UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS SOCIAIS
CURSO DE DIREITO

ALLINE TAVARES GARCIA

O DIREITO À INTIMIDADE E A FRÁGIL PRIVACIDADE DA ERA DIGITAL: uma análise sobre os crimes cibernéticos e a eficácia da lei Carolina Dieckmann

São Luís
2017

ALLINE TAVARES GARCIA

O DIREITO À INTIMIDADE E A FRÁGIL PRIVACIDADE DA ERA DIGITAL: uma análise sobre os crimes cibernéticos e a eficácia da lei Carolina Dieckmann

Monografia apresentada ao Curso de Direito da Universidade Federal do Maranhão para obtenção do grau de Bacharel em Direito.

Orientador: Profº. Gláucio Fernando Barros Cunha.

São Luís

2017

Garcia, Alline Tavares.
O direito à intimidade e a frágil privacidade da era digital : uma análise sobre os crimes cibernéticos e a eficácia da lei Carolina Dieckmann / Alline Tavares Garcia. - 2017.
63 f.

Orientador(a): Gláucio Fernando Barros Cunha.
Monografia (Graduação) - Curso de Direito, Universidade Federal do Maranhão, São Luís, 2017.

1.Delitos informáticos. 2.Direito à privacidade. 3. Era Digital. 4. Lei Carolina Dieckmann. I.Cunha, Gláucio Fernando Barros. II. Título.

ALLINE TAVARES GARCIA

O DIREITO À INTIMIDADE E A FRÁGIL PRIVACIDADE DA ERA DIGITAL: uma análise sobre os crimes cibernéticos e a eficácia da lei Carolina Dieckmann

Monografia apresentada ao Curso de Direito da Universidade Federal do Maranhão para obtenção do grau de Bacharel em Direito.

Aprovada em: _____/_____/_____

BANCA EXAMINADORA

_____

Prof.º Gláucio Fernando Barros Cunha (Orientador)

_____

1º Examinador

_____

2º Examinador

À minha família, base de tudo, por todo apoio e amor.

AGRADECIMENTOS

À Deus, Senhor de todas as coisas, que está sempre presente em minha vida, me abençoando e me guiando pelos melhores caminhos.

À minha saudosa mãe, Rosário de Fátima Tavares Garcia, minha saudade diária, mulher incrível e mãe exemplar. Por toda dedicação, ensinamentos e amor.

Ao meu querido pai, Hamilton Matos Garcia, por toda a sua paciência e carinho, por sempre acreditar nos meus esforços e por nunca ter me deixado faltar nada.

Às minhas irmãs, Camila e Beatriz, por todos os conselhos e apoio que recebi durante essa caminhada.

À minha tia, Lígia Maria Matos Garcia, pelos anos que me acolheu na sua casa como se sua filha fosse.

À minha avó, tios e primos, que tanto me ajudaram e por quem tenho uma enorme admiração.

Ao Gláucio Fernando Barros Cunha, estimado professor, pela gentileza de aceitar me orientar neste trabalho.

Aos meus amigos e colegas, que nos momentos cansativos, puderam me distrair e fazer sorrir.

A todos, meu muito obrigada!

“Que os vossos esforços desafiem as impossibilidades, lembrai-vos de que as grandes coisas do homem foram conquistadas do que parecia impossível”.

Charles Chaplin

RESUMO

Nos últimos anos a revolução informática levou a sociedade pós-moderna a entrar em uma nova Era, a Era digital. Nesse contexto, a disseminação da internet trouxe consigo, além de benefícios, uma enorme gama de problemas virtuais. Os crimes cibernéticos se proliferaram e, dentre eles, um dos mais frequentes foram os relacionados à invasão da privacidade do internauta. O direito à intimidade está garantido constitucionalmente no art. 5º, inciso X, da carta republicana de 1988, e sua violação gera consequências tanto na esfera civil como penal. As lacunas legislativas referentes à tutela dos crimes cometidos no ambiente virtual contribuiu para a prática desses ilícitos, o que tornou necessário, cada vez mais, a criação de um tipo penal que protegesse os dados informáticos. Nesse intuito, foi criada a lei n.º 12.737/12, apelidada de lei Carolina Dieckmann, que criminalizou os delitos informáticos, trazendo consigo avanços na legislação penal virtual, assim como diversas críticas referentes ao seu conteúdo e eficácia.

Palavras-chave: Delitos informáticos. Direito à privacidade. Era Digital. Lei Carolina Dieckmann.

ABSTRACT

In recent years the computer revolution has led postmodern society to enter a new era, the Digital Age. In this context, the spread of the internet has brought, along with benefits, a huge range of virtual problems. Cyber crimes proliferated and among them one of the most frequent were those related to invasion of the privacy of the internaut. The right to privacy is constitutionally guaranteed in art. 5. item X, of the republican charter of 1988, and its violation generates consequences both in the civil and criminal spheres. Legislative gaps regarding the protection of crimes committed in the virtual environment contributed to the practice of these illicit acts, which made it necessary, more and more, to create a criminal type that protected the computer data. To this end, act no. 12.737 / 12, dubbed the Carolina Dieckmann act, was created, which criminalized computer crimes, bringing with it advances in virtual criminal law, as well as several criticisms regarding its content and effectiveness.

Keywords: Computer crimes. Right to privacy. Digital Era. Law Carolina Dieckmann.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

CFB/88	Constituição Federal Brasileira de 1988
CPB	Código Penal Brasileiro
DRCI	Delegacia da Repressão aos Crimes de Informática
FECOMÉRCIO/SP	Federal do Comércio do Estado de São Paulo
ECA	Estatuto da Criança e do Adolescente
JECrim	Juizado Especial Criminal
MCI	Marco Civil da Internet
ONG	Organização Não Governamental
ONU	Organização das Nações Unidas
PL	Projeto de Lei
STF	Supremo Tribunal Federal

SUMÁRIO

1 INTRODUÇÃO

O direito constitucional à intimidade e vida privada é condição fundamental da dignidade da pessoa humana. A carta republicana de 1988 enfatizou a importância que esse direito trouxe para sociedade pós-moderna, razão pela qual, dedicou parte do seu texto para tutela e proteção da intimidade. Como sabe-se, nos últimos anos, o mundo transformou-se com o rápido avanço da tecnologia informática e com a expansão da internet. Estamos vivendo em uma Era onde as relações sociais praticamente tornaram-se digitais e todo tipo de transação pode ser realizada via internet. Nesse contexto, sem dúvidas, os avanços advindos da Era digital foram muito importantes para o desenvolvimento da sociedade, contudo, em conjunto com os benefícios sobrevieram alguns fatores negativos, como o surgimento de uma nova zona criminológica, os chamados crimes cibernéticos.

Nesse sentido, o presente estudo busca fazer uma relação entre a frágil privacidade da Era digital e os crimes cibernéticos, analisando os aspectos positivos e negativos da lei n.º 12.737/12 (Lei Carolina Dieckmann), e observando seu grau de eficácia.

Para fazer uma reflexão do tema e analisar o objetivo proposto, é necessário expor os principais pontos referentes ao direito constitucional à intimidade e vida privada, direito este previsto na Constituição Federal Brasileira de 1988, no seu art. 5º, inciso X. Suas definições são basicamente que o direito à intimidade diz respeito as relações íntimas e pessoais do indivíduo, enquanto a privacidade se refere a todas as outras relações, como as comerciais, de estudo, de trabalho e etc. Ademais, o direito em voga, possui determinados limites, um bom exemplo é a questão do sobrelevo do interesse público em detrimento do interesse particular.

Como sabe-se, não foram apenas vantagens que a revolução informática consagrou. Ao longo dos últimos anos houve uma crescente massa de crimes virtuais, que acabaram por transformar a privacidade na rede um fator de preocupação para as autoridades judiciárias. A frágil privacidade da internet auxiliou na prática de delitos informáticos que em conjunto com a escassa legislação penal virtual brasileira, tornou-os sinônimo de impunidade. Foi nesse sentido que foram criadas as leis n.º 12.737/12 e 12.965/14, conhecidas como lei Carolina Dieckmann e marco civil da internet.

O marco civil da internet, buscou regulamentar a internet no Brasil, assim como, estabelecer os princípios, garantias direitos e deveres para o uso da rede. Dessa maneira, depreende-se que foi um avanço muito importante para a proteção dos internautas, tendo em vista que seu texto legal trata de pontos relevantes como a privacidade na web, a neutralidade da rede e os registros de acesso.

A lei Carolina Dieckmann, criada às pressas devido o episódio ocorrido com a atriz brasileira Carolina Dieckmann, em que esta teve seu computador invadido e várias fotos íntimas divulgadas na internet, tipificou os delitos informáticos, alterando o Código Penal Brasileiro, com a inserção dos arts. 154-A e 154-B e modificação dos arts. 266 e 298. A lei trata sobre as condutas classificadas como crimes, as penas cominadas a elas, suas qualificadoras e a ação penal. Contudo, apesar de representar significativo avanço na legislação criminal brasileira, afinal possibilitou o enquadramento de condutas que até então não tinham respaldo legal, a lei sofre diversas críticas, principalmente em relação as suas penas brandas e seu texto ambíguo. As penas que variam de 3 (três) meses a 1 (um) ano de detenção e multa, não seriam fortes o suficiente para reprimir a práticas das condutas delituosas. Alguns termos utilizados no texto normativo também são alvo de críticas, por exemplo, "dispositivo informático" e "violação indevida de mecanismo de segurança".

Por fim, busca-se estabelecer algumas propostas de possibilidades de melhorias da lei n.º 12.737/12. Primeiramente seria necessária uma mudança na própria letra do texto. Seria necessário também, para efetividade da lei, a conjugação com jurisprudências e leis complementares além de se fazer um estudo do direito comparado e dos tratados e convenções internacionais.

Portanto, ao longo da presente monografia desenvolve-se uma pesquisa bibliográfica, que abraçou a legislação pátria, artigos periódicos, jurisprudências, livros, notícias de jornais e revistas e gráficos de estudos de campo.

2 O DIREITO CONSTITUCIONAL À INTIMIDADE E VIDA PRIVADA

O presente capítulo traz um breve histórico sobre o nascimento do direito constitucional à intimidade e à vida privada. Expõe ainda, sobre em que consiste esse direito, que, como qualquer outro, não é absoluto, e quais são os limites oponíveis a ele.

2.1 Antecedentes históricos

A promulgação da Constituição Federal Brasileira de 1988 (CFB/88) trouxe consigo uma série de garantias e direitos fundamentais que visam assegurar a dignidade da pessoa humana. Citando entendimento de Lira (2014), a Constituição Federal, norma suprema do ordenamento jurídico pátrio, traz em seu manto os direitos fundamentais com o objetivo de proteger os seres humanos contra abusos, excessos e medidas autoritárias, visando assim a construção de um Estado democrático de direito.

A carta magna brasileira de 1988 foi a primeira a referir-se à intimidade e à vida privada, notoriamente por influência da carta magna lusitana. Em seu art. 5º, adotou um amplo catálogo de garantias, dentre as quais, está o direito à intimidade e à privacidade, previsto no art. 5º, inciso X, da CFB/88, que enuncia:

> 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.

Desta feita, fica clara a tutela garantida ao direito à privacidade, já que este direito, como bem aduz Eduardo Tomasevicius Filho[1] (2016, p. 272), "é fundamental em uma sociedade democrática para materializar a liberdade de expressão".

Apesar de amplamente defendido nos dias atuais, o direito à privacidade não o foi assim sempre. Nesse sentido, Ferreira Filho (2011, p. 347), preleciona:

> O direito fundamental à privacidade (toma-se aqui o termo no seu sentido mais abrangente) não foi reconhecido nas primeiras Declarações, as do século XVIII. Entretanto, bem corresponde ele à "liberdade dos modernos", na fórmula de Constant, pois, corresponde a autonomia da conduta individual. Pode-se dizer que ele somente veio a ser apercebido como uma das projeções da dignidade da pessoa humana, quando o desenvolvimento dos meios de comunicação – primeiro da imprensa – vieram a ameaçar a privacidade individual. Com efeito, o desenvolvimento da

[1] Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142016000100269#aff1>. Acesso em: 4 abr. 2017.

> imprensa e particularmente dos meios audiovisuais de comunicação de massa, por um lado, da informática, por outro, veio pôr em grave risco o direito de cada um não ver exposta a sua vida privada, e, mais, a sua vida íntima à indiscrição alheia. Inclusive a do Estado.

Dessa maneira, depreende-se que o direito à privacidade possui raízes modernas, é apenas com o desenvolvimento dos meios de comunicação em massa que tal direito ganhou magnitude e passou a ter maior respaldo do legislador brasileiro. Nas precisas lições de Paesani (2013, p. 34), "esse direito vem assumindo, aos poucos, maior relevo, com a expansão das novas técnicas de comunicação, que colocam o homem numa exposição permanente".

Contudo, importante frisar que o direito à privacidade não é literalmente novo, pois, os Estados Unidos já o reconhecia há quase um século, como percebe-se pela obra do famoso artigo de Brandeis, chamado *The Right to Privacy*.

Além da garantia constitucional, a nossa lei maior também recepcionou em 1992 a Convenção Americana de Direitos Humanos, mais conhecida como Pacto de San José da Costa Rica[2]. De acordo com esse pacto, ninguém pode ser objeto de ingerências abusivas em sua vida privada. Toda pessoa tem direito à proteção da lei contra essas ingerências, ao respeito da sua honra e ao reconhecimento da sua dignidade.

Diante do exposto, resta claro que o ordenamento jurídico brasileiro é enfático ao proteger a privacidade dos seus cidadãos. Entretanto, como veremos adiante, o direito à intimidade e à vida privada não é absoluto, pois, sofre algumas restrições de acordo com cada caso.

2.2 Em que consiste o direito à intimidade e à vida privada?

Não é tarefa fácil explicar em que consiste o direito à intimidade e à vida privada. Vários doutrinadores já se dedicaram a esse estudo, como fez Tércio Sampaio Ferraz Júnior[3] (1993, p. 439-440), em sua obra Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado:

> Trata-se de um direito subjetivo fundamental. Como direito subjetivo, manifesta uma estrutura básica, cujos elementos são o sujeito, o conteúdo e o objeto. [...] o sujeito é toda e qualquer pessoa, física ou jurídica, brasileira ou estrangeira, residente no país. O conteúdo é a faculdade especifica atribuída ao sujeito, que pode ser a faculdade de constranger os outros, ou de resistir-lhes (caso dos direitos pessoais), ou de dispor,

[2] O tratado internacional tem objetivos de estabelecer os direitos fundamentais da pessoa humana, como o direito à vida, à liberdade, à dignidade, à integridade pessoal e moral, à educação, entre outros. A convenção proíbe ainda a escravidão e a servidão humana, trata das garantias judiciais, da liberdade de consciência e religião, de pensamento e expressão, bem como da proteção da honra e da dignidade.

[3] Disponível em: <http://www.scielo.br/pdf/ea/v30n86/0103-4014-ea-30-86-00269.pdf>. Acesso em: 4 abr. 2017

> gozar, usufruir (caso dos direitos reais). [...] O objeto é o bem protegido, que pode ser uma res (uma coisa, não necessariamente física, no caso de direitos reais), ou um interesse (no caso de direitos pessoais). No direito à privacidade, o objeto é sinteticamente, a integridade moral do sujeito.

A explicação do aludido autor resume de forma concisa a estrutura básica do direito à privacidade, quais sejam: seu sujeito, conteúdo e objeto.

No tocante a conceituação dos verbetes, embora doutrina e jurisprudência ainda sejam ambíguas, existem os que dizem que o direito à intimidade faz parte do direito à privacidade, isto é, o conceito de privacidade englobaria o de intimidade. Segundo Branco e Mendes (2012, p. 318):

> O direito à privacidade teria por objeto os comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, as relações comerciais e profissionais que o indivíduo não deseja que se espalhe ao conhecimento público. O objeto do direito à intimidade seriam as conversações e os episódios ainda mais íntimos envolvendo relações familiares e amizades mais próximas.

No mesmo sentido, é o parecer de Bulos (2011, p. 553):

> [...] a idéia de vida privada é mais ampla do que a de intimidade:
> Vida privada (ou privacidade) – envolve todos os relacionamentos do indivíduo, tais como suas relações comerciais, de trabalho, de estudo, de convívio diário; e
> Intimidade – diz respeito as relações intimas e pessoais do indivíduo, seus amigos, familiares, companheiros que participam da sua vida pessoal.

Sob o ponto de vista do direito civil, Amaral (2008, p. 306), afirma que o direito à privacidade é tido como, "o direito de isolar-se do contato com outras pessoas, bem como o direito de impedir que terceiros tenham acesso a informações acerca de sua pessoa".

Por fim, esclarece Novelino (2008, p. 269):

> A esfera pessoal abrange as relações com o meio social sem que, no entanto, haja vontade ou interesse na divulgação; a esfera privada compreende os dados relativos a situações de maior proximidade emocional ("contextos relacionais específicos") como, por exemplo, as opções pessoais ou a orientação sexual do indivíduo. As duas esferas integram a vida privada do indivíduo. A esfera íntima se refere ao modo de ser de cada pessoa, ao mundo intra-psíquico, aliado aos sentimentos identitários próprios (auto-estima, auto-confiança) e à sexualidade. Compreende as esferas confidencial e do segredo, referentes a intimidade.

Por certo, os direitos à intimidade e à vida privada podem ser considerados como direitos da personalidade. Eles decorrem da autonomia da vontade e do livre arbítrio, onde o direito à privacidade confere ao ser humano, o direito de seguir a sua própria vida da maneira que melhor lhe convir, sem qualquer intromissão alheia, porém, sempre respeitando a ordem pública, os bons costumes e os direitos de terceiros.

Sem esgotar o assunto, o alemão Heinrich Hubmann desenvolveu uma teoria que classificou os direitos da personalidade em 3 (três) esferas. Por essa teoria, o grau de proteção à privacidade varia de acordo com a área da personalidade afetada, ou seja, quanto mais próxima das experiências definidoras da identidade do indivíduo, maior a proteção dada a esfera. Dessa maneira, temos a esfera da publicidade[4], a esfera pessoal ou privada[5] e a esfera íntima[6].

Esse é o posicionamento do Supremo Tribunal Federal[7] (STF) e de alguns doutrinadores como Geraldo Andrade[8] (2015, s.p), que diz "quanto maior for a intervenção num determinado direito, maiores terão que ser os motivos que justifiquem o afastamento desse direito. E lembrando que os princípios da proporcionalidade e da razoabilidade devem sempre pautar a ponderação".

Lira (2014, p. 19) complementa, "quando há interesses públicos acolhidos por normas constitucionais, que sobrepujam o interesse de recolhimento do indivíduo, estar-se-á diante de limites ao direito à privacidade". Isso ocorre, pois, em determinadas situações o interesse público se sobreleva ao interesse particular.

Nessa lógica, têm-se a lição de Paesani (2013, p. 34):

> A predominância do interesse coletivo sobre o particular requer, em cada caso, a verificação do alcance respectivo, a fim de não se sacrificar indevidamente a pessoa salvo quando a divulgação de notícias com finalidades científicas ou de polícia venham a sacrificar o interesse particular em prol da coletividade.

Outro método de avaliação desses limites é feito de acordo com as circunstâncias de cada caso concreto. A divulgação de fatos ligados a esfera privada de determinado indivíduo pode ser tida como admissível ou como abusiva. Para isso, é importante levar em consideração o modo como o fato foi exposto ao público, sendo assim, existem casos em que a intimidade é propagada pelo próprio titular do direito e casos em que foi obtida contra a sua vontade.

---

[4] Que compreende os atos que são praticados em público com o desejo de torna-los públicos, ou seja, não basta que o local seja público, deve existir o elemento volitivo interno. Dentro dessa esfera, existe ainda os fatos pertencentes ao domínio público; as informações passiveis de serem obtidas licitamente de outra forma; e os atos administrativos praticados por agentes públicos respaldados pelo princípio da publicidade. Tal esfera encontra-se fora do âmbito de privacidade constitucionalmente protegido.

[5] Que abrange as relações com o meio social, sem contudo, que haja interesse na divulgação, como por exemplo, opções pessoais ou orientação sexual.

[6] Que se refere ao modo de ser de cada pessoa, seu mundo intra-psíquico, como por exemplo auto confiança e auto estima. Compreende as esferas confidencial e do segredo.

[7] (STF - HC: 93250 MS, Relator: Min. ELLEN GRACIE, Data de Julgamento: 10/06/2008, Segunda Turma, Data de Publicação: DJe-117 DIVULG 26-06-2008 PUBLIC 27-06-2008 EMENT VOL-02325-04 PP-00644).

[8] Disponível em: <https://quentasol.jusbrasil.com.br/artigos/214374415/direito-a-privacidade-intimidade-vida-privada-e-imagem> Acesso em: 3 abr. 2017.

Nesse espeque, Lira (2014, p. 20), exemplifica, “uma pessoa famosa pode consentir que exponha as suas agruras: durante um sequestro ou dar entrevista por ocasião da morte de algum ente querido, nada impede que o faça”

Aproveitando o ensejo, Pinheiro (2013, p. 87), acrescenta:

> É evidente que o direito à privacidade constitui um limite natural ao direito à informação. No entanto, não há lesão a direito se houver consentimento, mesmo que implícito, na hipótese em que a pessoa demonstra de algum modo interesse em divulgar aspectos da própria vida.

Por conseguinte, uma vez divulgadas as informações pelo próprio indivíduo, e estas tornando-se públicas, não haverá mais como retê-las.

2.2.1 Direito à intimidade *versus* interesse público: resistência do aplicativo *whatsapp* em fornecer dados e informações à justiça

Diante desse cenário, oportuno apresentar a atual discussão que envolve o direito à intimidade *versus* o interesse público, no que tange à resistência do aplicativo de mensagens instantâneas “*whatsapp*” em fornecer dados e informações à polícia, mesmo quando obrigado pelo Judiciário.

Como é de conhecimento geral, nos últimos tempos, o aplicativo *whatsapp* entrou em rota de colisão com a justiça brasileira por diversas vezes. Primeiro foi ameaçado de suspensão, depois teve seu acesso banido por algumas horas no país. Os casos que ocorrem no aplicativo são distintos, envolvendo inclusive diferentes crimes, mas o problema entre o *whatsapp* e a justiça é sempre o mesmo: o aplicativo não fornece as informações solicitadas pelas autoridades.

De acordo com a lei brasileira n.º 12.965/14, conhecida como marco civil da internet (MCI), o *whatsapp* é obrigado a guardar todos os registros de acessos dos usuários por um período mínimo de 6 (seis) meses, e fornecê-los mediante ordem judicial. Reforçando o exposto, o professor e coordenador do curso de direito digital do Insper, Renato Opice Blum (2016), admite que os apps podem ser obrigados a guardar as informações sobre determinados usuários a partir do recebimento de uma ordem. Ainda segundo ele, o descumprimento do pedido da justiça só é valido nos casos de impossibilidade técnica ou falta de acesso à informação solicitada. O último caso é inclusive o argumento que a empresa utiliza para justificar a sua postura.

Conforme entrevista realizada com o diretor de comunicação do aplicativo Matt Steinfeld, a explicação para que o *whatsapp* não colabore com os pedidos é simples: nenhuma mensagem é guardada em seus servidores. Existem recursos do aplicativo que limitam a capacidade de fornecer informações nessas investigações. Renato Santino[9] (2016, s.p), deixa claro essa afirmação ao dizer:

> Não importa quantas vezes a Justiça brasileira (ou de qualquer outro lugar do mundo) pedir, o WhatsApp não pode oferecer o que ele não tem. [...] É importante observar que o WhatsApp não armazena o conteúdo das mensagens. A partir do momento em que entregue entre duas pessoas, ela é apagada dos nossos servidores. Nós só temos nossos servidores com o propósito de entregar as mensagens. Não mantemos registros sobre o que as pessoas conversam nos nossos servidores [...] O mais interessante de toda esta situação é que, mesmo que armazenasse as mensagens, pouco poderia ser feito para ajudar a Justiça, porque o aplicativo aposta em criptografia end-to-end, que, basicamente, significa que as mensagens saem do celular já criptografadas, fazem todo o trajeto celular-servidor-outro celular e só são desencriptadas quando chegam ao recipiente final, para que ele possa ler o que foi escrito. Ou seja: mesmo que guardasse estas mensagens e fotos, o WhatsApp não teria a chave para poder vê-las, ou para permitir que as autoridades as vejam.

Ainda segundo Matt, a criptografia é importante pois oferece a garantia aos usuários de que suas mensagens não serão interceptadas, por qualquer motivo, como exemplos do cibercrime ou da ciberespionagem governamental.

Todavia, consoante Larissa Leiros Baroni[10] (2016, s.p), a inviolabilidade técnica também é questionada pelo especialista em telecomunicações e segurança da informação André Jaccon, que relata:

> Tecnicamente tudo é possível, desde que haja um aporte jurídico em cima", ressalta ele, que diz ser viável cruzar as informações do banco de dados do WhatsApp com o do Facebook. "Um cruzamento que poderia ser realizado usando apenas o número do celular e chegar a uma gama muito maior de informações.

À justiça, é facultado o pedido de perícia técnica para atestar a veracidade das informações fornecidas pela defesa do *whatsapp*, ou seja, se este estaria dizendo a verdade ou não sobre não possuir os dados requeridos.

Por fim, importante destacar, que a empresa participa de tratados internacionais que permitem pedidos governamentais por dados do *whatsapp*, além de também possuir canais para que as autoridades tragam as suas requisições e pedidos. Com isso, resta claro que existem outros caminhos para as autoridades pedirem informações ao aplicativo.

---

[9] Disponível em: <https://olhardigital.uol.com.br/fique_seguro/noticia/whatsapp-explica-por-que-nao-entrega-os-dados-que-a-policia-brasileira-pede/55829> Acesso em: 8 jun. 2017.

[10] Disponível em: <https://tecnologia.uol.com.br/noticias/redacao/2016/03/02/lei-brasileira-obriga-whatsapp-a-fornecer-dados.htm>. Acesso em: 8 jun. 2017.

3 A PRIVACIDADE E O MEIO DIGITAL

O presente capítulo trata sobre a frágil privacidade existente no meio digital e quais são as maneiras cabíveis para combater a invasão da mesma na web. Fala-se ainda da criação da lei n.º 12.965/14 – marco civil da internet, indagando como essa lei auxilia na proteção da privacidade virtual e analisando suas principais disposições.

3.1 Breves considerações sobre a internet

Segundo Corrêa (2002), a Internet surgiu em meados de 1969 nos Estados Unidos. Foi criada a partir de um projeto do governo norte-americano chamado de Arpanet que era de uso exclusivo dos militares durante a guerra fria e no início, era usada apenas para a transmissão de informações de texto por rede à distância.

A internet que conhecemos atualmente foi desenvolvida ao longo da década de 1980, quando instituições dos Estados Unidos e do mundo se interligaram para formar uma grande rede. Nessa época, o uso da internet não tinha cunho comercial, porém, cada vez mais, as empresas sofriam pressão para usufruir dessa revolucionária rede. Dessa maneira, a partir da década de 1990, foi permitida a abertura da rede para o uso comercial, fazendo com que o mundo entrasse em uma nova Era.

No Brasil, de acordo com Martins (2013, p. 3), a internet:

> Surgiu em 1991, trazida pela Rede Nacional de Pesquisas (RNP), com o objetivo de conectar redes de universidades e centros de pesquisa. Entretanto, somente em 1995 que o Ministério de Comunicações e de Ciência e Tecnologia autorizou sua abertura para a comercialização, através da RNP, e depois com a Embratel. Aqui, a regulação da internet é feita pelo Comitê Gestor da internet, criado pela Portaria Interministerial nº 147, e alterada pelo Decreto presidencial nº 4829, de 03 de setembro de 2003, que tem como funções integrar todas as iniciativas de serviços internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados.

Importante trazer à baila a definição de internet, que segundo Corrêa (2002, p. 8):

> É um sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina a qualquer outra conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem limitação de fronteiras culminando na criação de novos mecanismos de relacionamento.

Vale ressaltar que a internet não é *World Wide Web* (WWW, 3W ou Web). Esta nasceu apenas em 1989, em Genebra, e foi o elemento responsável pela popularização da internet. O

WWW é a base da internet simples e prática de hoje, que além de tornar a internet mais acessível, transformou o mundo digital.

3.2 Tratamento legal da privacidade na internet

Ao nos depararmos com o tema privacidade no espaço cibernético, duas ordens de problemas se apresentam. Rodotà (1996 apud PAESANI, 2013, p. 39), explica:

> O primeiro reporta-se ao respeito a esfera privada alheia que nos conduz no terreno tradicional da tutela da privacidade. O segundo refere-se a privacidade de quem se movimenta naquele espaço e, consequentemente, requer o anonimato. Contudo, os dois problemas estão destinados a se cruzarem e indaga-se quais serão as consequências se uma pessoa considerar que sua privacidade está sendo violada por urna informação anônima na rede.

A exigência do anonimato tornou-se uma das principais características da internet. Na rede, é possível ser quem você deseja ser, assumindo uma identidade livre de condicionamentos e pressões. Qualquer tentativa de limitação dessa possibilidade violaria um dos pontos cardeais da internet, que é o de espaço da liberdade total. Entretanto, a absoluta falta de regras coloca em risco a própria liberdade o que pode envolver um dos assuntos mais polêmicos da internet, qual seja, a violação da privacidade. Sobre esse assunto, trataremos mais detalhadamente no tópico a seguir.

3.3 A fragilidade da privacidade no meio digital

O avanço da Internet nos últimos tempos incorporou à vida de milhões de pessoas enormes benefícios. Em menos de 20 (vinte) anos de uso comercial, a internet modificou vários aspectos da convivência humana, nos colocando em contato com um mundo que ultrapassa barreiras físicas e transformando a sociedade pós-moderna na sociedade da informação. Essa evolução indiscriminada proporcionada pela globalização acabou ocasionando alguns riscos trazidos pela Era digital, que além de estabelecer novos contatos sociais, gerou uma nova zona criminológica.

Corroborando com essa tese, Lira (2014, p. 28), leciona:

> Ressalte-se que com os avanços da tecnologia e da difusão de informação, a sociedade pós-moderna tornou-se volátil, de modo que ninguém escapa à vigilância e à privacidade. O autor evidencia que na era digital, a proteção dos direitos fundamentais dos indivíduos, inerentes à vida privada, estão em situação delicada. Percebe-se que os meios de informatização exercem um poder sobre os indivíduos, uma vez que controlam a sua vida e os seus dados; por isso, como novel direito fundamental, faz-

> se necessária a proteção de dados, instrumento de defesa à vida privada e à intimidade, núcleos do direito à privacidade.

No mesmo aspecto, a referida autora acrescenta, "os novos riscos disponibilizados pela era da informática passaram a causar conflitos até então desconhecidos pelo Direito, razão pela qual exigiu-se que novas providências fossem tomadas [...]. (LIRA, 2014, p. 27)

Rapidamente o meio digital confundiu-se com sinônimo de exposição. Fato atual se reflete no surgimento das redes sociais[11], onde os usuários da rede acabam utilizando essa ferramenta de maneira irresponsável, pois, expõem a sua intimidade para qualquer pessoa que acesse seu perfil. Todavia, não é somente nas redes sociais que acontece a invasão da privacidade. Sites de compras, e-mails, programas de buscas, todos esses mecanismos se não forem manuseados com os devidos cuidados, apresentam sérios riscos à segurança do internauta.

De acordo com Alexandre Atheniense[12] (2010, s.p), isso ocorre pois "estamos em um momento de transição em que as relações humanas se tornam cada vez mais interativas através dos dispositivos móveis de comunicação, porém, estamos nos tornando cada vez mais vulneráveis aos ataques a nossa esfera de privacidade".

Se lançarmos um olhar sobre esta transição percebemos que um dos maiores desafios será o de preservar a reputação e a privacidade dentro desse ambiente de interconexão, pois, como sabemos, a privacidade na rede pode ser quebrada com facilidade.

Nessa perspectiva Anderson Soares[13] (2014, s.p), preleciona:

> Na nova era digital esse direito é muito vulnerável frente ao imenso mundo da internet. Resultado dessa fragilidade, a lei de regulação da utilização da internet procurou proteger esse valor tão essencial para a intimidade dos usuários de rede móvel de computador, tanto em modo off-line quanto em modo on-line.

Na mesma linha de raciocínio, Lira (2014, p. 16), admite:

> Essa comodidade desenfreada fez com que surgissem mentes perversas capazes de invadir os dispositivos informáticos alheios, interromper serviços telemáticos ou de utilidade pública e até mesmo falsificar cartões de crédito e débito; condutas criminais

---

[11] Redes sociais virtuais ou sites de relacionamento são páginas da internet que tem como principal objetivo, a facilitação da interação entre os usuários. A maioria dos sites de relacionamento é baseada nos perfis dos usuários, onde podem ser compartilhados os gostos e preferências de cada um. Em alguns sites, o usuário ainda tem a possibilidade de controlar a privacidade, protegendo informações do perfil.

[12] Disponívelem:<http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=7967>. Acesso em 03 abr. 2017.

[13] Disponível em: < https://jus.com.br/artigos/30520/marco-civil-da-internet-e-a-garantia-consticional-da-privacidade-e-liberdade-de-expressao>. Acesso em 05 abr. 2017.

> que violam: a intimidade, a vida privada, a honra e a imagem das pessoas trazendo danos econômicos e sociais irreparáveis.

Importante destacar, que na maioria das vezes a privacidade é violada e os crimes digitais são estimulados devido a insegurança do meio virtual. Para Pinheiro (2013, p. 311), "o maior estímulo aos crimes virtuais é dado pela crença de que o meio digital é um ambiente marginal, um submundo em que a ilegalidade impera". Tal postura existe devido a insegurança do meio, uma vez que a vigilância não é feita de forma suficiente e os crimes não recebem a punição adequada frente ao dano causado.

3.4 Medidas para combater a invasão de privacidade na Internet

Como visto acima, a privacidade na Era digital é bastante frágil. Podemos citar diversos fatores que auxiliam a invasão da privacidade na internet, tais como: a super exposição, a falta de segurança dos sites, a engenharia social, os vírus, a ação dos crackers[14], a sensação de anonimato, a legislação vigente lacunosa e etc.

Além disso, "muitos criminosos cometem delitos informáticos a partir de dados fornecidos pelas próprias vítimas em redes sociais e de descuidos na segurança do computador e dos dados" (BUSCATO, 2012 apud LIRA, 2014, p. 98). Nesse sentido, as pessoas mostram fotos da casa, dos filhos, viagens, os nomes, endereço, tudo, facilitando ainda mais a ação das mentes criminosas.

Tendo em vista essa fragilidade aconselha-se o internauta a tomar algumas precauções. O bom senso, aliado a um programa de antivírus atualizado e o cuidado ao inserir dados pessoais em sites duvidosos são um bom começo para a proteção da sua privacidade digital.

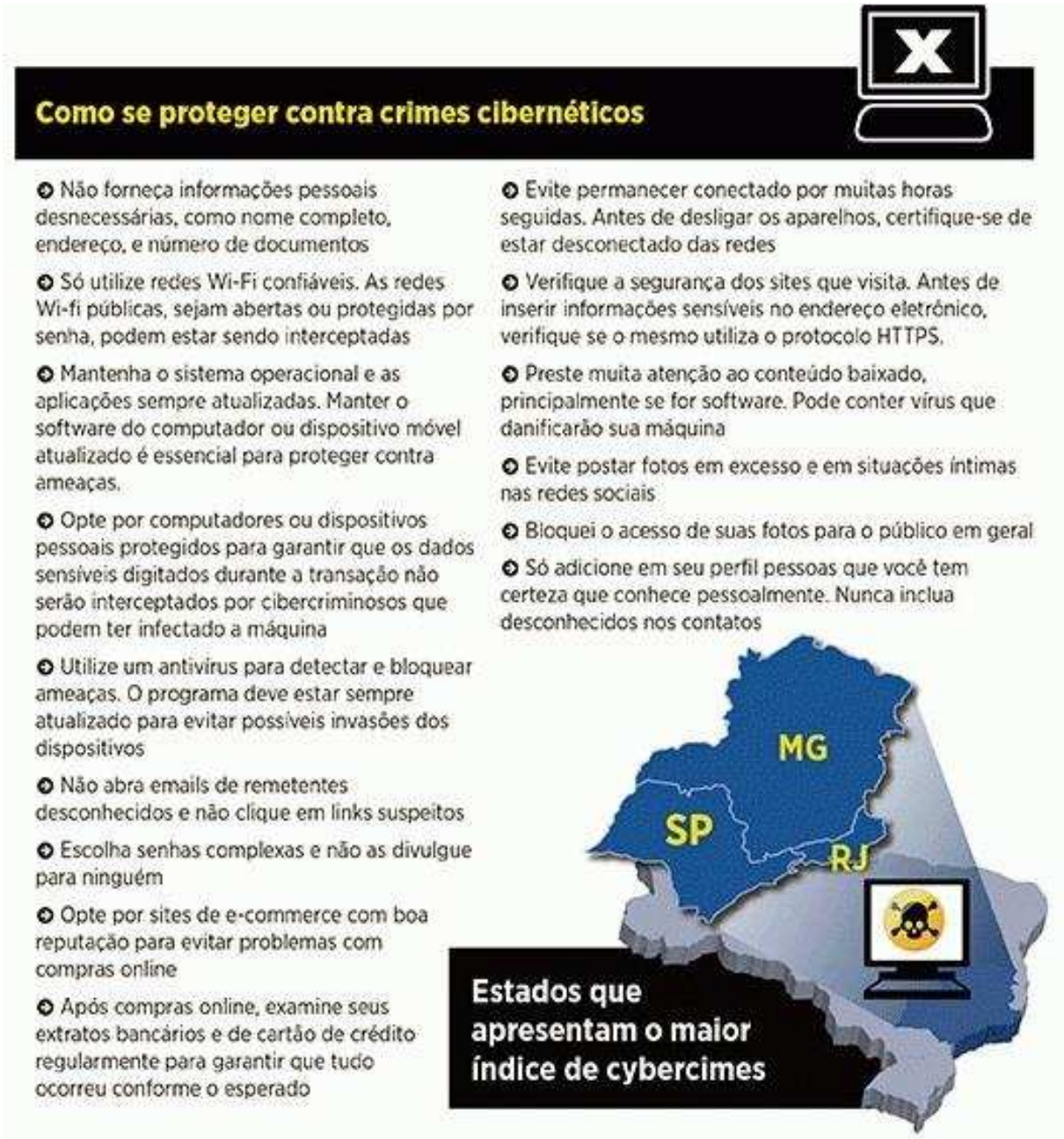
Adiante, o site Jornal do Commercio – JC Online[15] (2014, s.p), reuniu as principais maneiras do internauta se proteger contra os crimes cibernéticos, vejamos:

---

[14] Os crackers são pessoas aficionadas por informática que utilizam seu grande conhecimento na área para quebrar códigos de segurança, senhas de acesso a redes e códigos de programas com fins criminosos.

[15] Disponível em: <http://jconline.ne10.uol.com.br/canal/cidades/geral/noticia/2014/08/06/saiba-como-evitar-os-crimes-virtuais-138960.php>. Acesso em 20 jun. 2017.

Figura 1- Como se proteger contra crimes cibernéticos



Fonte: JC online.

Além disso, a Cartilha de segurança para internet[16] também selecionou alguns cuidados que o usuário da rede deve tomar. Por seu texto, ao usar navegadores web:

> Mantenha-o atualizado, com a versão mais recente e com todas as atualizações aplicadas; [...] Seja cuidadoso ao usar cookies caso deseje ter mais privacidade; [...] Permita que programas ActiveX sejam executados apenas quando vierem de sites conhecidos e confiáveis.

[16] Disponível em: <https://cartilha.cert.br/uso-seguro/>. Acesso em: 5 jul. 2017.

Ao usar programas leitores de e-mails:

> Mantenha-o atualizado, com a versão mais recente e com as todas atualizações aplicadas; Seja cuidadoso ao clicar em links presentes em e-mails; [...] Desconfie de arquivos anexados à mensagem mesmo que tenham sido enviados por pessoas ou instituições conhecidas (o endereço do remetente pode ter sido falsificado e o arquivo anexo pode estar infectado); [...] Desligue as opções que permitem abrir ou executar automaticamente arquivos ou programas anexados às mensagens.

Ao acessar *webmails*:

> Seja cuidadoso ao acessar a página de seu Webmail para não ser vítima de phishing. Digite a URL diretamente no navegador e tenha cuidado ao clicar em links recebidos por meio de mensagens eletrônicas; [...] Configure opções de recuperação de senha, como um endereço de e-mail alternativo, uma questão de segurança e um número de telefone celular; [...] Evite acessar seu Webmail em computadores de terceiros e, caso seja realmente necessário, ative o modo de navegação anônima.

Ao efetuar transações bancárias e acessar sites de *internet banking*:

> Certifique-se da procedência do site e da utilização de conexões seguras ao realizar transações bancárias via Web; [...] Ao acessar seu banco, forneça apenas uma posição do seu cartão de segurança (desconfie caso, em um mesmo acesso, seja solicitada mais de uma posição); [...] Antes de instalar um módulo de segurança, de qualquer Internet Banking, certifique-se de que o autor módulo é realmente a instituição em questão.

Contudo, tais cuidados, como sabe-se, ainda não conseguem ser 100% eficazes.

Diante desse cenário, com o objetivo geral de fortalecer a proteção à privacidade dos internautas, recentemente foram sancionadas as leis n.º 12.965/14 (marco civil da internet) e n.º 12.737/12 (lei Carolina Dieckmann), que buscam, respectivamente, regulamentar o uso da internet no Brasil e tipificar criminalmente os delitos informáticos.

De qualquer maneira, essas leis trouxeram consigo avanços importantes já que até então, as normas relativas à informática e à internet no Brasil eram bastante escassas.

3.5 A criação da lei n.º 12.965/14 – marco civil da internet

O rápido desenvolvimento tecnológico da internet fez com que houvesse um uso indiscriminado dessa poderosa ferramenta. As relações sociais tornaram-se cada vez mais dependentes da rede, e junto a elas veio a prática de violações constitucionais. Consoante Tomasevicius Filho (2016), as transformações resultantes do uso livre da internet, geraram dúvidas nas pessoas que ainda não sabiam exatamente como se comportar nessa terceira esfera de ação humana. Diante dessas dúvidas, imaginou-se que a internet seria uma "terra sem lei", onde tudo era permitido.

Então, fez-se necessário, a elaboração de um instrumento de regulamentação que norteasse o comportamento dos internautas na esfera virtual. Além do mais, Soares (2014, s.p), é categórico ao afirmar que, "o grande intuito da lei é a garantia dos direitos humanos como principal fundamento o respeito à liberdade de expressão na rede mundial de computadores, no qual seja essencial ao exercício da cidadania". Com essa finalidade foi promulgada em 2014 a lei n.º 12.965/14, conhecida nacionalmente como O marco civil da internet, que estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil.

O projeto de lei (PL), que foi inclusive submetido a consultas públicas, já tramitava na câmara desde 2011, mas foi apenas em 2014 que o plenário da casa o aprovou. Essa lei é uma espécie de "Constituição da internet" que traz em seu escopo alguns pontos marcantes, tais como: a privacidade na web, a neutralidade da rede e os registros de acesso. Sobre a privacidade na web o Portal EBC[17] (2014, s.p), deixa claro que:

> Além de criar um ponto de referência sobre a web no Brasil, o Marco prevê a inviolabilidade e sigilo de suas comunicações. O projeto de lei regula o monitoramento, filtro, análise e fiscalização de conteúdo para garantir o direito à privacidade. Somente por meio de ordens judiciais para fins de investigação criminal será possível ter acesso a esses conteúdos. Outro ponto da proposta garante o direito dos usuários à privacidade, especialmente à inviolabilidade e ao sigilo das comunicações pela internet. O texto determina que as empresas desenvolvam mecanismos para garantir, por exemplo, que os e-mails só serão lidos pelos emissores e pelos destinatários da mensagem. O projeto assegura proteção a dados pessoais e registros de conexão e coloca na ilegalidade a cooperação das empresas de internet com órgãos de informação estrangeiros. As empresas que descumprirem as regras poderão ser penalizadas com advertência, multa, suspensão e até proibição definitiva de suas atividades. E ainda existe a possibilidade de penalidades administrativas, cíveis e criminais.

A neutralidade da rede, por sua vez, se refere ao princípio de que a rede deve ser igual para todos, sem diferença quanto ao tipo de uso. Nesse sentido, Tomasevicius Filho (2016, p. 275), declara:

> Aspecto relevante é a neutralidade da rede [...] Por meio desta, impõe-se o tratamento isonômico aos dados transmitidos, sem distinção de conteúdo, origem e destino, serviço, terminal e aplicação. A ideia é que se possa acessar indistintamente uma página de internet, enviar um e-mail ou assistir a um filme ou conversar por videoconferência, sem prejuízo da velocidade de transmissão dos dados.

Já em relação aos registros de acesso, os provedores são proibidos de guardá-los, ou seja, o seu rastro digital em sites não ficará armazenado pela empresa que fornece o acesso[18].

---

[17]Disponível em: <http://www.ebc.com.br/tecnologia/2014/04/entenda-o-marco-civil-da-internet-ponto-a-ponto>. Acesso em: 3 abr. 2017.

[18] Vide nota de rodapé n. 15.

3.6 Breve análise da lei n.º 12.965/14 – marco civil da internet

Não é apenas sobre os tópicos supracitados que versa a lei em questão. Além deles, a lei trata ainda de outros tão importantes quanto os mencionados, tais como, os direitos dos internautas, os registros de conexão dos provedores[19], o combate às ilicitudes civil e criminal praticadas na internet, a responsabilidade civil dos provedores de internet, entre outros.

Dentro desse rol, merece destaque o art. 7º, pois, aborda diretamente sobre os direitos e garantias dos usuários. Logo em seus primeiros incisos, o texto normativo garante a inviolabilidade da intimidade e da vida privada, o sigilo do fluxo das comunicações na internet e o sigilo das comunicações privadas armazenadas, vejamos senão, a letra da lei:

> 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

[19] Esclarece-se que toda ação praticada pela internet é passível de registro pelos provedores de acesso, desse modo, o Marco Civil da Internet exige a guarda dos registros de conexão pelo prazo de 1 (um) ano e o registro de acesso a aplicações pelo prazo de 6 (seis) meses, contudo, o acesso a informações desses dados somente se dará pela atuação do Poder Judiciário.

> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet. (BRASIL, 2014)

Outro aspecto importante da lei diz respeito à censura. Pela leitura do texto, observa-se uma preocupação em afastar as críticas de que se poderia restaurar a censura no país. Isso fica explicito no art. 2º, *caput*, e 19 que aduzem: Art. 2º, *caput*, "a disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão". Art. 19, "com o intuito de assegurar a liberdade de expressão e impedir a censura [...]". Tudo isso corrobora com o previsto no art. 3º, inciso I, quando afirma que um dos princípios do uso da internet no Brasil é "a garantia da liberdade de expressão, comunicação e manifestação do pensamento, nos termos da Constituição Federal".

Doravante, em seus últimos arts., o MCI regulou a atuação do poder público frente o desenvolvimento da internet no Brasil. Tomasevicius Filho (2016, p. 276) arremata:

> Previu-se nos art. 24 e 25 o estabelecimento de mecanismos de governança multiparticipativa, envolvendo o governo, empresas, sociedade civil e comunidade acadêmica, a racionalização da gestão, expansão e uso da internet no Brasil, em especial, na implantação de serviços de governo eletrônico e se serviços públicos, a adoção preferencial de tecnologias, padrões e formatos abertos e livres, a publicidade de dados e informações públicos na internet e, sobretudo, o estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no Brasil.

3.6.1 Marco Civil da Internet como forma de proteção à privacidade dos internautas

O MCI, ao definir diretrizes para o uso da internet no Brasil, objetivou estabelecer uma forma de proteção ao internauta. Como já bem explicitado no tópico anterior, o MCI trouxe consigo contornos gerais de garantia dos direitos das personalidades, e nesse panorama assumiu um avanço na tutela dos dados pessoais e dos direitos fundamentais. Como preleciona Soares (2014, s.p), "com a aprovação da lei marco civil da internet, foi dado um passo importante para assegurar ainda mais essas garantias constitucionais que eram tão fragilizadas diante da ausência de leis [...]".

Nessa lógica, Oliveira[20] (2013, s.p), analisa os benefícios do marco civil, relatando:

> O Marco Civil determina que o sigilo das comunicações dos usuários da internet não pode ser violado. Provedores de acesso à internet serão obrigados a guardar os registros das horas de acesso e do fim da conexão dos usuários pelo prazo de um ano, mas isso deve ser feito em ambiente controlado. [...] Provedores de acesso e aplicações não poderão ceder dados a terceiros sem que os usuários permitam. O projeto

[20] Disponível em: <http://cut.org.br/noticias/para-entender-a-importancia-do-marco-civil-da-internet-826b/>. Acesso em: 5 abr. 2017

> estabelece proteção aos dados pessoais do internauta - nome, endereço, telefone, fotografias ou outros que possam identificá-lo. Também será obrigada a exclusão de dados pessoais de usuários que termine uma relação com uma aplicação na internet.

Entretanto, mesmo com a criação da lei, é fato que o ordenamento jurídico brasileiro ainda é precário no que tange ao direito virtual. Para Soares (2014, s.p):

> [...] Mesmo esta lei abordando tais princípios, ainda é necessário ampliar esses entendimentos [...] Nosso ordenamento jurídico necessita ainda mais de regulamentos jurídicos, eficientes e capazes de salvaguardar o direito à privacidade e à vida privada, a liberdade de expressão e dados pessoais de todos os cidadãos do país, principalmente no que tange a movimentação de dados eletrônicos, pois é um setor que é ainda é carente de regulamentação.

De modo mais radical é o entendimento de Tomasevicius Filho (2016, p. 276):

> Embora o Marco Civil da Internet tenha sido bastante festejado por ser a primeira lei do mundo a disciplinar os direitos e deveres dos usuários da rede, não se perceberão mudanças substanciais, uma vez que esta não acrescentou praticamente nada à legislação vigente.

Para o doutrinador, seria ingenuidade da parte do legislador brasileiro achar que uma lei nacional solucionaria um problema de escala mundial. Nessa seara, surgem diversas críticas ao MCI, uma delas se refere a redundância que a lei faz à várias disposições do texto constitucional[21], outra, diz respeito a proteção dos usuários na internet, já que o MCI diminuiu a responsabilidade dos provedores de aplicações.

De fato, o que se pode extrair do texto, é que o marco civil é uma lei sem conteúdo normativo, lacunosa e que, do modo como se encontra, não consegue solucionar de maneira eficaz os problemas globais do âmbito virtual.

[21] Exemplos dessa redundância estão presentes no art. 7º, I, do MCI que alude ao art. 5º, X da CF/88 e no art. 7º, II e III que possui o mesmo teor do art. 5º, XII da CF/88.

4 OS CRIMES CIBERNÉTICOS

O presente capítulo busca conceituar e organizar de maneira sistemática os principais crimes cibernéticos. Além disso, se faz uma breve exposição do caso Carolina Dieckmann, explicando como ele ajudou na célere aprovação da lei n.º 12.737/12, apelidada de lei Carolina Dieckmann justamente pelo grande impacto que teve na mídia.

4.1 Definição de crimes cibernéticos

O crescimento exponencial da tecnologia informática fez surgir no meio digital um tipo de crime que se tornou bem frequente nos dias atuais. Segundo Paesani (2013, apud LIRA 2014, p. 39):

> Na segunda metade da década de 1990, com o advento da Internet e da globalização da economia, surge uma nova modalidade de crimes - denominados Crimes eletrônicos ou Crimes Virtuais – cometidos no espaço virtual da rede, através de: e-mails, websites, ou ocorridos em comunidades de relacionamentos na Internet, entre as quais a mais conhecida é o Facebook.

Tal como a criminalidade tradicional, a cibercriminalidade[22] se manifesta de diversas formas e pode ocorrer em qualquer hora ou lugar ocasionando lides que ainda são de difícil elucidação.

Os crimes cibernéticos ou crimes virtuais/digitais são todos aqueles procedimentos praticados contra o sistema de informática ou através deste que atente para os dados na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão. São todas as atividades ilícitas na internet, que variam desde invasões à sistemas até roubo de dados e informações confidenciais. Na mesma linha de pensamento, Rosa (2002, apud RAMOS 2015, p. 18), define:

> A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão [...] 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.

[22] Criminalidade relacionada com o universo cibernético e as redes de comunicação entre computadores ou ainda conjunto de infracções cometidas com recurso às novas tecnologias de informação e de comunicação.

Noutro viés, os crimes convencionais também podem ser classificados como cibercrimes, quando aqueles são realizados por meio de dispositivos eletrônicos, por exemplo, o estelionato virtual[23].

De modo geral, os crimes cibernéticos são definidos como toda conduta ilegal ou não autorizada, que envolva o uso da infraestrutura tecnológica da informática, em que computadores ou dispositivos informáticos são utilizados como instrumentos para sua execução ou consistem em seu objeto material.

4.2 Os principais crimes cibernéticos

O aparecimento dos primeiros relatos de crimes informáticos data da década de 1960, onde o infrator apenas sabotava, espionava ou exercia o uso abusivo de computadores e sistemas. Foi apenas a partir de meados de 1980 que houve um aumento desses tipos de crimes, nascendo assim, práticas como a pirataria, o abuso de comunicação, a pornografia infantil, os crimes contra a privacidade e etc.

Por certo, a enorme gama de crimes virtuais que acontecem atualmente pode ser justificada tanto pela insegurança do meio, como também pelo caráter transnacional da internet e pela sensação de anonimato que ela proporciona. Nas exatas palavras de Camila Requião Fentanes da Silva[24] (2014, p. 47):

> O fato de ser uma rede de comunicação abrangente e individual implica no acontecimento de fraudes, proporcionando insegurança aos seus usuários quanto à utilização de seus dados pessoais na rede, os quais podem ser roubados ou clonados. Por ser uma rede que proporciona relacionamento à distância existe a possibilidade de criação de perfis falsos, bem como a navegação anônima favorece o cometimento de vários ilícitos.

Ainda, Daoun (apud ROSSETO 2011, p. 11), argumenta que as redes sociais aumentaram a incidência dos crimes cibernéticos, pois, "as pessoas tem uma falsa sensação de anonimato e diminuem os freios pessoais quando estão na frente de um teclado e de um monitor. Então, isso, naturalmente, na proporção acaba gerando mais infrações".

Também, Corrêa (2002, apud FENTANES DA SILVA, 2014, p. 48), entende:

> A internet pode ser também identificada como meio perfeito para a ação de comerciantes fraudulentos, pedófilos, piratas de software, traficantes de informação

[23] Ocorre quando o criminoso engana a vítima para conseguir uma vantagem financeira. Pode acontecer em sites de leilões, por exemplo, se o vendedor enganar o comprador recebendo o dinheiro da transação sem entregar a mercadoria.

[24] Disponível em: <https://jus.com.br/artigos/32265/analise-das-leis-n-12-735-2012-e-12-737-2012-e-a-des-necessidade-de-uma-legislacao-especifica-sobre-crimes-ciberneticos>. Acesso em: 14 jun. 2017.

> terrorista, crackers e muito mais. Uma pessoa navegando na internet é perfeitamente vulnerável à ação de hackers, vírus de computadores, podendo até cometer atos ilícitos, quando a usa de forma desmedida, desrespeitando os limites impostos por sistemas de segurança ou até ameaçando alguém anonimamente.

De fato, são incontáveis as infrações que ocorrem no meio digital, sendo assim, o Website Safernet Brasil reuniu um tópico com as 5 (cinco) violações virtuais mais frequentes no Brasil registradas em 2016, vejamos:

Figura 2- Top 5 de violações virtuais no Brasil

Fonte: Safernet Brasil.

Como percebe-se pela imagem acima, o ciberbullying e a exposição íntima figuram no topo da lista, seguidos pelo roubo de dados pessoais, conteúdos de ódio e fraudes. Nesse

diapasão, importante lembrar outros crimes que também são frequentes e fazem parte da realidade digital. Vejamos a seguir.

4.2.1 Veiculação de pornografia através da internet

Esse crime estava previsto no art. 14 do PL nº 84/99, que mais tarde foi convertido na lei ordinária n.º 12.735/12, e sua tipificação consiste em: oferecer serviço ou informação de caráter pornográfico em rede de computadores sem exibir, previamente, de forma facilmente visível e destacada, aviso sobre sua natureza e indicando o seu conteúdo.

Recentemente houve uma alteração no Estatuto da Criança e do Adolescente (ECA), que inseriu os arts. 240 a 241-E, versando sobre a pornografia envolvendo crianças e adolescentes. Além disso, os artigos acrescentam outras condutas como: trocar, transmitir, divulgar, adquirir ou armazenar vídeos ou imagens de caráter pornográfico que contenham crianças e adolescentes. Observa-se a abrangência do texto normativo que, no caput do art. 241-A, dispõe: "por qualquer meio, inclusive por meio de sistema de informática ou telemático".

Importante notar que a alteração do ECA possui caráter específico para casos abrangendo crianças e adolescentes, não se aplicando aos casos de pornografia adulta.

4.2.2 Espionagem e sabotagem informática

Segundo Ramos (2014, p. 21):

> Configura-se espionagem informática pela alteração de programas e troca de peças, modificando a programação original, e facilitando de certa forma o acesso a dados e registros de todo um computador. Sendo assim, ocorre o acesso à computadores de forma intencional e não justificada por pessoas que não estão autorizadas pelo proprietário ou operador do computador, configurando um ato sujeito a ser punido pelo Estado. Já a sabotagem informática tem como elemento objetivo, a destruição ou dano de material ou componente pertencente a um computador. O objetivo da sabotagem são os danos físicos e lógicos, visando inutilizar informações e dados valiosos contidas no computador de alguém.

A alteração dos programas do computador na espionagem informática pode ser feita pela troca de cartões, discos ou fitas originais, por falsos, o que modifica a programação originária e promove assim o acesso ao banco de dados.

No caso da sabotagem informática, ela também pode ser caracterizada pela interferência indevida ou sem autorização contra a funcionalidade do sistema informático, causando-lhe entrave, impedimento, interrupção ou perturbação grave.

4.2.3 Pirataria

O crime de pirataria consiste na distribuição/venda de produtos ou marcas sem a autorização dos autores dos mesmos, não pagando a eles os devidos direitos autorais. Na esfera digital, a pirataria pode ocorrer com softwares, músicas e filmes.

A pirataria de softwares já está regulamentada pela lei n.º 9.609/98, que dispõe sobre a proteção da propriedade intelectual de programas e computadores. Sua tipificação consiste em distribuir ou vender programas de computador sem a autorização do proprietário e não pagando os seus direitos autorais. Também a transferência de músicas através da internet ganhou tipificação após agosto de 2003, quando passou a ser regulada pela lei n.º 10.965/93, que alterou os arts. 184 e 186 do CPB.

4.2.4 Crimes contra a honra

Os crimes contra a honra estão tipificados nos arts. 138 ao 140 do CPB, são eles: calúnia, difamação e injúria. Esses crimes podem ser praticados de diversas maneiras, tanto pessoalmente, como através dos meios de comunicações, por exemplo, televisão e internet.

A calúnia seria o ato de imputar a alguém falsamente fato definido como crime. Nesse caso, o agente causador tem ciência de que o crime é falso, mas mesmo assim o divulga, tornando-o público. No contexto digital, o compartilhamento em redes sociais pode ser considerado uma forma de divulgação do ato.

A difamação seria o ato de imputar fato ofensivo a reputação de alguém. No contexto digital, seria o ato de ofender a reputação de alguém e levar isso ao conhecimento público, o famoso “falar mal”.

Já a injúria é o ato de injuriar alguém ofendendo-lhe a dignidade ou o decoro, porém, nesse caso não é necessário que haja o conhecimento de terceiros, pois, o simples fato da vítima se sentir ofendida já configura o crime.

4.2.5 Crimes contra a privacidade

Como já exaustivamente explanado, a evolução da internet, tornou a proteção à privacidade um fator de preocupação para a sociedade atual. Isso porque a evolução tecnológica facilitou o acesso aos dados pessoais dos internautas. Nesse contexto, em 2012, o computador pessoal da atriz e modelo brasileira Carolina Dieckmann foi invadido, e foram propagadas na

internet inúmeras fotos da atriz em poses sensuais e também fotos de seus filhos em momentos íntimos da família. Como será explicado adiante, tal fato acelerou a aprovação da lei n.º 12.737/12, que visa punir o indivíduo que invade dispositivo informático alheio, a fim de obter, destruir ou adulterar dados sem a autorização expressa ou tácita do proprietário do dispositivo ou instala vulnerabilidades para obter vantagem ilícita.

4.3 O caso "Carolina Dieckmann"

No dia 7 de maio de 2012, a atriz Carolina Dieckmann[25] procurou a polícia para dar início a uma investigação sobre 36 (trinta e seis) fotos íntimas suas que foram publicadas na internet. As fotografias continham imagens de nudez da atriz, além de outras fotos do seu filho de 4 (quatro) anos de idade. A propagação das imagens se deu em virtude da invasão de seu computador pessoal, que foi comandada por quatro crackers dos estados de São Paulo e Minas Gerais.

Nas investigações, o grupo especializado da Delegacia da Repressão aos Crimes de Informática (DRCI), em conjunto com a Polícia Civil do Rio de Janeiro, usaram programas desenvolvidos para esse tipo de situação chegando assim até os suspeitos e descobrindo que eles furtaram mais de 60 (sessenta) arquivos da atriz.

De acordo com informações do site O Globo[26] (2012, s.p), os invasores teriam enviado um e-mail mal intencionado, mais conhecido como spam, para Carolina, que sem querer, clicou e abriu o arquivo em seu computador. Por meio de uma troca de mensagens dos criminosos na internet, os investigadores descobriram como eles teriam conseguido as fotos. Foi utilizado um programa específico que foi enviado para a conta de e-mail da atriz, tal programa mascarado, permitiu que os crackers acessassem seu computador e subtraíssem fotos provavelmente da caixa de e-mails enviados.

Carolina recebia ameaças de extorsão desde o fim de março de 2012, e ainda não havia registrado queixa por temer que o assunto se tornasse público. Conforme Medina (2012, apud LIRA, 2014, p. 38):

> A atriz estava sendo chantageada a pagar R$ 10.000,00 (dez mil reais) para não ter suas curvas divulgadas na rede. Os criminosos efetuaram 03 (três) ligações, bem como enviaram 05 (cinco) e-mails mostrando as fotos para o secretário da atriz, Alisson Oliveira, e seu empresário, Alex Lerner. Nesta oportunidade a atriz "foi orientada por

[25] Famosa atriz brasileira reconhecida por suas atuações em diversas telenovelas e seriados da emissora de televisão Rede Globo.

[26] Disponível em: <http://oglobo.globo.com/rio/apos-identificacao-de-hackers-carolina-dieckmann-afirma-que-espera-justica-4889891> Acesso em 24 abr. 2017.

> autoridades de segurança a manter contato para tentar armar um flagrante", mas não deu certo, segundo relatou seu advogado Antônio Carlos de Almeida Castro.

A empregada doméstica de Carolina foi quem atendeu ao primeiro telefonema do criminoso, depois duas fotos foram enviadas ao seu empresário. De acordo com Sardas (2013, p. 59), a divulgação das fotos na rede se deu devido à recusa do pagamento pedido pelos crackers:

> Os criminosos pediram R$ 10.000,00 (dez mil reais) para não devassarem as curvas da atriz ao grande público, que ironicamente, figura na lista das musas ainda sonhadas pela revista playboy. Sem terem o pedido atendido, em poucos minutos, soltaram na web a coleção de fotos, que, ajudada pela rápida proliferação do meio, ainda pode ser encontrada em diversos sites.

Pelo fato de na época não haver legislação específica que regulasse a prática da invasão de dispositivo informático, a ação judicial promovida por Carolina deparou-se com um obstáculo jurídico. Nesse contexto, Crespo (2013 apud LIRA, 2014, p. 39) apresenta:

> Se eu invadisse uma máquina e me valesse de informações confidenciais para ter um proveito financeiro, eu poderia responder por concorrência desleal, por extorsão, mas não pela invasão [...] Por isso, os invasores responderão por crimes que a legislação brasileira já tipifica: furto, extorsão e difamação.

Nesse seguimento, o delegado responsável pelas investigações, Gilson Perdigão, afirma que foi aberto um registro de ocorrência de extorsão qualificada pelo concurso de agentes, difamação e furto. Destarte, com a promulgação da lei n.º 12.737/12, os crimes iguais ou análogos ao cometido contra a atriz terão tratamento diferenciado, uma vez que a lei tipificou tais crimes e regulou os delitos cibernéticos.

4.3.1 Repercussão na mídia e a célere aprovação da lei

A abertura do caso ao público criou uma grande repercussão midiática. Rapidamente houve uma disseminação das fotos da atriz pelas redes sociais, pelos sites de notícias e pelos jornais populares, ocasionando um verdadeiro alvoroço na web. Foi por conta desse episódio ter sido bastante divulgado, que o legislador brasileiro passou a dar prioridade para a sanção de um tipo penal que tutelasse os dados informáticos.

Não obstante, segundo Galvão (2013), o congresso nacional já vinha discutindo esse tema há mais de uma década. Em 1999, o deputado do PSDB-PE Luiz Piauhylino de Melo Monteiro, apresentou o PL n.º 84/99, que dispunha sobre os crimes cometidos na área da

informática e suas penalidades. Após isso, em 2011, sites do governo brasileiro sofreram diversos ataques de negação de serviços, fato este, que incentivou outros deputados a apresentarem em novembro de 2011 o PL n.º 2.793/11, que dispunha, por sua vez, sobre a tipificação criminal de delitos informáticos. No entanto, tais projetos não obtiveram a devida importância, continuando assim "na sombra".

Somente após a ocorrência do "caso Carolina Dieckmann" que os projetos de lei ganharam força e o congresso nacional tomou providências mais concretas. O caso gerou intensa pressão social para a criminalização, em regime de urgência, dessas condutas que até então não eram previstas como crimes em espécie pelo CPB. Como assevera Ramos (2015, p. 40), "a repercussão da história ocorrida com a atriz foi muito relevante para a aprovação da lei, pois acabou dando velocidade ao processo legislativo e vontade de mudança".

Em conclusão análoga, Lira (2014, p. 55), declara "a pressão da opinião pública, nesse caso, de fato influenciou a célere reação do congresso nacional" [...], é unânime que a grande repercussão do episódio, por envolver uma atriz famosa, foi determinante para a rapidez da aprovação da lei".

Eis que, em 30 de novembro de 2012, foi aprovado, na câmara dos deputados, o PL n.º 35/2012, originado pelo PL n.º 2.793/2011, que por sua vez foi apresentado como proposta alternativa ao PL n.º 84/99. Nessa ocasião, o projeto foi promulgado e sancionado pela presidência da república através da lei n.º 12.737/12, mais conhecida como lei Carolina Dieckmann, da qual trataremos mais detalhadamente no capítulo que se segue.

5 CRIAÇÃO DA LEI N.º 12.737/12 – "LEI CAROLINA DIECKMANN"

O presente capítulo trata da lei n.º 12.737/12, examinando seus dispositivos normativos e seu grau de eficácia em relação ao combate dos delitos informáticos. Além disso, faz-se uma breve análise dos aspectos positivos e negativos da lei e por fim, apresenta-se propostas para melhorias da legislação informática brasileira.

5.1 A lei e suas disposições

A lei n.º 12.737/12 veio tutelar o bem jurídico da liberdade individual e do direito ao sigilo pessoal e profissional, dispondo sobre a tipificação criminal dos delitos informáticos. Essa lei alterou o Código Penal Brasileiro, acrescentando em seu corpo os arts. 154-A e 154-B, intitulados "invasão de dispositivo informático". Outras pequenas modificações também foram realizadas nos arts. 266 e 298, ambos do CPB, para tipificar a "interrupção ou perturbação de serviço informático, telemático ou de informação de utilidade pública" e a "falsificação de cartões de débito e crédito", respectivamente.

Dessa maneira, oportuno trazer à baila o referido diploma legal, "*in verbis*":

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 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 n. 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.
> § 5ºAumenta-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."
> **"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."
> 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 (BRASIL, 2012)

Como visto, a lei supracitada é curta e sem muitas delongas. Com poucos artigos, tentou trazer à sociedade um modo de regulamentar e punir as ações criminosas que vem acontecendo no mundo digital. Contudo, apesar de breve, a recente lei traz em seu bojo enunciados de difícil entendimento.

Para facilitar a compreensão, grandes doutrinadores como, Fernando Capez, Guilherme de Souza Nucci, Luiz Regis Prado e Rogério Greco, formaram um conjunto de ideias, opiniões e ensinamentos dos dispositivos da norma jurídica, mais especificamente no que concerne a: 1) classificação doutrinária, 2) bem jurídico tutelado; 3) objeto material; 4) ação nuclear; 5) sujeitos ativo e passivo; 6) tipicidades objetiva e subjetiva; 7) concurso de agentes; 8) benefícios legais; 9) modalidade equiparada e qualificada; 10) causas especiais de aumento de pena; 11) pena e ação penal; e, 13) competência para julgamento.

Adiante, trataremos de modo mais específico cada um desses tópicos.

5.2 Invasão de dispositivo informático (arts. 154-A e 154-B do CPB)

Os crimes praticados com o uso da tecnologia informática podem seguir duas vertentes: os cometidos com o computador[27] e os cometidos contra o computador[28]. É nesse último aspecto que o art. 154-A foi inserido no rol de crimes do CPB, sendo o crime, cuja conduta ilícita, nos dizeres de Marco Aurélio Rodrigues da Costa[29] (1997, s.p), "tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas".

Vale ressaltar, que para efetiva caracterização do crime é necessário que todos os elementos que compõe o tipo penal se realizem, quais sejam: a) o núcleo invadir; b) dispositivo informático alheio; c) conectado ou não à rede de computadores; d) 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; f) ou instalar vulnerabilidades para obter vantagem ilícita.

Nessa perspectiva, Guilherme de Souza Nucci, anuncia a classificação do delito, adiante exposta.

5.2.1 Classificação doutrinária

Nos ensinamentos de Nucci (2013, p. 777), o delito em voga:

> Trata-se de crime comum (pode ser cometido por qualquer pessoa); formal (delito que não exige resultado naturalístico, consistente na efetiva lesão à intimidade ou a vida privada da vítima, embora possa ocorrer); de forma livre (pode ser cometido por qualquer meio eleito pelo agente); comissivo (as condutas implicam ações); instantâneo (o resultado se dá de maneira determinada na linha do tempo), podendo assumir a forma de instantâneo de efeitos permanentes, quando a invasão ou a instalação de vulnerabilidade perpetua-se no tempo, como rastro da conduta; unissubjetivo (pode ser cometido por uma só pessoa); plurissubsistente (cometido por vários atos).

---

[27] Se subdividem em dois ramos: os crimes cibernéticos impróprios ou comuns e os crimes cibernéticos mistos. Os impróprios, são aqueles em que o computador é usado como instrumento para a execução do crime, porém não há ofensa ao bem jurídico inviolabilidade dos dados ou informações. O agente apenas se utiliza do computador como mera ferramenta a perpetração de crime comum, sendo ele dispensável para consumação do delito. Exemplos: crimes contra a honra cometidos por meio da internet. Já os mistos são todas aquelas ações onde o agente não visa o sistema de informática e seus componentes, mas a informática é instrumento indispensável para a consumação da ação criminosa.

[28] Também conhecidos como crimes cibernéticos próprios ou puros, são aqueles que o bem jurídico protegido pela normal penal é a inviolabilidade dos dados ou informações. O sujeito ativo visa especificamente o sistema de informática, em todas as suas formas. Entendemos que os elementos que compõe o "software", o "hardware", os dados e sistemas contidos no computador e etc. Exemplos: arts. 313-A e 154-A. do CPB.

[29] Disponível em: <https://albertodiwan.jusbrasil.com.br/artigos/199631200/o-crime-de-invasao-de-dispositivo-de-informatica-art-154-a-do-codigo-penal>. Acesso em 09 jun. 2017.

5.2.2 Bem jurídico tutelado

O bem jurídico tutelado é a inviolabilidade dos dados informáticos, que além de abranger o direito à privacidade e ao sigilo de dados, também tutela a proteção contra qualquer alteração ou destruição.

Nesse diapasão, Nucci (2013, p. 774/775), aduz:

> Insere-se no contexto dos crimes contra a liberdade individual, bem jurídico mediato a ser tutelado. Porém, de forma imediata, ingressou, com propriedade, no campo dos crimes contra a inviolabilidade dos segredos, cuja proteção se volta à intimidade, à vida privada, à honra, à inviolabilidade de comunicação e correspondência, enfim, a livre manifestação do pensamento, sem qualquer intromissão de terceiros.

5.2.3 Ação nuclear

Referente a ação nuclear do tipo, o núcleo central se consolida no verbo "invadir", isto é, ingressar virtualmente sem autorização expressa ou tácita do titular do dispositivo. No entanto, é lógico que na conduta de invadir está implícita a ausência de autorização do proprietário, caso contrário, não há de se falar em invasão. Reforçando esse parecer Capez (2013, p. 346), elucida:

> A conduta de invadir traz ínsita a ausência de autorização do proprietário ou usuário do dispositivo, pois não se pode dizer que houve invasão quando o acesso se dá mediante sua aquiescência. Mesmo assim, o tipo penal do art. 154-A, caput, do CP, de modo supérfluo, repete ao final a exigência do elemento normativo do tipo "sem autorização expressa ou tácita do titular do dispositivo".

5.2.4 Objeto material

Acerca do objeto material, Fernando Capez (2013), explica que o crime consiste em invadir dispositivo informático alheio (hardware) utilizado para rodar programas (softwares), ou ser conectado a outros equipamentos (smartphone, tablet). O dispositivo informático deve ser de titularidade de terceiros podendo ou não estar conectado à internet.

A invasão deve se dar por meio de violação indevida de mecanismo de segurança (antivírus, firewall, senhas e etc.) instituído pelo próprio usuário do dispositivo. Por fim, para que o crime se aperfeiçoe é exigida a finalidade especial do agente de buscar a obtenção, adulteração ou destruição de dados e informações.

5.2.5 Sujeito ativo e passivo

A invasão de dispositivo informático é crime comum, assim, o sujeito ativo pode ser qualquer pessoa, uma vez que o tipo penal não exige nenhuma qualidade especial do agente. Túlio Lima Vianna (2013) explica ainda que o sujeito ativo não deve estar autorizado a acessar os dados, exceto, claro, o proprietário do dispositivo informático.

Nesse sentido, até mesmo o cônjuge ou o empregador podem ser sujeitos ativos se não tiverem autorização para o acesso. Já sujeito passivo é qualquer pessoa física ou jurídica dona dos dados informáticos, que pode sofrer dano material ou moral em decorrência da invasão indevida do dispositivo ou em consequência da instalação de vulnerabilidades.

5.2.6 Tipicidade objetiva e subjetiva

Cezar Roberto Bittencourt (2014) leciona que se trata de um tipo penal complexo que possui um elemento especial de antijuridicidade – mediante violação indevida de mecanismos de segurança – e ainda com dois elementos subjetivos – (i) com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou (ii) instalar vulnerabilidades para obter vantagem ilícita.

Em relação ao tipo subjetivo é o dolo genérico, ou seja, a vontade livre e consciente de acessar os dados sem autorização da vítima, mediante violação indevida de mecanismo de segurança ou de instalar no mesmo vulnerabilidades. Não se admite modalidade culposa.

Sendo assim, Nucci (2013, p. 776), esclarece sobre o tipo subjetivo:

> É o dolo. Há elemento subjetivo do tipo específico para as duas condutas previstas no tipo. No tocante à invasão de dispositivo informático é o fim de obter, adulterar ou destruir dados ou informações. Focaliza-se a obtenção (ter acesso a algo), a adulteração (modificação do estado original) ou a destruição (eliminação total ou parcial) de dados (elementos apropriados à utilização de algo) ou informações (conhecimento de algo em relação a pessoa, coisa ou situação). Quanto à instalação de vulnerabilidade é a obtenção de vantagem ilícita (qualquer lucro ou proveito contrário ao ordenamento jurídico). Pode ser, inclusive, a obtenção da invasão do dispositivo informático em momento posterior para obter dados e informações.

5.2.7 Concurso de agentes

É perfeitamente possível a participação e coautoria nesses crimes, sendo estas unilateral ou plurilateral. Unilateral, quando os agentes utilizam apenas um computador para prática do crime, e plurilateral, quando são utilizados dois ou mais computadores. No caso da atriz

Carolina Dieckmann, houve coautoria na invasão do seu computador, já que o crime foi praticado por quatro pessoas em locais diferentes.

5.2.8 Benefícios legais

A respeito dos benefícios legais, Nucci (2013), esclarece que mesmo a forma qualificada é infração de menor potencial ofensivo, o que comporta o instituto da transação penal[30]. Caso este não seja possível, outros institutos podem ser aplicados, por exemplo, as penas restritivas de direito e o regime aberto. Fato interessante, é que a forma qualificada do tipo consiste em figura subsidiária, isto é, somente se pune caso não existe delito mais grave.

5.2.9 Modalidade equiparada e qualificada

A modalidade equiparada, no entendimento de Capez (2013), encontra-se no § 1º, do art. 154-A que responsabiliza com pena de detenção de 3 (três) meses a 1 (um) ano e multa, quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a invasão de dispositivo informático alheio.

Tais programas nada mais são do que softwares utilizados para permitir a invasão do computador alheio, os conhecidos "cavalos de tróia". Existem programas que funcionam como "espiões", coletando os dados digitados no computador, o que acaba possibilitando a violação de informações sigilosas como senhas e contas.

A modalidade qualificada, por sua vez, encontra-se no § 3º, do art. 154-A que responsabiliza com pena de 6 (seis) meses a 2 (dois) anos e multa 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. O foco da qualificação se refere à natureza dos dados e informações obtidos, quer dizer, aqueles relacionados a comunicações privadas, segredos comerciais ou industriais, informações sigilosas ou controle remoto não autorizado.

---

[30] A transação penal tem o objetivo de evitar que contra um suposto autor de fato delituoso seja instaurada uma ação penal. É cabível nos casos de delitos de menor potencial ofensivo, ou seja, aqueles cuja a pena máxima não ultrapassa 2 (dois) anos. Entretanto, existem dois casos que mesmo sendo de menor potencial ofensivo, não cabe a transação penal, são eles: quando o suposto autor da infração tiver sido condenado, pela prática de crime, à pena privativa de liberdade, por sentença definitiva; e quando não indicarem os antecedentes, a conduta social e a personalidade do agente, bem como os motivos e as circunstâncias, restando não ser suficiente a adoção da medida. Os objetivos da transação penal são desburocratizar o processo penal; fazer com que a justiça criminal seja mais célere; evitar que o suposto infrator enfrente um processo criminal que poderá culminar com uma condenação e etc.

5.2.10 Causas especiais de aumento de pena

As causas de aumento de pena se encontram nos §§ 2º, 4º e 5º, do art. 154-A e são de duas espécies. Uma incide sobre as figuras simples e equiparada e as outras sobre as figuras qualificadas.

Nas figuras simples e equiparada, a pena é aumentada de 1/6 (um sexto) a 1/3 (um terço) se da invasão resulta prejuízo econômico, ou melhor, se resulta em perda material ou financeira. Nesse caso, se o prejuízo for moral não haverá incidência dessa causa de aumento.

Nas figuras qualificadas, o § 4º diz que a pena é aumentada de 1/3 a 2/3 (um a dois terços) se houver divulgação, comercialização ou transmissão a terceiros, dos dados ou informações obtidos. Já nos termos do § 5º, a pena é aumentada de 1/3 a ½ (um terço a metade) se quaisquer dos crimes (previstos no caput, e nos §§ 1º e 3º do art. 154-A) for praticado contra: presidente da república, governadores e prefeitos; presidente do supremo tribunal federal; presidente da câmara dos deputados, do senado federal, de assembleia legislativa de estado, da câmara legislativa do distrito federal ou de câmara municipal; e dirigente máximo da administração direta e indireta, federal, estadual, municipal ou do distrito federal.

5.2.11 Pena e ação penal

Em relação a pena e a ação penal, Prado (2014, apud LIRA, 2014, p. 47), explana:

> A pena prevista para o delito do artigo 154-A é de detenção, de 3 (três) meses a 1 (um) ano, e multa.
> Como observado, 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, a pena passa a ser de reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constituir crime mais grave (§3º).
> O artigo 154-B determina que a ação penal nos delitos definidos pelo artigo 154-A será pública condicionada, salvo se o crime é cometido contra Administração Pública Direta ou Indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos, hipótese em que a ação é pública incondicionada.

Sem esgotar o assunto, quando o delito for praticado contra pessoa física é necessária autorização da mesma para que o ministério público inicie a ação penal, sendo então uma ação penal pública condicionada à representação. A representação somente é desnecessária nos casos em que o sujeito passivo é o Estado, sendo desse modo, uma ação penal pública incondicionada.

5.2.12 Competência para julgamento

A competência para julgamento tem gerado muitas discussões atualmente. Alguns doutrinadores, como Vianna (apud, LIRA, 2014) inferem que quando um crime é praticado na internet, deve ser julgado pela Justiça Federal, uma vez que, a internet é um serviço público da União. Todavia, pela interpretação literal do art. 109 da CFB/88, não há nenhum dispositivo fazendo referência aos crimes cometidos pela internet. O que pode se levar em conta para a competência ser da justiça federal, estaria inscrito no inciso IV do mesmo artigo, o qual trata dos crimes virtuais cometidos contra o Estado, veja-se:

> Art. 109. Aos juízes federais compete processar e julgar:
> (...)
> IV - os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral;

Logo, entende-se, que se o crime for cometido dentro do território nacional mas não estiver nas hipóteses do art. 109 da CFB/88, a competência será da justiça estadual. Em conclusão análoga, Galvão (2013, apud LIRA, 2014, p. 47):

> A competência para processar e julgar o crime é do Juizado Especial da Justiça comum estadual. No entanto, a competência será do Juizado Especial da Justiça comum Federal quando o crime for cometido contra a administração pública, direta ou indireta, de qualquer dos Poderes da União, quando cometidos a bordo de navios ou aeronaves brasileiras, quando o sujeito ativo ou a vítima for funcionário público federal no exercício de suas funções (inciso IV do art. 109 da CF – Súmula n. 147 do STJ), ou se houver concurso com um crime da competência da Justiça Federal (Súmula n. 122 do STJ).

5.3 Interrupção ou perturbação de serviço telegráfico, telefônico, informático, ou de informação de utilidade pública e falsificação de documento particular (arts. 266 e 298 do CPB)

Insta salientar, que a referida lei modificou o CPB nos arts. 266 e 298, que passaram a vigorar com a seguinte redação:

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um a três anos, e multa.
> § 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.

> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
> Pena - reclusão, de um a 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.

Sobre esses artigos faremos uma rápida descrição apenas para melhor explicar do que eles tratam.

5.3.1 Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (art. 266 do CPB)

Trata-se de crime comum, doloso, comissivo, de perigo, instantâneo, monossubjetivo, plurissubsistente e não transeunte. O bem jurídico tutelado é a incolumidade pública, mas, nesse caso, apenas quando abarca condutas que atingem um número indeterminado de pessoas e nunca a uma vítima ou grupo de vítimas determinado. O objeto material é o serviço telemático[31] ou de informação pública[32]. O sujeito ativo é qualquer pessoa e o passivo é a coletividade em geral. O elemento objetivo do tipo, segundo informa Nucci (2013, p. 1075), "é o dolo de perigo (gerar risco intolerável a terceiros). Não há elemento subjetivo específico, nem se pune a forma culposa". O delito consuma-se, segundo relata Capez (2013, p. 547) "com a prática dos atos que interrompam, perturbem o serviço ou que impeçam ou dificultem seu restabelecimento. Cuida-se aqui mais uma vez de crime de perigo abstrato, isto é, presumido. A tentativa é admissível".

A pena se aplica em dobro se o delito é cometido por ocasião de calamidade pública, quer dizer, durante uma situação excepcional ou de tragédia coletiva, por exemplo, guerras e inundações. Quanto aos benefícios legais, ação penal, a suspensão condicional do processo e a competência para julgamento, Vianna (2013, apud LIRA, 2014, p. 50-51), explana:

> Tem-se um crime que é processado mediante ação penal pública incondicionada em que, considerando os patamares mínimo e máximo cominados ao delito em apreço (detenção, de um a três anos, e multa), há a possibilidade de aplicação da suspensão condicional do processo (art. 89 da Lei nº 9.99/95). Contudo, se a conduta do art. 266

---

[31] Aquele formado pela união de tecnologias de transmissão de dados proveniente de recursos das telecomunicações (v.g.: telefonia, satélite, fibras ópticas, entre outros) com recursos atrelados à informática (v.g.: computadores, softwares, entre outros), junção esta que permite o processamento e a transmissão de grande quantidade de dados em diversos formatos de modo instantâneo, destacando-se textos, sons e imagens. A título exemplificativo, podemos citar alguns softwares de destaque nesse segmento, são eles: MSN, Skype, WhatsApp, entre outros.

[32] É aquele que tem como destinatário direto a coletividade como um todo, e não apenas determinado órgão oficial, não se prestando como tal, por exemplo, os chamados "serviços de inteligência", especialmente das autoridades repressoras.

> do CPB for cometida por ocasião de calamidade pública, a pena deverá ser duplicada, e, portanto, inviável será a aplicação do benefício da suspensão condicional do processo. Isto porque a pena mínima que, *a priori*, era de um ano, será obrigatoriamente de dois anos. Por fim, ressalta-se que, como a pena máxima em abstrato excede a dois anos, a competência para julgamento do crime é do juízo comum e não do JECrim.

5.3.2 Falsificação de documento particular (art. 298 do CPB)

Trata-se de crime comum, doloso, comissivo, de forma livre, instantâneo, monossubjetivo, plurissubsistente e não transeunte. O bem jurídico tutelado é a fé pública. O objeto material, nas lições de Greco (2014, p. 955), "é o documento particular falsificado, no todo ou em parte, ou o documento particular verdadeiro que foi alterado pelo agente". O sujeito ativo pode ser qualquer pessoa, já o passivo é primariamente o Estado e depois pode ser a pessoa prejudicada pela falsificação. O tipo subjetivo é o dolo, caracterizado na vontade livre de falsificar documento particular. Sob a pena, ação penal e suspensão condicional do processo, Greco (2014, p. 956), expõe:

> A pena cominada ao delito de falsificação de documento particular é de reclusão, de 1 (um) a 5 (cinco) anos, e multa. A ação Penal é de iniciativa pública incondicionada. Será possível a confecção de proposta de suspensão condicional do processo, nos termos da Lei 9.099/95).

A competência para julgamento, de acordo com Vianna (2013, apud LIRA 2014), é do juizado comum. Por fim, vale lembrar, que com a alteração do art. 298, a lei equipara cartão de crédito e débito a documento particular, pois, segundo Fentanes da Silva (2014, p. 67), isso ocorre "no intuito de evitar o uso indevido e criminoso das informações pessoais de terceiros para a prática de fraudes eletrônicas".

Ultrapassada a análise da lei, passaremos a discorrer sobre seus efeitos, destacando os aspectos positivos e negativos que ela trouxe.

5.4 Efeitos da lei Carolina Dieckmann

Como já exaustivamente explanado, as mudanças que a revolução da internet proporcionou tornaram a sociedade mais vulnerável a ações criminosas de pessoas que antes praticavam tais condutas sob o manto da impunidade. Em verdade, um dos fatores que mais contribuíram para que surgissem novos crimes foi a fragilidade das leis brasileiras. Nessa ocasião, Amâncio (2013, apud LIRA 2014) entende que, de fato, muitas condutas podiam ser abrangidas por disposições já existentes na Constituição, no Código Penal, no Código Civil e

no ECA, porém, a criação de leis específicas, torna a repressão à cibercriminalidade mais impositiva.

Em relação a mudança social que a lei trouxe, Paesani (2013, apud LIRA, 2014, p. 54), declara: "inequívoco afirmar que a lei dos delitos informáticos, ao alterar o Código Penal, almeja prevenir a ação delituosa, porém, não possui o alcance de promover mudança na estrutura social". Com isso a autora quis demonstrar que a possibilidade de mudança na estrutura social depende da futura efetividade que o instituto poderá fornecer, principalmente no que diz respeito ao fundamento para ações do ministério público e decisões do poder judiciário para inibir os delitos informáticos.

Ainda de acordo com a reportada autora, a promulgação da lei é uma etapa de amoldamento do direito brasileiro à sociedade da informação, já que as normas e o recurso ao aparelho judiciário não são os únicos mecanismos de solução de conflitos nas sociedades. Entretanto, a inovação legislativa é tida como uma positivação jurídica que vem auxiliar no combate ao crime cibernético no Brasil.

Nessas circunstâncias, passaremos a discorrer sobre os efeitos da lei, analisando os seus aspectos positivos e negativos.

5.4.1 Aspectos positivos da lei Carolina Dieckmann

A criação da lei n.º 12.737/12 coadunou com as necessidades atuais da população. Mesmo ainda limitada, a lei revelou-se como um grande salto na proteção às vítimas dos crimes virtuais, além de representar um avanço legislativo pátrio, afinal criou-se um novo bem jurídico, qual seja, o dispositivo informático.

O advento da lei acabou trazendo mais segurança jurídica e maior rigor penal. Conforme parecer de Mazoni (apud RAMOS, 2013, p. 41), "a lei é positiva no sentido de estabelecer maior rigor penal (as penas variam de um a três anos de detenção mais multa). Esperamos que isso possa causar uma sensação de que o risco de punição é maior". Também, os magistrados não precisarão mais utilizar a analogia para aplicar a legislação que puna condutas semelhantes[33], pois, a lei em voga veio particularizá-las. Nesse sentido, Blum (2013, apud LIRA, 2014, p. 57) acrescenta, "pode parecer estranho, mas até a publicação da lei n.º

[33] A violação de e-mail era enquadrada como crime de violação de correspondência, previsto na Lei n.º 6.538/78, que, em seu art. 40, estatui que é crime devassar indevidamente o conteúdo de correspondência fechada dirigida a outrem, estabelecendo a pena de detenção, de até seis meses, ou o pagamento não excedente a vinte dias-multa.

12.737/12, invadir dispositivos informáticos no Brasil não era crime. [...], Casos como o de Carolina eram decididos com adaptações de artigos que já constavam no CPB".

Rodrigo Alves Zaparoli[34], também enaltece as vantagens da lei, ao afirmar:

> A entrada em vigor da presente lei, independente de sua motivação para aprovação acaba por ser um primeiro avanço à tutela jurídica existente para coibir e ao mesmo tempo sancionar os crimes praticados no ambiente virtual. Logo, a legislação pátria passa a contar com novas ferramentas de apoio à sociedade que antigamente se reservava à esfera cível para buscar alguma espécie de reparação/sanção, esta que em momento algum deixava de ser restrita ao campo monetário.

Observa-se assim que o legislador pátrio conseguiu significativo avanço com as alterações realizadas, pois estas, além de demonstrar uma evolução do nosso ordenamento complementam os institutos jurídicos existentes. Na verdade, o que se espera da lei em toga é que haja uma justiça mais ágil, afinal, a norma possui sim instrumentos capazes de criminalizar a invasão de dispositivos informáticos e reprimir a ação desses agentes.

5.4.2 Aspectos negativos da lei Carolina Dieckmann

Na opinião de Loes (apud LIRA, 2014), a criação da lei que regula os crimes digitais foi apenas o primeiro passo, já que as lacunas do texto e a infraestrutura deficitária da polícia podem atrapalhar, além de que a lei dependerá de jurisprudência para funcionar.

De acordo com alguns operadores do direito digital, um dos principais pontos fracos da lei se refere a punição. A pena, que varia de 3 (três) meses a 1 (um) ano de detenção, não seria severa o suficiente para prevenir a ocorrência da prática delituosa.

Nesse sentido, França (2013, apud LIRA, 2014) elucida que a pena máxima cominada ao diploma legal afasta o crime para o rito sumaríssimo dos juizados especiais, facilitando assim, a suspensão condicional do processo, a conciliação, a composição civil dos danos e a transação penal.

Do mesmo modo, o presidente da Organização Não Governamental (ONG) Safernet Brasil, Tavares (2013, apud LIRA, 2014, p. 61) complementa:

> Ainda que a medida seja exaltada pelo esforço de tipificação, [...], as penas estabelecidas para a invasão de computadores, celulares, tablets e contas de e-mails têm sido vistas como brandas. O tempo de reclusão é de três meses a um ano, com previsão de fatores de majoração de pena. "No Brasil, se o réu for primário, penas

[34] Disponível em: <http://www.direitonet.com.br/artigos/exibir/7936/Comentarios-a-Lei-no-12737-12>. Acesso em: 19 jun. 2017.

> inferiores a quatro anos podem ser convertidas, por exemplo, à prestação de serviços à comunidade. Ou seja, ninguém vai para a cadeia por esse crime".

Blum (2013, apud LIRA, 2014, p. 62), por sua vez, estima que as penas leves impostas ao réu primário viabilizam a conversão em pagamento de cestas básicas. Nesse caso, cria-se um novo problema: a nova lei pode estimular o delito ao invés de coibi-lo, pois:

> Tem muito computador por aí com informação que vale muito mais do que uma cesta básica […], Aos criminosos, cometer o delito, ser pego e ter de pagar pelo crime de invasão pode compensar. Isso se o sujeito for pego, identificado e julgado a tempo. Como as penas para o crime são pequenas, elas prescrevem rapidamente, inviabilizando a punição.

Dessa forma, a pena cominada precisa ter o mínimo de força dissuasória para garantir sua função, que é a de prevenir a ocorrência e recorrência dos comportamentos criminosos.

Além disso, críticas foram feitas pelo fato de a lei ter sido criada às pressas em resposta ao público fã da atriz Carolina Dieckmann. Essa pressão acelerou a aprovação do PL, sem que fossem analisadas outras formas de se cometer crimes através da internet.

O termo "dispositivo informático" também foi alvo de críticas, pois, de acordo com alguns juristas, o legislador deveria usar o termo "dispositivo eletrônico", já que, hoje em dia, é possível ter acesso a internet através de diferentes tipos de dispositivos, por exemplo, celular, tablet, televisão e etc.

Outra ressalva, está relacionada à "violação indevida de mecanismos de proteção do computador", uma vez que, se o computador não possuir antivírus ou senhas, não há como demonstrar que ocorreu a violação. Brito (2013, apud LIRA, 2014, p. 58), destaca que é importante "que se observe cada elementar do crime para que se tenha total noção dos limites da imputação penal". A elementar invadir seria "entrar sem autorização do proprietário". Já a elementar mediante violação indevida de mecanismo de segurança significa que "só haverá o crime do art. 154-A se o autor da conduta usar sua habilidade para superar a proteção do sistema informático, por mais simples que ela seja". Logo, se o dispositivo estiver completamente desprotegido, não há crime.

Por fim, Loes (apud LIRA, 2014) entende que o fato dos crimes possuírem penas pequenas requer uma apuração veloz para à lei funcionar, pois, caso contrário, não haverá punição devido a prescrição. Do mesmo modo, Crespo (2013, apud LIRA, 2014, p. 66), aduz, "como a pena é pequena, o prazo para investigar o crime é menor. Então, se você coloca uma investigação curta com exigências complexas, como perícias demoradas, muitas penas vão prescrever".

Esse é inclusive um dos maiores entraves para o sucesso da lei, visto que o Brasil ainda carece de profissionais treinados para lidar com esses delitos, apesar de já possuir alguns centros de excelência em perícia digital. Nessa seara, Bissoli (2013, apud LIRA, 2014, p. 65) alerta que diante da atual conjuntura é necessário se ter uma equipe competente e rápida, já que, "os rastros do crime digital são frágeis e sem uma perícia competente e rápida, pouco se salva".

5.5 Propostas de possibilidades para melhoria da lei Carolina Dieckmann

De acordo com Loes (apud LIRA, 2014), a lei para tornar-se efetiva terá que passar por algumas modificações, a começar pela própria letra do texto. Segundo especialistas o texto normativo encontra-se excessivamente ambíguo, o que atrapalha a implantação da nova legislação. Alguns conceitos como "dispositivo informático", "mecanismos de segurança" e "obtenção de dados" estão pouco claros o que pode dar margem pra interpretações oportunistas. Nesse contexto, Blum (2013, apud LIRA, 2014, p. 69), indaga sobre mecanismo de segurança:

> Usuários que não usam um sistema de segurança, como uma senha, não estão protegidos pela lei? Em casos nos quais o usuário tem uma senha, mas o aparelho foi violado quando o dispositivo estava temporariamente desbloqueado, a vítima continua sem a proteção da lei?

Bissoli e Blum (2013, apud LIRA, 2014, p. 69), questionam também acerca do verbo obter dados, "quando a lei fala em obter dados, não se sabe se ela diz respeito apenas ao criminoso que copia ou retira os dados de um dispositivo invadido ou também ao criminoso que só faz a consulta desses dados, sem copiá-los".

Desta feita, necessário atentar-se para amplitude e aplicabilidade da lei, pois, quanto mais ampla for a legislação, mais aplicável ela é. Luiz Flávio Gomes, no V Congresso – Crimes Eletrônicos – Formas de Proteção, critica a eficácia da lei, já que cada disposição possui um verbo, e cada verbo emana uma interpretação diferente que varia de juiz para juiz. Assim, conclui o aludido autor que a lei Carolina Dieckmann dependerá de jurisprudências e leis complementares para funcionar efetivamente.

Além disso, como os delitos informáticos ultrapassam fronteiras nacionais, é relevante o estudo do direito comparado de legislações e tratados estrangeiros para tentar encontrar um meio de adoção de medidas satisfatórias na justa punição dos criminosos. Nesse ínterim, em 2001, foi realizada a convenção sobre o cibercrime, mais conhecida como Convenção de Budapeste, na qual, sugeriu-se a uniformização da legislação penal pelo mundo e os mecanismos e instrumentos de colaboração visando vencer a luta contra a criminalidade no

ambiente virtual. Nas claras lições de Brito (2013, apud LIRA, 2014, p. 79), os objetivos fundamentais da convenção são:

> [...] a) harmonizar a tipicidade penal no ambiente do ciberespaço pelos Estados signatários; b) definir os elementos do sistema de informática promovendo a unidade na interpretação da legislação penal interna e possibilitar a credibilidade da prova eletrônica no ambiente virtual; c) implementar um sistema rápido e eficaz de cooperação internacional no combate à criminalidade informática.

Nesta oportunidade, o que Tatiana Malta Vieira (2009) propõe é comparar a legislação nacional com a Convenção de Budapeste de forma a auxiliar eventuais propostas de reformas penais na lei brasileira. Todavia, Brito (2013, apud LIRA, 2014, p. 87), destaca que boa parte das condutas que a convenção tutela já se encontram na legislação penal brasileira. Apesar disso, muitos projetos de lei, vem sofrendo alterações significativas em seu conteúdo, devido à "importância da intervenção de profissionais especializados em delitos informáticos - para que não se aprove uma lei que gere problemas de ordem prática ou que apresente dispositivos que desrespeitem preceitos fundamentais do estado democrático de direito".

Nesse diapasão, Spencer (2013, apud, LIRA, 2014, p. 95), relata que outra proposta de combate aos crimes cibernéticos foi elaborada pela Organização das Nações Unidas (ONU), onde criou um texto denominado "Manual para prevenção e controle dos delitos relacionados com computadores", o qual aponta os principais problemas na temática, vejamos:

> a) a falta de um consenso global sobre quais tipos de conduta deveriam ser considerados delitos relacionados com computadores; b) a ausência de um consenso acerca da definição legal de condutas criminosas; c) ausência de conhecimento técnico por parte da polícia, Ministério Público e das cortes ao tratar do tema; d) a falta de adequação dos poderes para investigar e acessar sistemas informáticos, incluindo a inaplicabilidade dos poderes de sequestro (medidas constritivas) para bens intangíveis como os dados computadorizados; e) a falta de harmonia entre procedimentos legais de diferentes nações concernentes à investigação de delitos relacionados com computadores; f) a caráter transacional de muitos delitos de computador; e; g) a falta de tratados de extradição e de assistência mútua e mecanismos de coação sincronizados que permitam a cooperação internacional, ou a incapacidade que os tratados existentes têm para lidar com as necessidades especiais de investigação de delitos de computador.

O renomado autor acredita, que a elaboração dessa proposta de prevenção e controle dos delitos informáticos, possa ser capaz de contribuir para uma melhor compreensão da legislação penal do Brasil.

Outras propostas para sanar os problemas foram sugeridas pelo Oitavo Congresso das Nações Unidas para Prevenção de Crimes e Tratamentos Criminosos. De acordo com Spencer (2013, apud LIRA, 2014, p. 96), algumas dessas propostas são:

> a) Modernização das leis e procedimentos criminais, incluindo-se medidas para:
> 1. assegurar que os tipos existentes e as leis relativas a poderes de investigação e admissibilidade de evidências em procedimentos judiciais apliquem-se adequadamente e, se necessário, fazer mudanças;
> 2. na falta de leis que se apliquem adequadamente, criar tipos penais e procedimentos investigativos para coleta de evidências que necessariamente sejam capazes de lidar com as novas e sofisticadas formas de atividade criminosa;
> 3. providenciar o confisco ou a restituição de bens adquiridos ilegalmente pelo cometimento de delitos relativos a computador;
> b) Melhoria de segurança de computadores e medidas de prevenção, levando-se em conta problemas relacionados à proteção da privacidade, o respeito aos direitos humanos e direitos fundamentais e qualquer mecanismo regulatório pertinente a uso de computadores; c) Adoção de medidas para sensibilizar o público, o judiciário e as agências reguladoras sobre o problema e a importância da prevenção acerca de delitos relacionados a computadores; d) Adoção de medidas para treinamento adequado de juízes, oficiais e agências reguladoras responsáveis pela prevenção, investigação, persecução e adjudicação de delitos econômicos e relacionados a computadores;
> e) Elaboração, em colaboração com organizações interessadas, de regras sobre ética no uso de computadores e ensinamento de tais regras como parte do currículo e treinamento em informática; f) Adoção de políticas para as vítimas de delitos relacionados com computadores para que sejam conscientes com a Declaração das Nações Unidas de Princípios Básicos de Justiça para Vítimas de Crime e Abuso de Poder, incluindo a restituição de bens ilegalmente obtidos e medidas de encorajamento das vítimas a comunicar tais crimes às autoridades competentes.

5.5.1 Adesão a tratados e convenções internacionais, com o intuito de uniformizar a legislação penal para delitos informáticos

Pinheiro (2010) realiza diversas indagações a respeito da criação de um ordenamento jurídico global. Segundo ela, será que a sociedade digital caminha no sentido de se criar um ordenamento jurídico global? Como tratar as situações de obrigações ou mesmo de ilícitos ocorridos nos meios eletrônicos e que envolvam múltiplos países ou ordenamentos jurídicos? Seria possível assinar uma carta de princípios gerais, aplicável a qualquer um e em qualquer lugar, que pudesse contribuir e facilitar o tratamento das questões digitais, aumentando o grau de segurança jurídica das relações eletrônicas?

A autora sustenta a ideia de que nas próximas reuniões referentes a sustentabilidade na internet, seria necessário assumir a criação de uma Corte internacional para julgamento de ilícitos virtuais, que seriam regidos pelos princípios do acesso e da celeridade, bem como, utilizados os recursos da mediação e arbitragem. Porém, importante destacar, que tal direito supranacional não retiraria a autonomia dos Estados, pelo contrário:

> […], Seria a única forma de garantir a aplicação da justiça na era das fronteiras da informação, em que o espaço e tempo foram relativizados. Nesse sentido, se os Estados não encontrarem uma solução viável para os conflitos da era digital, corremos o risco de voltar ao estado de natureza, a se "fazer justiça com o próprio mouse". (PINHEIRO, 2010, p. 97).

Atualmente, o único instrumento transnacional referente a legislação sobre crimes cibernéticos é a Convenção de Budapeste, onde aos países signatários, recomenda-se a adaptação das suas respectivas legislações penais informáticas de modo a torná-las uniformes. Esse fato justifica a pressão internacional para que o Brasil assine a convenção. É com esse intuito, que o poder legislativo vem unindo forças para efetuar as modificações pertinentes junto ao CPB e legislação especial. (BRITO, apud LIRA, 2014).

Finalmente, como elucida Pinheiro (2013), o que devemos fazer é acompanhar todos os projetos e tratados para internet, principalmente no que se refere aos delitos informáticos, afinal, legislar sobre esses temas novos não é fácil, mas os desafios precisam ser vencidos, de modo que, não existe lei perfeita, mas necessária.

6 CONSIDERAÇÕES FINAIS

No presente estudo monográfico, procurou-se demonstrar, tomando-se por base a frágil privacidade da Era digital (fato que gera inúmeros crimes virtuais), de que maneira a criação da lei n.º 12.737/12 (lei Carolina Dieckmann), pôde colaborar no combate e prevenção de tais crimes, analisando-se seu grau de eficácia, seus aspectos positivos e negativos, bem como quais as possibilidades de melhorias de reforma da lei para que a mesma consagre uma maior efetividade.

Assim, inicialmente, reitera-se que os direitos fundamentais da intimidade, vida privada, honra e imagem das pessoas são garantias invioláveis que merecem a tutela do Estado. Dentre eles, a privacidade é o bem da vida mais cara ao ser humano, já que sem ela, o homem expõe-se de modo a violar sua própria personalidade. Dessa maneira, estudou-se acerca do que se trata o direito constitucional à intimidade e vida privada, por meio da previsão constitucional e pelas lições doutrinárias de renomados autores, pontuando os limites e exceções oponíveis a ele.

Posteriormente abordou-se o tema da fragilidade da Era digital. Com a chegada da Era digital, estão em risco os nichos mais preciosos da privacidade, pois, os avanços tecnológicos proporcionaram um crescimento exponencial dos riscos virtuais, riscos estes que podem gerar a prática de crimes que ofendem os direitos fundamentais. Essas práticas delituosas foram impulsionadas sobremaneira pela frágil privacidade que a internet possui, conjuntamente com a escassa legislação brasileira sobre direito virtual. Outrossim, procedeu-se a análise das medidas para combater a invasão da privacidade na internet, listando-se alguns cuidados que os internautas devem tomar.

Ato contínuo, com base na frágil privacidade virtual, discutiu-se sobre os crimes cibernéticos, descrevendo os principais crimes digitais atualmente. Nesse ínterim, chamou-se atenção para o famoso caso da atriz Carolina Dieckmann, ocasião onde seu computador pessoal foi invadido por crackers e diversas fotos intimas suas foram divulgadas na rede, o que ocasionou uma repercussão midiática sem limites. Tal repercussão acelerou o projeto de lei que tramitava na câmara e em 2012 foi sancionada a lei n.º 12.737/12, tipificando criminalmente os delitos informáticos.

Logo após, para melhor compreensão da lei, analisou-se seus dispositivos normativos, como, o objeto material, sujeito ativo e passivo, pena e ação penal e etc. Na oportunidade, tratou-se dos efeitos da lei, observando seus aspectos positivos e negativos, bem como sugeriu-se propostas para melhoria da eficácia da lei em voga. Sem dúvidas, o advento da norma trouxe um avanço legislativo, uma vez que, foi o primeiro instituto a criminalizar os delitos

informáticos, trazendo assim mais segurança jurídica e maior rigor penal. Contudo, alguns aspectos negativos também sobrevieram, por exemplo, os termos normativos ambíguos, as penas brandas, a rápida sanção da lei e etc.

Por fim, diante de todas as retenções teóricas proporcionadas pelo estudo, conclui-se que a lei Carolina Dieckmann, precisa de uma reforma em seu conteúdo para extinguir, ou ao menos, minimizar as ambiguidades, além de que, é estritamente necessário a conjugação da lei com jurisprudências e legislações alienígenas, como tratados e convenções internacionais, afinal, a rede mundial de computadores possui dimensões globais e o estudo dessas legislações estrangeiras poderiam auxiliar na busca de um meio de adoção de novas medidas para a justa punição dos criminosos virtuais.

Com efeito, o presente trabalho não buscou esgotar o tema proposto, vez que, diante da complexidade deste não seria possível. Em verdade, tem mais a pretensão de promover uma reflexão do que dar uma resposta, realizando uma crítica aos critérios e fundamentos doutrinários com os quais se vem procurando equacionar a questão.

REFERÊNCIAS

AMÂNCIO, Tania Maria Cardoso. **O impacto da informática na sociedade e o direito no Brasil**. In: Revista Jurídica Consulex, v. 17, n. 405, p.24-28, dez./2013.

AMARAL, F. **Direito Civil**. Introdução. 7.ed. Rio de Janeiro: Renovar, 2008.

ANDRADE, Geraldo. **Direito à Privacidade: intimidade, vida privada e imagem.** Disponível em: < https://quentasol.jusbrasil.com.br/artigos/214374415/direito-a-privacidade-intimidade-vida-privada-e-imagem>. Acesso em 29 mar. 2017.

ASSIS, José Francisco De. **Direito à privacidade no uso da internet: omissão da legislação vigente e violação ao princípio fundamental da privacidade**. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=12848> Acesso em: 05 abr. 2017.

BARONI, Larissa Leiros. **Lei Brasileira Obriga Whatsapp a fornecer dados.** Disponível em: <https://tecnologia.uol.com.br/noticias/redacao/2016/03/02/lei-brasileira-obriga-whatsapp-a-fornecer-dados.htm>. Acesso em: 08 jun. 2017.

BITENCOURT, César Roberto. **Código Penal Comentado**. 8. ed. - São Paulo: Saraiva, 2014.

BRAZ, Ricardo Nery**. Internet, o consumo e a invasão de privacidade**. Disponível em: <http://infobrasil.inf.br/noticia/internet-o-consumo-e-invasao-de-privacidade>. Acesso em: 05 abr. 2017.

BULOS, Uadi Lammêgo. **Curso de Direito Constitucional**. 6 ed. rev. e atual. São Paulo: Saraiva, 2011.

_____. Constituição (1988). **Constituição da República Federativa do Brasil**: promulgada em 05 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>. Acesso em: 29 mar. 2017.

_____. Decreto-Lei nº 2.848, de 07 de dezembro de 1940. **Código Penal.** Brasília: 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 21 abr. 2017.

_____. Lei Federal nº 12.965, de 23 de abril de 2014. **Princípios, garantias, direitos e deveres para o uso da Internet no Brasil – Marco Civil da Internet.** Brasília: 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 28 abr. 2017.

_____. Lei Federal nº 8.069, de 13 de Julho de 1990. **Estatuto da Criança e do Adolescente**. Brasília: 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L8069Compilado.htm>. Acesso em: 05 abr. 2017.

_____. Lei Federal nº 12.737, de 30 de Novembro de 2012. **Tipificação Criminal dos Delitos Informáticos – Lei Carolina Dieckmann**. Brasília: 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 05 jun. 2017.

CAPEZ, Fernando; GARCIA, Maria Stela Prado. **Código penal comentado**. 4. ed. – São Paulo: Saraiva, 2013.

CAVALCANTE, Waldek Fachinelli. **Crimes cibernéticos: noções básicas de investigação e ameaças na internet**.

CERT. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha Para Segurança na INTERNET.** Disponível em: <https://cartilha.cert.br/mecanismos/>. Acesso em: 15 jun. 2017.

CIBERCRIMINALIDADE in Dicionário infopédia da Língua Portuguesa sem Acordo Ortográfico Porto: Porto Editora, 2003-2017. Disponível em: <https://www.infopedia.pt/dicionarios/lingua-portuguesa-aao/cibercriminalidade>. Acesso em: 09 jun. 2017.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet**. 2ª ed. rev. São Paulo: Saraiva, 2002.

DA SILVA, Camila Requião Fentanes. **Análise das Leis nº 12.735/2012 e 12.737/2012 e a (des)necessidade de uma legislação específica sobre crimes cibernéticos**. Disponível em: <https://jus.com.br/artigos/32265/analise-das-leis-n-12-735-2012-e-12-737-2012-e-a-des-necessidade-de-uma-legislacao-especifica-sobre-crimes-ciberneticos>. Acesso em: 15 jun. 2017.

DAOUN, Alexandre Jean apud ROSSETTO, Marcela. **Direito penal mínimo na web**. Visão jurídica. São Paulo: Escola, ano V, edição 62, Junho/2011.

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

FERRAZ JUNIOR, Tércio Sampaio. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado.** Disponível em: <http://www.revistas.usp.br/rfdusp/article/viewFile/67231/69841>. Acesso em: 03 abr. 2017.

GALVÃO, Fernando. **Direito Penal: Crimes contra a pessoa**. - São Paulo: Saraiva, 2013.

GOMES, Luiz Flávio. **V Congresso de Crimes Eletrônicos, realizado nos dias 12 e 13 de agosto pela Fecomercio SP**. Disponível em: <http://atualidadesdodireito.com.br/lfg/2013/08/14/jurista-luiz-flavio-gomes-fala-sobre-a-lei-carolina-dieckmann>. Acesso em: 19 abr. 2017.

GRECO, Rogério. **Código penal comentado.** 8.ed. rev., ampl. e atual. até 1º de janeiro 2014. Niterói, RJ: Impetus, 2014.

JC ONLINE**. Saiba como evitar os crimes virtuais.** Disponível em: <http://jconline.ne10.uol.com.br/canal/cidades/geral/noticia/2014/08/06/saiba-como-evitar-os-crimes-virtuais-138960.php>. Acesso em: 19 jun. 2017.

LIRA, Leide de Almeida. **Lei Carolina Dieckmann: (in) eficácia na proteção dos direitos fundamentais à intimidade e à vida privada em face da pena cominada aos delitos informáticos**. Conteúdo Jurídico, Brasília-DF: 01 jul. 2014. Disponível em: <http://www.conteudojuridico.com.br/?artigos&ver=1055.48868&seo=1>. Acesso em: 24 mar. 2017.

LOES, João; BLUM; Renato Opice; BISSOLI, Leandro. **Lei Carolina Dieckmann: Apenas o primeiro passo**. In: Revista Isto é, v.37, n. 2264, p. 62-64, 10 abr./2013.

MAGGIO, Vicente de Paula Rodrigues. **Novo crime: invasão de dispositivo informático - CP, Art. 154-A.** Disponível em: <https://vicentemaggio.jusbrasil.com.br/artigos/121942478/novo-crime-invasao-de-dispositivo-informatico-cp-art-154-a>. Acesso em: 14 jun. 2017.

MEDINA, Alessandra. **Ao alcance de todos**. In: Veja, ed. 2269, v. 45, n. 20, p.94-95, maio./2012.

MEIRA, Lais Moreschi; SOARES, Matheus Fernandes de Sousa; PIRES, Panmela Rodrigues. **Direito à privacidade e as relações na internet.** JurisWay, 2012. Disponível em: < https://www.jurisway.org.br/v2/dhall.asp?id_dh=7319 >. Acesso em: 29 mar. 2017.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. - 8.ed. rev.e atual.- São Paulo: Saraiva, 2013.

NOVELINO, Marcelo. **Direito Constitucional**. São Paulo: Método, 2008.

NUCCI, Guilherme de Souza. **Princípios constitucionais penais e processuais penais**. São Paulo: Ed. Revista dos Tribunais, 2010.

O GLOBO. GOULART, Gustavo. **Após identificação de hackers, Carolina Dieckmann afirma que espera justiça.** Disponível em: <https://oglobo.globo.com/rio/apos-identificacao-de-hackers-carolina-dieckmann-afirma-que-espera-justica-4889891>. Acesso em: 10 abr. 2017.

OLIVEIRA, Solange. **Como Denunciar Um Crime Virtual.** Disponível em: <http://ecommercegirl.com/dicas-e-commerce-girl/como-denunciar-um-crime-virtual/>. Acesso em: 10 jun. 2017.

OLIVEIRA, Vanilda. **Para entender a importância do Marco Civil da Internet.** Disponível em: <http://cut.org.br/noticias/para-entender-a-importancia-do-marco-civil-da-internet-826b/>. Acesso em: 07 abr. 2017.

PAESANI, Liliana Minardi. **Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil**. 6 ed. São Paulo: Atlas, 2013.

PIAUHYLINO, Luiz. **PROJETO DE LEI Nº 84 DE 1999.** Disponível em: <http://www.cedeca.org.br/conteudo/noticia/arquivo/39C06587-F3651D3CC1D1F2C5835.pdf>. Acesso em: 14 jun. 2017.

PINHEIRO, Patrícia Peck. **Direito digital global e seus princípios fundamentais**. In: Revista Jurídica Consulex, v. 14, n. 326, p. 46-47, ago/2010.

PORTAL EBC**. Entenda o Marco Civil da Internet ponto a ponto.** Disponível em: <http://www.ebc.com.br/tecnologia/2014/04/entenda-o-marco-civil-da-internet-ponto-a-ponto>. Acesso em: 04 abr. 2017.

QUEIROZ, Iranilda Ulisses Parente. **Proteção a intimidade e a vida privada a luz da Constituição Federal de 1988.** Disponível em: <http://www.direitonet.com.br/artigos/exibir/2662/Protecao-a-intimidade-e-a-vida-privada-a-luz-da-Constituicao-Federal-de-1988>. Acesso em: 29 mar. 2017.

RAMOS, Lívia Peruque. **Análise jurídica da Lei 12.737/12**. São Paulo: 2015. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/21580-69163-1-pb_0.pdf>. Acesso em: 25 mar. 2017.

REIS, Wanderlei José dos. **Delitos Cibernéticos: Implicações da Lei n.º 12.737/12**. In: Revista Jurídica Consulex, v. 17, n. 405, p.32-35, dez./2013.

ROCHA, Carolina Borges**. A evolução criminológica do Direito Penal: Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012**. Disponível em: <https://jus.com.br/artigos/25120/a-evolucao-criminologica-do-direito-penal-aspectos-gerais-sobre-os-crimes-ciberneticos-e-a-lei-12-737-2012>. Acesso em: 12 jun. 2017.

RODOTA', S. **Teledemocrazia e liberta individuali**. In: TELECOMI TALIA. Nápoles: Castel dell'Ovo. Sum.mit della comunicazione, 2000.

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

SANTINO, Renato. **WhatsApp explica por que não entrega os dados que a polícia brasileira pede.** Disponível em: <https://olhardigital.com.br/fique_seguro/noticia/whatsapp-explica-por-que-nao-entrega-os-dados-que-a-policia-brasileira-pede/55829>. Acesso em: 10 mai. 2017.

SILVA, Remy Gama. **Crimes da Informática.** Disponível em: <http://docplayer.com.br/983651-Crimes-da-informatica-remy-gama-silva.html>. Acesso em: 14 jun. 2017.

SOARES, Anderson. **Marco civil da internet e a garantia constitucional da privacidade e liberdade de expressão.** Disponível em: <https://jus.com.br/artigos/30520/marco-civil-da-internet-e-a-garantia-consticional-da-privacidade-e-liberdade-de-expressao>. Acesso em: 05 abr. 2017.

TOMASEVICIUS FILHO, Eduardo. **Marco civil da internet: uma lei sem conteúdo normativo?.** Disponível em: <https://jus.com.br/artigos/45471/marco-civil-da-internet-uma-lei-sem-conteudo-normativo>. Acesso em: 05 abr. 2017.

VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos**. Belo Horizonte: Ed. Fórum, 2013.

VIEIRA, Alexandre Pires; RALVES, Cláudio. **O direito à privacidade frente aos avanços tecnológicos na sociedade da informação.** Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 19, n. 3979, 24 maio 2014. Disponível em: <https://jus.com.br/artigos/27972>. Acesso em: 03 abr. 2017.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Porto Alegre: Sergio Antônio Fabris. Ed. 2007.

ZAPAROLI, Rodrigo Alves. **Comentários à Lei nº 12.737/12.** Disponível em: <http://www.direitonet.com.br/artigos/exibir/7936/Comentarios-a-Lei-no-12737-12>. Acesso em: 16 jun. 2017.