforense.com.br/conteudo/artigos/as-modificacoes-promovidas-pela-lei-carolina-dieckmann-no-codigo-penal/9986>. Acesso em: 22 abr. 2013.

LENZA, Pedro. **Direito constitucional esquematizado**. 14. ed., rev., atual. e ampl. São Paulo: Saraiva, 2010.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. Campinas: Millennium, 2006.

MARQUES, Jader. **O direito na era digital**. Porto Alegre: Livraria do Advogado, 2012.

MASSON, Cleber. **Direito penal esquematizado**: parte especial. 5. ed. rev., atual. e ampl. Rio de Janeiro: Forense, São Paulo: Método, 2013.

MASSON, Cleber. **Direito penal esquematizado**: parte geral. 7. ed. rev., atual. e ampl. São Paulo: Método, Rio de Janeiro: Forense, 2013.

MONTEIRO NETO. João Araújo. **Crimes informáticos uma abordagem dinâmica ao direito penal informático**. Fortaleza, Pensar. 2003.

NOGUEIRA, Sandro D'Amato. **Crimes de informática**. 1. ed. Leme, SP: BH, 2008.

NUCCI, Guilherme de Souza. **Princípios constitucionais penais e processuais penais**. 2. ed. São Paulo: Revista dos Tribunais, 2012.

PAESANI, Liliana Minardi. **Direito e internet**: liberdade de informação, privacidade e responsabilidade civil. São Paulo: Atlas, 2000.

PAULINO, José Alves. **Crimes de informática**. Brasília: Projecto Editorial, 2001.

PECK, Patricia. **Direito digital**. 5.ed. rev., atual. e ampl. São Paulo: Saraiva, 2013.

QUALISERVE. **Computadores brasileiros estão entre os mais vulneráveis do mundo**. Disponível em: <http://www.qualiserve.com.br/wordpress/?p=51>. Acesso em: 30 ago. 2013.

REIS, Maria Helena Junqueira. **Computer crimes**: a criminalidade na era dos computadores. Belo Horizonte: Del Rey, 1997.

ROHRMANN, Carlos Alberto. **Curso de direito virtual**. Belo Horizonte: Del Rey, 2005.

ROQUE, Sérgio Marcos. **Criminalidade Informática** – Crimes e Criminosos do Computador. 1 ed. São Paulo: ADPESP Cultural, 2007.

ROSA, Fabrízio. **Crimes de informática**. 1. ed. Campinas: Bookseller, 2002.

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

SANTOS, Fernando da Cruz Alves. **Aspectos relevantes da criminalidade através da informática**. Presidente Prudente, 2003. 59 f. Monografia (Graduação) - Faculdades Integradas Antônio Eufrásio de Toledo, 2003.

TAKUSHI, Tiago Tadashi. **Crimes virtuais**: aspectos gerais, persecução criminal e de competência. Presidente Prudente, 2009. 72 f. Monografia (Graduação) - Faculdades Integradas Antônio Eufrásio de Toledo, 2009.

TOMIZAWA, Guilherme. **A invasão de privacidade através da internet**. 1. ed. Curitiba: J M Livraria Jurídica, 2008.

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

ANEXOS

ANEXO A – Lei Nº 12.735, de 30 de novembro de 2012

LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012.

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 PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1o Esta Lei 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.

Art. 2o (VETADO)

Art. 3o (VETADO)

Art. 4o Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Art. 5o O inciso II do § 3o do art. 20 da Lei no 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

“Art. 20. .....

.....

§ 3o .....

.....

II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;

.....” (NR)

Art. 6o Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

Brasília, 30 de novembro de 2012; 191o da Independência e 124o da República.

DILMA ROUSSEFF

José Eduardo Cardozo

Paulo Bernardo Silva

Maria do Rosário Nunes

Este texto não substitui o publicado no DOU de 3.12.2012

ANEXO B – Lei Nº 12.737, de 30 de novembro de 2012

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

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."

"Ação penal

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

Art. 3o Os arts. 266 e 298 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Art. 266. .....

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2o Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública." (NR)

"Falsificação de documento particular

Art. 298. .....

Falsificação de cartão

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito." (NR)

Art. 4o Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

Brasília, 30 de novembro de 2012; 191o da Independência e 124o da República.

DILMA ROUSSEFF
José Eduardo Cardozo

ANEXO C – Lei Nº 12.965, de 23 de abril de 2014

LEI Nº 12.965, DE 23 ABRIL DE 2014.

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1o Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Art. 2o A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:

I - o reconhecimento da escala mundial da rede;

II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração;

V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VI - a finalidade social da rede.

Art. 3o A disciplina do uso da internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

IV - preservação e garantia da neutralidade de rede;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 4o A disciplina do uso da internet no Brasil tem por objetivo a promoção:

I - do direito de acesso à internet a todos;

II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e

IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Art. 5o Para os efeitos desta Lei, considera-se:

I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

II - terminal: o computador ou qualquer dispositivo que se conecte à internet;

III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;

V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e

VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Art. 6o Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

CAPÍTULO II
DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7o O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;

V - manutenção da qualidade contratada da conexão à internet;

VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Art. 8o A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:

I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

CAPÍTULO III
DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

Seção I
Da Neutralidade de Rede

Art. 9o O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

§ 1o A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:

I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e

II - priorização de serviços de emergência.

§ 2o Na hipótese de discriminação ou degradação do tráfego prevista no § 1o, o responsável mencionado no caput deve:

I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei no 10.406, de 10 de janeiro de 2002 - Código Civil;

II - agir com proporcionalidade, transparência e isonomia;

III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

§ 3o Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

Seção II
Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1o O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7o.

§ 2o O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7o.

§ 3o O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

§ 4o As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1o O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2o O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3o Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4o Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.

Subseção I
Da Guarda de Registros de Conexão

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1o A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2o A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.

§ 3o Na hipótese do § 2o, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.

§ 4o O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2o, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3o.

§ 5o Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6o Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Subseção II
Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão

Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.

Subseção III
Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1o Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de

acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2o A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3o e 4o do art. 13.

§ 3o Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4o Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7o; ou

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

Art. 17. Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

Seção III
Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros

Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

§ 1o A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

§ 2o A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a

liberdade de expressão e demais garantias previstas no art. 5o da Constituição Federal.

§ 3o As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.

§ 4o O juiz, inclusive no procedimento previsto no § 3o, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.

Parágrafo único. Quando solicitado pelo usuário que disponibilizou o conteúdo tornado indisponível, o provedor de aplicações de internet que exerce essa atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização.

Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

Seção IV
Da Requisição Judicial de Registros

Art. 22. 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.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros.

Art. 23. Cabe ao juiz tomar as 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.

CAPÍTULO IV
DA ATUAÇÃO DO PODER PÚBLICO

Art. 24. Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da internet no Brasil:

I - estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica;

II - promoção da racionalização da gestão, expansão e uso da internet, com participação do Comitê Gestor da internet no Brasil;

III - promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, para permitir o intercâmbio de informações e a celeridade de procedimentos;

IV - promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade;

V - adoção preferencial de tecnologias, padrões e formatos abertos e livres;

VI - publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada;

VII - otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País, promovendo a qualidade técnica, a inovação e a difusão das aplicações de internet, sem prejuízo à abertura, à neutralidade e à natureza participativa;

VIII - desenvolvimento de ações e programas de capacitação para uso da internet;

IX - promoção da cultura e da cidadania; e

X - prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos.

Art. 25. As aplicações de internet de entes do poder público devem buscar:

I - compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso;

II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;

III - compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações;

IV - facilidade de uso dos serviços de governo eletrônico; e

V - fortalecimento da participação social nas políticas públicas.

Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.

Art. 27. As iniciativas públicas de fomento à cultura digital e de promoção da internet como ferramenta social devem:

I - promover a inclusão digital;

II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e

III - fomentar a produção e circulação de conteúdo nacional.

Art. 28. O Estado deve, periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas, referentes ao uso e desenvolvimento da internet no País.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente.

Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e

fornecer informações sobre o uso dos programas de computador previstos no caput, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes.

Art. 30. A defesa dos interesses e dos direitos estabelecidos nesta Lei poderá ser exercida em juízo, individual ou coletivamente, na forma da lei.

Art. 31. Até a entrada em vigor da lei específica prevista no § 2o do art. 19, a responsabilidade do provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros, quando se tratar de infração a direitos de autor ou a direitos conexos, continuará a ser disciplinada pela legislação autoral vigente aplicável na data da entrada em vigor desta Lei.

Art. 32. Esta Lei entra em vigor após decorridos 60 (sessenta) dias de sua publicação oficial.

Brasília, 23 de abril de 2014; 193o da Independência e 126o da República.

DILMA ROUSSEFF
José Eduardo Cardozo
Miriam Belchior
Paulo Bernardo Silva
Clélio Campolina Diniz