CENTRO UNIVERSITARIO METODISTA IZABELA HENDRIX
Coordenação do Curso de Direito

Waldinei Bernardo da Silva

UMA ANÁLISE DA LEI CAROLINA DIECKMNN E OS CRIMES CIBERNÉTICOS:

Ineficácia na proteção do Direito a intimidade e a privacidade na internet.

Belo Horizonte

2015

Waldinei Bernardo da Silva

UMA ANÁLISE DA LEI CAROLINA DIECKMANN E OS CRIMES CIBERNÉTICOS: Ineficácia na proteção do Direito a intimidade e a privacidade na internet.

Monografia apresentada ao Curso de Direito do Centro Universitário Instituto Metodista Izabela Hendrix, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Guilherme Vasconcelos.

Belo horizonte

2015

Waldinei Bernardo da Silva

UMA ANÁLISE DA LEI CAROLINA DIECKMANN E OS CRIMES CIBERNÉTICOS: Ineficácia na proteção do direito a intimidade e a privacidade na internet.

Monografia apresentada ao Curso de Direito do Centro Universitário Instituto Metodista Izabela Hendrix de Minas Gerais, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Guilherme Vasconcelos.

Guilherme Vasconcelos (orientador) Izabela Hendrix

Belo Horizonte

2015

Dedicatória

Dedico esse trabalho aos meus pais, pelo incentivo e carinho, a minha família pelo apoio incondicional, a minha esposa, aos amigos e professores que contribuíram de forma significativa para a construção desse conhecimento.

AGRADECIMENTO

A Deus, por ter me dado força para superar os obstáculos. A todos que contribuíram para a realização deste trabalho, fica expresso aqui a minha gratidão.

Ao meu Orientador, Prof. Guilherme Vasconcelos, pela orientação, pelo aprendizado e apoio.

Aos colegas de classe pela rica troca de experiências.

A todos que, de alguma forma, contribuíram para esta construção.

"poucos são os que têm privacidade para ficar tristes. Nesse mundo de vigília e patrulha constantes, é um luxo poder sofrer sem ter ninguém nos observando". (Crônica: O primeiro quarto – livro: Coisas da vida)

RESUMO

O presente trabalho aborda a lei Carolina Dieckmann e sua ineficácia na proteção de direitos fundamentais à intimidade, privacidade, honra e imagem. Referida lei recebeu este nome, devido à divulgação de 36 fotos intimas da atriz na rede, fato que impulsionou o legislador na aceleração e promulgação do projeto de lei que já existia, buscando resguardar esses direitos. Referida lei entrou no ordenamento jurídico brasileiro, com a missão de combater delitos informáticos, entretanto, devido a falhas no aspecto técnico do dispositivo legal, deixou a desejar. Este trabalho realizou um estudo com o objetivo de apontar as falhas e brechas da lei, através de um conjunto harmonioso de opiniões de grandes doutrinadores e juristas. Foi realizado um estudo do direito comparado, objetivando esclarecer que o direito a intimidade e privacidade são bens juridicamente reconhecidos em todo o mundo, seja através de constituição, bem como de instrumentos internacionais, dentre eles, a Declaração Universal dos Direitos Humanos de 1948, Declaração Americana dos Direitos e Deveres do homem, Convenção de Budapeste e o próprio direito brasileiro. Viu-se a necessidade de criação de uma agravante nos crimes praticados pela internet, visto que trata-se de um instrumento facilitador de condutas indesejadas, com inquestionável danosidade a coletividade.

Palavras – chave: Ciberespaço. Delitos Informáticos. Direito Fundamental. Instrumentos Internacionais. Vida privada e Intimidade.

ABSTRAT

His paper addresses the Carolina Dieckmann law and its inefficiency in fundamental rights protection intimacy, privacy, honor and image. the Law got its name because the disclosure of 36 intimate photos of the actress on thbe network, a fact that impuslsionou the legislature in acceleration and enactment of the bill that already existed, seeking to safeguard those rights. said law entered the Brazilian legal system, with the mission of combating computer crime, however, due to flaws in the technical aspect of the legal provision, left to be desired. This paper conducted a study in order to point out the flaws and loopholes of the law, through a harmonious set of reviews of great scholars and jurists. It conducted a study of comparative law, aiming to clarify that the right to intimacy and privacy are juridicamentes assets recognized worldwide, either through the constitution as well as international instruments, including the Universal Declaration of Human Rights 1948, the American Declaration Rights and Duties of Man, convention of Budapest and the own Brazilian law. We saw the need to create an aggravating factor in crimes committed over the Internet, since it is a facilitator of unwanted behaviors with unquestioned danosidade society.

Words - key: cyberspace. computer crimes. fundamental right. International instruments. Privacy and Intimacy.

SUMARIO

INTRODUÇÃO

O presente estudo versa sobre a lei 12.737/12 “Carolina Dieckmann” e sua ineficácia na proteção da intimidade e privacidade. A modernidade, juntamente com os benefícios tecnológicos, econômicos e sociais, propiciou uma série de novos riscos que incrementaram a maioria dos contatos sociais. A rede de computadores, por sua vez, revolucionou os meios de comunicação, e foi responsável pela integração mundial desses contatos, e como conseqüência, distribuiu os riscos decorrentes de seu uso para todo o universo.

A internet e a informática, apesar de serem ferramentas importantíssimas para o desenvolvimento econômico e social, viabilizaram um novo campo de exploração criminosa, onde crimes que já eram conhecidos passaram a ser praticados no espaço virtual, e ganhou um novo meio de execução, provocando o surgimento de novas condutas, e o questionamento sobre a relevância de bens jurídicos não tutelados pelo direito penal. O problema é pontecializado quando se percebe que, apesar da reprovabilidade social dessas condutas, a persecução penal vem sendo prejudicada em razão de uma insuficiência legislativa.

O tema desperta interesse, uma vez que tem sido pouco abordado pelos doutrinadores, mas também e em especial, pelas questões relativas aos efeitos de lesão a personalidade, decorrentes da violação da privacidade e da intimidade, que vem sendo provocadas cada vez em escala maior.

Com o advento da constituição Federal de 1988, tem-se reconhecido a relevância dos direitos denominados da personalidade, bem como a obrigação da reparação do dano ensejada por qualquer conduta que venha lesionar esses direitos. O código civil de 2002 também inovou nesse sentido, assegurando a responsabilidade civil, decorrente de ato ilícito, que viole o direito a intimidade a privacidade, a honra e a imagem.

Assim, a investigação da intimidade, da privacidade, honra e imagem como direito fundamental, é um primeiro ponto de partida, em que se busca a compreensão da morfologia desse direito, e a distinção entre intimidade e privacidade, que é tratada como sinônimo. Um elemento salutar neste sentido é a análise de instrumentos internacionais, voltados à proteção de direitos fundamentais, como a Declaração Universal dos Direitos de Direitos Humanos, a

Declaração Americana dos direitos e deveres do homem, a Convenção de Budapeste, e no plano do direito brasileiro.

O presente trabalho terá seu início marcado por uma abordagem desses direitos fundamentais, constitucionalmente tutelado pelo estado brasileiro, a evolução da sociedade e dos meios de comunicação e o surgimento da internet, e sua influencia e relacionamento com o direito. Em seguida serão analisados os bens jurídicos ameaçados ou lesionados pelos delitos informáticos, verificando a necessidade de uma regulamentação que assegure a eficácia desses direitos ou se a simples adaptação será suficiente.

Para uma melhor reflexão do tema, o trabalho foi dividido em 4 (quatro) capítulos. No primeiro, o objetivo proposto foi uma análise e reflexão dos direitos fundamentais a luz da Constituição Federal de 1988, como a intimidade, a privacidade, a honra e a imagem, violadas pela sociedade digital criminosa.

No segundo capítulo, foi abordado o direito a intimidade e a divulgação de informações na internet, vinculada a aspectos e sinais mais profundos do ser, da vivencia e dos sentimentos humanos, que é lançada sob risco diante a circulação de dados pessoais na Sociedade da informação, impulsionada sobremaneira pelas tecnologias de informática e telecomunicações, corriqueiramente aplicadas nos mais diversos segmentos da vida cotidiana. Foi abordado o caso “Carolina Dieckmann” que impulsionou a regulamentação de uma nova norma, qual seja, a invasão de dispositivo informático, mediante violação de mecanismo de segurança, bem como sua ineficácia na proteção da intimidade e da privacidade, devido a falha no aspecto técnico, apresentada no dispositivo de lei. Neste diapasão, serão explanados os crimes tipificados na lei 12.737/12, elucidados mediante um conjunto harmônico de idéias, opiniões e ensinamentos de doutrinadores do direito penal e digital.

O terceiro capitulo buscou analisar a ineficácia da referida norma, bem como a dissensão entre doutrinadores, quando ao termo “invadir” e “mecanismo de segurança” “obter”. Para uma melhor compreensão dos leitores, buscou-se analisar: a classificação doutrinária, bem juridicamente protegido, objeto material, sujeito ativo e passivo, bem como a consumação e a tentativa.

Fixadas as premissas sobre a proteção dos dados pessoais, o estudo ocupa-se de determinar se o tratamento concreto conferido a tais condutas não autorizadas, que se concretiza a parti da invasão de dispositivo informático, é ou não, efetivo como fator de desestímulo, assim

como avaliar se há ou não a necessidade de uma regulamentação legal que lide especificamente com a questão.

O quarto e ultimo capitulo dedicar-se-á a uma reflexão sobre a convenção de Budapeste e o possível ingresso no ordenamento jurídico brasileiro, bem como o tratamento dessas condutas na referida convenção, determinando entre outros pontos, o legitimado da conduta de divulgação indevida de informações e dados pela internet, o tipo de responsabilidade civil e penal dos administradores dos sites ou provedores de acesso nas quais essa divulgação ocorre. Abordou-se o Marco Civil da Internet no Brasil, sancionado em 23 de Abril de 2014 Pela Presidente Dilma Rousseff, cuja finalidade é estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Ao final, arremata-se com informações gerais sobre o tema, juntamente com as conclusões que se obtiveram durante as investigações para a elaboração deste trabalho.

1 BREVE CONSIDERAÇÕES DOS DIREITOS FUNDAMENTAIS À INTIMIDADE, A VIDA PRIVADA, A HONRA E A IMAGEM, TUTELADOS PELA CONSTITUIÇÃO FEDERAL DE 1988.

No ordenamento jurídico brasileiro, o direito a intimidade e a privacidade estão positivados na constituição federal, em seu art. 5, X, como sendo direito fundamental, objetivando promover a dignidade da pessoa humana.

Com o avanço da tecnologia, a intimidade e a privacidade passaram a ser seriamente comprometidas. A internet e a informática têm contribuído de forma expressiva para a violação desse direito, e tem tornado as pessoas escravas da tecnologia, no que concerne ao espaço virtual. Essa inovação tem permitido ataques à vida privada e a conseqüente violação de direito fundamental constitucionalmente tutelado pelo estado.

Não resta dúvida de que todos os seres humanos são titulares de direitos fundamentais.

Na lição de Mendes, (1998, p. 23) "a pessoa humana sente necessidade de preservar sua individualidade, afim de que se mantenham íntegros seus valores, podendo assim, cumprir os respectivos fins da sociedade".

Perez Luno, citado por Mendes (p. 25) conceitua direitos fundamentais:

> Conjunto de faculdades e instituições que, em cada momento histórico, caracterizavam as exigências da dignidade, da liberdade e da igualdade humanas as quais devem ser reconhecidas positivamente pelos ordenamentos jurídicos em nível nacional e internacional.[1]

Para Farias (2008, P.92) os direitos fundamentais, alem de complexos em sua estrutura interna, denotam uma pluralidade de tipos. De acordo com o autor, são inúmeras as tentativas de classificações destes, com a utilização de diversos critérios, "quanto a titularidade e aos sujeitos, quanto ao conteúdo ou ao objeto, quanto a estrutura, quando ao modo de proteção, quando a força jurídica e, em geral, quanto ao regime."

Nesse sentido Faria explica:

---

[1] MENDES, Gilmar Ferreira. Curso de Direito Constitucional. 8ª. Ed. Ver. Atual. – São Paulo: Saraiva 2013.

> Não obstante, um critério bastante difundido para a classificação dos direitos fundamentais é a teoria dos quatro status de Giorgio Jellinek. Esta teoria, "o exemplo mais grandioso de uma teorização analítica no âmbito dos direitos fundamentais, dotou a teoria dos direitos fundamentais de um suporte rigoroso ancorado no plano da estrita positividade, ao possibilitar o melhor conhecimento do conteúdo dos direitos fundamentais, bem como sua construção dogmática. Ademais, conforme anota Miranda (1991), a classificação de Jellinek corresponde aproximadamente ao processo histórico de afirmação da pessoa humana e seus direitos. [2]

O autor explica que, a segunda relação é estabelecida em função da afirmação constante do valor da pessoa humana, o que conduz a redução da extensão do status passivo e, com isso, a limitação do poder estatal pelos cidadãos.

A terceira relação resulta do fato de que a atividade estatal é realizada de acordo com o interesse dos cidadãos. E, para o cumprimento de suas tarefas, o estado reconhece o indivíduo à capacidade jurídica de pretender que o poder estatal seja adotado em seu interesse.

A quarta e ultima relação decorre da circunstancia da atividade estatal só tornar-se possível através da ação dos cidadãos. O estado reconhece ao indivíduo a capacidade de agir por conta do estado, promovendo-o a uma condição mais elevada, mais qualificada, a cidadania ativa.

1.1 A honra, a intimidade, a vida privada e a imagem como direitos da personalidade

Faria (2008, P. 118) conclui que esses direitos possuem duplo caráter:

> Alem de constituírem direitos fundamentais (com sua especial proteção pelo ordenamento jurídico) são ao mesmo tempo direitos da personalidade, isto é, essenciais a pessoa, inerentes a mesma e em principio extrapatrimoniais. Na verdade, os direito a honra, a intimidade, a vida privada e a imagem foram paulatinamente sendo perfilados primeiramente como direitos subjetivos da personalidade, com eficácia prevalente no âmbito inter privado para só mais tarde alcançar a estatura constitucional. Nessa ordem de idéias, cumpre mencionar a observação judiciosa realizada por Durig, de que os direitos da personalidade constituem o mais audaz e o melhor impulso do direito privado nos últimos anos[3].

A classe dos direitos da personalidade é composta por aqueles direitos que constituem o *minimum* necessário e imprescindível ao conteúdo da personalidade, sendo próprio da pessoa em si, como ente humano, existentes desde o seu nascimento.

---

[2] FARIAS, Edilson Pereira. Colisão de Direitos. 3ª Ed. Sergio Antonio Fabris Editor, 2009.
[3] FARIAS, Edilson Pereira. Colisão de Direitos, 3ª Edição. Sergio Antonio Fabris Editor, 2009.

1.2 Direito a intimidade

Antes de aprofundarmos no tema direito a intimidade, faz-se mister conceituar o que é a intimidade. As origens do vocábulo intimidade provem do latim *intimus e* significa em sentido restrito, íntimo, o mais profundo, estreito.

Mendes, (1999, p.42) conceitua:

> A intimidade é um sentimento que brota do mais profundo do ser humano, um sentimento essencialmente espiritual. È quase sempre considerado como sinônimo de privacidade, ou seja, uma terminologia de direito anglo americano (right of privacy), sendo a expressão direito a intimidade mais utilizada pelos povos latinos.[4]

O art. 5, X da CF/88 é enfático, ao abordar a intimidade como dignidade da pessoa humana, e como direito inviolável, senão vejamos:

> 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.

A intimidade, no dizer de Paulo José da Costa, "é um dos valores que merece pronta e urgente tutela do direito. O homem sente, por vezes, necessidade de se fechar na sua intimidade e de ser resguardar da curiosidade dos olhares e dos ouvidos ávidos".

Embora a jurisprudência e vários autores não distingam ordinariamente entre direito a privacidade e a intimidade, Gilmar Mendes define:

> O direito a 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 espalhem ao conhecimento publico. O objeto do direito a intimidade seriam as conversações e os episódios ainda mais íntimos, envolvendo relações familiares e amizades mais profundas. (MENDES, 2013)

Nesse diapasão Canotilho ensina:

> As informações que se encontram protegidas são aquelas de caráter "privado", "particular" ou "pessoal". É o mesmo que dizer, ainda que sob os riscos da tautologia, aquelas informações associadas às particulares do ser. Na caracterização da "informação pessoal" se deve ter em conta: o papel da vontade; a definição do que seja "obtenção de informação"; a compreensão do termo "uso de informação" e a natureza ampla de informação "pessoal" […] a opção religiosa ou a orientação sexual, por exemplo, são comumente vistas como aspectos da vida íntima. (CANOTILHO, 2013, p. 282)[5]

---

[4] MENDES, Gilmar Ferreira. Curso de Direito constitucional. 8ª Ed. Ver. E atual. – São Paulo: Saraiva 2013.
[5] CANOTILHO, J.J Gomes. Et al. Comentários a constituição do Brasil. – São Paulo: Saraiva 2013.

Não se pode olvidar que, guarda relação com a intimidade e vida privada, o principio da dignidade da pessoa humana, que é o cerne da intimidade e da vida privada, sem a qual não seria possível a tutela de nenhum outro direito. Insta ressaltar que, estão intimamente interligados à intimidade, princípios constitucionais, como a inviolabilidade da casa (art. 5º, XI), sigilo dos dados, da correspondência e das comunicações (art. 5º, XII), a inadmissibilidade no processo das provas obtidas por meios ilícitos (art. 5º, LVI) e o habeas data (art. 5º, LXXII).

Para Sampaio, (1998, P.364) o homem tem um direito a controlar impressões sensitivas advindas do exterior. Em suas linhas gerais, pode ser identificado como o clássico "direito a ser deixado em paz" ou, na versão de Bostwick como a liberdade de não ser perturbado ou excitado.

Corroborando com esse entendimento, o autor explica:

> Tranqüilidade, sossego, repouso são estados espirituais ou se quisermos psicofisiológicos, de homeostase com o ambiente próximo que se pretende garantir. Há, com efeito, outros domínios jurídicos envolvidos, direito a propriedade, direito a saúde, interesse publico, por exemplo, que não se dissolvem ou desmerecem o enforque de intimidade ora apresentado, mas, contrariamente, com ela, reforçam a proteção de um espaço de livre desenvolvimento da personalidade, conseguintemente, da realização de reflexões pessoais mais serenas, indispensáveis para a existência de uma sociedade livre.[6]

De acordo com o autor, nesse critério de relevância de interesses em jogo, muito influi o ambiente em que se encontra o indivíduo. No lar, por exemplo, há o reforço do principio da inviolabilidade da casa, a ponto de prevalecer à intimidade sobre outros princípios ocorrentes. Em um lugar publico, todavia, esse direito normalmente não apresenta suporte para se contrapor e prevalecer sobre tais liberdades.

1.3 Limites do direito a intimidade

Embora tutelado pela CF/88, o direito a intimidade não é absoluto, pois encontra limitações.

Sampaio (1998, P.379) colaciona:

[6] SAMPAIO, Jose Adércio Leite. Direito a intimidade e a vida privada. Del Rey, 1998.

> O direito a intimidade não é, na prática, absoluto, encontrando suas fronteiras em outros direitos ou bens constitucionais. Essa limitação deverá ter por fundamento uma disposição constitucional, enunciadora de outro direito ou bem protegido.[7]

O autor explica que a referida restrição se pode fazer diretamente, através de uma lei que incida sobre o âmbito da proteção do direito a intimidade, desde que haja autorização constitucional expressa nesse sentido. É o caso da reserva de lei restritiva da inviolabilidade as comunicações telefônicas, prevista no art. 5, XII, CF/88.

O autor alude que esse direito também pode sofrer limitação de forma indireta, que se concretiza a partir da conformação ou concretização de outro direito, competência ou bem constitucional. Exemplificando, pode haver a permissão legislativa de quebra do sigilo bancário, em nome da "segurança" (art.144 CF/88) e dá "moralidade publica" (art. 37 CF/88).

Em que pese limitações ao direito a intimidade, essa autorização deve encontrar respaldo jurídico, quais sejam, a lei precisa ser clara e precisa em suas disposições, deve haver adequação, necessidade e proporcionalidade da medida.

1.3.1 Limites ao direito da privacidade

Na lição de Mendes, a vida em comunidade impede que seja atribuído valor radical a privacidade. É possível descobrir interesses públicos, com respaldo a normas constitucionais, que estão em um plano superior aos interesses individuais. Segundo o autor, o interesse público despertado por certo acontecimento ou por determinada pessoa que vive de uma imagem cultivada perante a sociedade, pode sobrepujar a pretensão de "ser deixado só". A depender das circunstancias do caso concreto, a divulgação de informações sobre determinada pessoa pode ser admissível ou abusiva:

> Da mesma forma, há de se levar em consideração o modo como ocorreu o desvendamento do fato relatado ao publico. Diferem entre si os casos em que um aspecto da intimidade de alguém é livremente exposto pelo titular do direito daqueles outros em que a noticia foi obtida e propalada contra a vontade do seu protagonista. A extensão e a intensidade da proteção a vida privada dependem, em parte, do modo de viver do indivíduo, reduzindo-se, mas não se anulando, quando se trata de celebridade. Dependem ainda, da finalidade a ser alcançada com a exposição do modo como a noticia foi coletada.[8]

---

[7] SAMPAIO, Jose Adércio Leite. Direito a intimidade e a vida privada. Del Rey, 1998.
[8] MENDES, Gilmar Ferreira. Direitos e garantias individuais/Direito de personalidade/liberdade de expressão. Revista de informação legislativa: v.31, n. 122, p.297-301, abr./jun 1994.

Nesta esteira, Sampaio (1998, p. 379) aduz que os direitos fundamentais, na prática, não são nem ilimitados nem absolutos. E não o são por uma razão intrínseca: a multiplicidade de aspectos e projeções valorativas dos direitos humanos que pode levar a situação de aparente conflito, imprimindo a necessidade de opção.

Essa problemática, segundo o autor, levou ao desenvolvimento, ainda inconcluso, da teoria dos limites dos direitos fundamentais, cuja tormentosa tarefa tem como premissas e preocupações iniciais:

1. Que os direitos fundamentais não podem ser relegados a plano secundário, ensejando sua dependência ao beneplácito ou benevolência dos poderes públicos;

2. Que a sociedade, em razão de sua complexidade e interesses multidirecionais, exige a solução de possíveis (ou aparentes) conflitos entre os direitos fundamentais ou entre estes e valores sociais que se buscam alcançar.

Para Sampaio, a limitação ou restrição pode-se operar de varias formas. O primeiro tipo de limitação, não desafia maiores problemas. Estes surgem mesmo no trabalho de concretização – restrição de um direito fundamental, quando entra em conflito com outro direito fundamental ou bem constitucional. O autor anota como soluções alternativas aventadas:

1. Através do conceito de limites imanentes e da concepção de tatbestand reduzido, excluir-se-iam, a priori, certos modos de exercício do âmbito de proteção normativa;

2. Através da justificação da restrição, em que resulta, no fundo, a teoria relativa de núcleo essencial;

3. Mediante uma interpretação sistemática e unitária, ou

4. Usando um juízo de ponderação e de adequação dos princípios/bens/valores constitucionais, conduzindo a uma concordância prática com outros direitos ou bens colidentes. (SAMPAIO, 1998. P.381)

Para o autor, todas têm suas verdades e as suas incompletudes. Nenhuma tem a capacidade de oferecer soluções aprioristicas dos problemas, nem assegurar respostas unânimes.

1.4 Distinções entre intimidade e vida privada

Para muitos, intimidade e privacidade podem parecer sinônimas, entretanto existe uma distinção entre elas, tanto é verdade, que a CF/88 se encarregou de demonstrar essa distinção, quando afirma no art. 5º, X que, "são invioláveis, a intimidade, a vida priva, a honra e a imagem". Embora exista certa dificuldade para conceituar esses dois institutos, segundo Mendes, (1999 P.46) existe uma teoria bastante elucidativa, que é a teoria alemã, evocada por Costa Junior, senão vejamos:

> A vida particular ou privada poderia ser subdividida em outras esferas gradativamente menores, à proporção que a intimidade se fosse restringindo. Na esfera maior, a privada passa-se os acontecimentos que o indivíduo não quer que se tornem públicos. Fora dessa esfera situam-se as ocorrências e condutas de natureza pública, ao alcance da coletividade em geral, não cabendo, aí, os delitos de indiscrição. A esfera da intimidade, ou esfera confidencial, está contida na esfera privada, é um circulo fechado de que tomam parte somente pessoas muito íntimas. Por ultimo, mais no centro, encontra-se a esfera do segredo, que deve ser protegida de toda forma de indiscrição. Dessa esfera não participam sequer as pessoas da intimidade do sujeito: a necessidade de proteção contra a indiscrição é bem mais intensa.[9]

A autora explana que a sociedade tem especial interesse em penetrar e conhecer a vida intima das pessoas célebres, e com isso há uma limitação no direito a intimidade dessas pessoas, não podendo, no entanto, haver uma supressão total desse direito.

A propósito, observe-se a lição de Sampaio, 1998 (Apud Mendes,1999, p.48,):

> A intimidade é o âmbito do exclusivo que alguém reserva para si, sem nenhuma repercussão social, nem mesmo ao alcance de sua vida privada que, por mais isolada que seja, é sempre um viver entre os outros (na família, no trabalho, no lazer comum) não há um conceito absoluto de intimidade, embora se possa dizer que seu atributo básico que é o estar só, não exclui o segredo e autonomia.[10]

O autor faz distinção entre intimidade – diário intimo, segredo – e vida privada, pois esta envolve a proteção de forma exclusiva de convivência em que a comunicação entre os membros interessados é inevitável, mas podem excluir terceiros.

Sampaio esclarece que a vida privada pode envolver situações de opção pessoal, como a escolha do regime de bens no casamento, mas que, em alguns momentos, pode requerer a comunicação a terceiros. O autor explica que o direito a intimidade surge como uma das novas realidades do mundo contemporâneo, em que se observa a crescente interferência do poder publico na vida privada (tanto no exercício do poder de policia, quanto no campo da atividade

---

[9] MENDES, Maria Gilmaíse Oliveira de. Direito a intimidade e interceptação telefônicas. Livraria Mandamentos, 1999.

[10] SAMPAIO, Jose Adércio Leite. Direito a intimidade e a vida privada. Del Rey, 1998, apud MENDES, Maria Gilmaíse Oliveira de. Direito a intimidade e interceptações telefônicas. Livraria Mandamentos, 1998.

judiciária) bem como a maior possibilidade da intromissão de terceiros na esfera da intimidade para essa invasão com diversos artefatos, como teleobjetivas, minúsculos gravadores, aparelhos de interceptação telefônica e computadores.

1.5 direito a intimidade e a tutela constitucional em outros países.

O direito a intimidade e a vida privada tiveram proteção tutelada pela Declaração Americana dos Direitos e Deveres do homem de 1948, aprovada pela IX conferencia Internacional Americana, celebrada em Bogotá, cujo art. 5º dispõe que "toda pessoa tem direito a proteção da lei contra os ataques abusivos a sua vida privada e domiciliar". (MENDES, 1998, P.50)

Esse mesmo direito foi assegurado pela Declaração Universal dos Direitos do Homem, aprovada pela assembléia geral das Nações Unidas, como se vê:

> Art. 12: 1.ninguém será objeto de ingerências arbitrárias em sua vida privada, sua vida familiar, seu domicilio ou sua correspondência, nem de ataques a sua honra ou sua reputação.
>
> 2. Toda pessoa tem direito a proteção da lei contra tais ingerências e ataques.

Objetivando dar maior segurança jurídica, a convenção Européia de Direitos do Homem assinada em Roma, assegurando em seu art. 8º o mesmo entendimento da Declaração:

> Art. 8º 1. Qualquer pessoa tem direito ao respeito da sua vida privada, do seu domicílio e da sua correspondência.
>
> 3. Não pode haver ingerência da autoridade pública no exercício desse direito, senão quando esta ingerência estiver prevista na lei e constituir uma providencia que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem estar econômico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

No dizer de Mendes, o direito a intimidade tem se firmado, dia a dia, como forma de concretização da idéia de estado de direito.

O direito a intimidade e a vida privada ganharam forma constitucional, inicialmente, através da construção da jurisprudência constitucional de países como os Estados Unidos, e a Alemanha. (SAMPAIO, Apud MENDES, 1998, P. 54).

1.5.1 A Tutela constitucional da intimidade em outros países

Mendes menciona a previsão constitucional do direito a intimidade, destacando apenas os seguintes:

- Na Nicarágua, a constituição de 1986, publicada em 9/1/87, assegura, no art. 26.1 "o direito a sua vida privada e ao de sua família";
- A Republica do Suriname, na constituição promulgada em 3/10/87, expressa, no art. 17.1 "todos tem direito ao respeito de sua vida privada, de sua vida, de seu domicilio e de sua honra e boa reputação;
- Na Coréia, a Emenda de 1987 a Constituição de 1948 garante a privacidade dos cidadãos;
- A Iugoslávia, no art. 176 de sua Constituição de 21/2/74 estabeleceu, de forma genérica, o direito a intimidade, quando garante a inviolabilidade da integridade da pessoa humana, da vida privada e familiar e dos outros direitos da pessoa.

Desta feita, tem-se a idéia de quanto o direito a intimidade e a vida privada passou a ter um lugar de destaque nos textos constitucionais em plano internacional.

1.6 Direito a honra

Conforme o dicionário da língua portuguesa HOUAISS, (2009 p.1034) que define a honra como "principio que leva alguém a ter uma conduta proba, virtuosa, corajosa, e que lhe permite gozar de bom conceito junto à sociedade".

Na lição de Canotilho, honra pode ser definida como: "conceitua-se direito a honra aquele que tem toda pessoa de ser respeitada perante si mesmo e perante os outros".

Segundo o autor, existem duas faces no que se refere ao direito à honra, as quais são: subjetiva e objetiva. A honra subjetiva é a valoração que o ser humano faz de si mesmo, já a honra objetiva relaciona com o interesse que a pessoa tem de alcançar: prestígio, reputação e bom nome.

Nesse diapasão, Lira, expõe entendimentos jurisprudenciais de Alexandre de Moraes:

> **Liberdade de informação e divulgação e inviolabilidade da honra e a vida privada:** STJ – "Se, de um lado a constituição assegura a liberdade de informação,

> certo é que, de outros, há limitações, como se extrai do parágrafo 1º do art. 220, que determina seja observado o contido no inc. X do art. 5º, mostrando-se consentâneo o segredo de justiça disciplinando na lei processual com a inviolabilidade ali garantida" (STJ – 3ª T. – RMS Nº 3.292-2 PR – Rel. Min. Costa Leite – Ementário STJ, nº 12/254) (MORAES, 2007, P. 197).
>
> **Liberdade de divulgação e indenização por dano moral:** STJ – "É indenizável o dano moral decorrente de noticiário veiculado pela imprensa, considerado ofensivo a honra do autor (art. 49, inciso I, da lei nº5.250 de, 09/02/67)". (STJ – 4ª T. – Resp. nº287/RJ – Rel. Min. Barros Monteiro – Ementário STJ, Nº 4/160) **no mesmo sentido:** 3ª T. – Resp nº 15.672-0/PR – Rel. Min. Dias Trindade – Ementário STJ, Nº 1/153.) (MORAES, 2007, P.197)[11]

Por fim, a autora traz à baila a lição de Canotilho (2013) segundo a qual, existem dois sentidos que o direito a honra pode apresentar diante do caso concreto, sendo que no aspecto negativo, a intenção dirigida à sua depreciação, a sua desvalorização, que pode ser inexata, confundido-se certa medida, com a identidade, sendo mais que simples manipulação de um determinado dado pessoal; com relação ao aspecto positivo, pode dizer aos aspectos particulares, privados, confluindo com as águas da intimidade; por outro viés, pode também se referir a atividades públicas, as quais permitem maior liberdade de divulgação devido ao ofício.

1.7 Direito a imagem

Canotilho traz a composição da imagem e sua interface como direito fundamental:

> A imagem de uma pessoa se compõe de seu traço físico, de suas feições, de sua aparência *in natura* ou representada gráfica, plástica ou fotograficamente. Nesse sentido, poder-se-ia falar em um direito a uma certa aparência e representação; ou um controle do signo físico distintivo, em todas as suas etapas, inclusive de sua capacitação e reprodução. Sob esse ângulo, seria mera faculdade do direito a identidade pessoal. (CANOTILHO, 2013, P. 283)[12]

Segundo o autor, o direito à imagem pode ser classificado sob duas vertentes: como objeto de um direito e como instrumento de formação comunicativa. O direito a imagem será considerado como objeto de um direito, conforme a experiência jurídica, quando for associado

---

[11] LIRA, Leide Almeida de. Lei Carolina Dieckmann: (in) eficácia na proteção dos direitos fundamentais a intimidade e a 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: 31 out. 2015.

[12]CANOTILHO, J.J. Gomes. Et al. Comentários a constituição do Brasil. – São Paulo: Saraiva, 2013.

a componentes que se destacam na precisa definição dos poderes atribuídos a seus titulares. Sendo negativos: no que tange ao conhecimento alheio, impedindo a produção, reprodução, oposição a sua realização, bem como positivos quando consentir a atribuição de todos pontos negativos. Por outro viés será considerado como instrumento de formação comunicativa quando a imagem integrar o âmbito do direito a intimidade.

No tocante ao direito a imagem, Alexandre de Moraes expõe alguns entendimentos jurisprudenciais que assegura as pessoas públicas, a proteção do estado no que tange a imagem, senão vejamos:

> **Tutela a própria imagem: STF –** "Direito a proteção da própria imagem, diante da utilização de fotografia, em anuncio com fim lucrativo, sem a devida autorização da pessoa correspondente. Indenização pelo uso indevido da imagem. Tutela jurídica resultante do alcance do direito positivo". (STF – 2ª T. – Rextrnº90.328/SP – Rel. Min. Djaci Falcão, Diário da Justiça, seção I, 11 de Dez. 1981, p. 12.605). (MORAES, 2007, P.22).
>
> **Proteção a própria imagem e prescrição vintenária:** TJSP – " O direito sobre a própria imagem é direito pessoal protegido pelo art. 5º, XXVIII, a, da Constituição da República e prescreve em vinte anos, de conformidade com o art. 177 do Código Civil" (TJSP – 4ª Câmara Civil – Ag. Nº229.213-1/SP – Rel. Des. Cunha Cintra – JTJSP – Lex, 161.219). (MORAES, 2007, P. 222).[13]

Segundo Moraes (2007) o direito a imagem deve ser interpretado de maneira elástica, quando estiver relacionado a autoridades publicas, políticos, artista ou assemelhados, considerando a maior existência de exposição à mídia, bem como a própria natureza das funções exercidas, uma vez que os fatos que envolvem essas pessoas alem de dizer respeito ao interesse publico, também deve ser exposto ao conhecimento de todos. Por outro lado, nada obsta que essas pessoas busquem a tutela jurisdicional do estado, nos casos em que extrapolar a linha do respeito aos direitos fundamentais a honra a imagem e a vida privada.

1.8 Sociedade digital

[13] MORAES, Alexandre de. Constituição do Brasil interpretada e legislação constitucional. 7. Ed. Atualizada até a EC Nº55/07 – São Paulo: Atlas, 2007.

O avanço tecnológico na comunicação sempre perseguiu o objetivo de criar uma Aldeia Global, permitindo que todas as pessoas do mundo pudessem ter acesso a um fato de modo simultâneo.

Nessa toada Pinheiro (2013, p.63) explica:

> Este é o principio que orienta a criação de redes mundiais de telejornalismo, como a CNN, alem de toda uma rede Broadcast Digital para transmissões ao vivo e em tempo real, de qualquer lugar do mundo. O mundo financeiro também persegue essa mesma facilidade de comunicação, investindo grandes somas na modernização dos equipamentos para permitir a criação de uma comunidade financeira mais dinâmica. Os chamados programas de home-brokers já são uma realidade. Seguindo a necessidade de corte de gastos e controles maiores sobre as filiais, as empresas passam a investir em redes de comunicação rápida, economizando papel, pulsos telefônicos, viagens e tempo[14].

Segundo Pinheiro, este contato no trabalho passa a provocar uma necessidade de expandir tais benefícios para os lares. Assim começa o movimento para instalar um computador em cada casa. A convergência sai da esteira econômico-corporativa e passa a levar a tecnologia para dentro dos lares, interligando uma rede de consumidores ávidos por informação, serviços e produtos. Segundo a autora, essa convergência total possibilita novas economias para as empresas, principalmente de custos operacionais, logística, vendas e distribuição, alem de instituir um canal de venda personalizada, com maior eficiência para a aplicação do principio de estoque zero.

A autora alude sobre a complexidade de um mundo em que todos estão conectados em uma única aldeia e, ao mesmo tempo, tem a possibilidade de agir, como nunca antes na história da humanidade, como indivíduos.

Nesse diapasão a autora ilustra:

> Os mercados financeiros, como grandes precursores dessa era de convergência, foram os primeiros a sentir na pele as dificuldades desse universo. Se, por um lado, é muito bom estar conectado, por outro o comportamento irracional de mercado afeta a todos, onde quer que estejam de maneira nunca antes experimentada. A aludida complexidade é agravada pelo fator tempo, pela velocidade crescente com que os efeitos dessa rede de relações são sentidos em toda parte. Desde o inicio da era Mercantilista, os efeitos de uma crise local podiam ser sentidos em todo o mundo. Por exemplo, uma crise entre ingleses e chineses causada pelo comercio do chá no século XIX acarretava conseqüências na economia de todo o mundo, mas os efeitos dessa crise demoravam meses para chegar em todas as partes do planeta. Hoje, com a velocidade de transmissão de informações, tais efeitos são imediatos tanto em Londres como em São Paulo, no Cairo como em Sidney.[15]

---

[14] PINHEIRO, Patrícia Peck. Direito digital. 4ª edição. Saraiva, 2009. Vitalbook fille.
[15] PINHEIRO, Patrícia Peck. Direito digital 4ª edição. Saraiva, 2009. Vitalbook fille.

Esse exemplo macroeconômico serve como alerta sobre a complexidade de enfrentamos em todos os setores da sociedade.

Nessa linha de entendimento, a autora esclarece a necessidade que o ser humano sente da interatividade a nível global:

> A questão fica mais clara se refletirmos sobre um dos aspectos centrais da sociedade convergente: a interatividade, ou seja, a possibilidade de participação humana em um nível de inter-relação global. Vários avanços técnicos permitem que mais e mais pessoas atuem num mundo interativo: o movimento do software livre, de internet grátis, do MP3, entre outros. A interatividade exige que as empresas virtuais estejam preparadas para atender seus consumidores e qualquer tempo e em qualquer lugar. No mundo virtual e interativo, uma empresa sediada em Litlle Rock, Arkansas, vive com a possibilidade – e o risco – de interagir rapidamente com um consumidor, digamos, Mendonza, Argentina, numa realidade impecável há pouquíssimo tempo. Uma pessoa no interior de Goiás pode comprar e vender ações de uma empresa sediada na china com capital aberto na Bolsa de Nova York, EUA[16].

Paesani aponta que o avanço tecnológico atingiu as telecomunicações e, ainda no séc. XX, propiciou que a humanidade desenvolvesse, entre outras tecnologias, a invenção da televisão, a possibilidade de transmissões de imagens, sons e dados vias satélites, cabo físico, fibra ótica e, a mudança definitiva: o surgimento e disseminação em escala mundial da Internet.

Nesse diapasão, a autora explana:

> Cria-se no cidadão usuário da rede, um poderoso pólo ativo na produção e disseminação de informações e de conteúdos em escala planetária. Esses teores são relacionados aos mais diversos assuntos, desde a cultura, religião e lazer, até mesmo em relação a política, cidadania e relações globais, tal como a luta pela disseminação da democracia, educação ambiental e liberdade de disseminação de informações. Seus paradigmas são a internet de terceira geração (WWW3), as tecnologias móveis de dados (3G e 4G). (PAESANI, 2013, P.117)

Ter uma janela aberta para o mundo exige muito mais que apenas a seleção do público-alvo. Exige a criação de uma logística jurídica que reflita a diversidade cultural dos consumidores/clientes virtuais.

Pinheiro explana que, atualmente, a maior parte dos websites da Internet está localizada nos Estados Unidos, porem quem paga a maior parte da conta pelo uso dos backbones são outros países, e o Brasil é um dos que vivem mais intensamente o problema. Isso porque, segundo a autora, apesar de nossa febre pelo ciberespaço, a América Latina sofre carência de "peering points" e vários de SUS provedores ainda não fizeram a interconexão de suas redes. A auto-

[16] *Ibidem,* 2009, p.63-68.

estrada da informação está para a economia digital assim como a energia elétrica e as estradas estavam para a economia industrial.

Nessa linha de entendimento, a autora discorre que, se a internet for entendida como um lugar, então muitas questões do direito devem ser redesenhadas, uma vez que o território ou jurisdição deveria ser a própria internet. Se a internet é um meio, então necessário voltar a resolver a questão da territorialidade para aplicação da norma, já havendo como referencia a atuação do Direito Internacional.

Se a internet é um meio, como é o rádio, a televisão, o fax, o telefone, então não há que falar em Direito de Internet, mas sim em um único Direito Digital cujo grande desafio é estar preparado para o desconhecido, seja aplicando antigas ou novas normas, mas com a capacidade de interpretar a realidade social e adequar a solução ao caso concreto na mesma velocidade das mudanças da sociedade.

1.8.1 Direito digital

Para Pinheiro (2009, P. 61) o direito digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional, etc.)

A autora lembra-se da era do videocassete, que foi suplantado pela era digital. Atualmente existe a Internet Banking, DVD, MP3, HDTV – TV interativa, TV digital, Banda Larga, WAP, VoIP. A autora esclarece que essas siglas significam no mundo jurídico atual que, são os novos profissionais do Direito, os responsáveis por garantir o direito a privacidade, a proteção do direito autoral, do direito de imagem, da propriedade intelectual, dos royalties, da segurança da informação, dos acordos e parcerias estratégicas, dos processos contra Hackers e muito mais. Para isso, o direito digital deve ser entendido e estudado de modo a criar novos instrumentos capazes de atender a esses anseios.

Historicamente, todos os veículos de comunicação que compõem a sociedade convergente passaram a ter relevância jurídica a partir do momento em que se tornaram

instrumentos de comunicação de massa, pois a massificação do comportamento exige que a conduta passe a ser abordada pelo Direito, sob pena de criar insegurança no ordenamento jurídico e na sociedade. Pinheiro (2009, P. 73) explica:

> O que propomos aqui, portanto, não é a criação de uma infinidade de leis próprias – como vimos, tal legislação seria limitada no tempo (vigência) e no espaço (territorialidade), dois conceitos que ganham outra dimensão em uma sociedade convergente. A proposta é que o direito siga sua vocação de refletir as grandes mudanças culturais e comportamentais vividas pela sociedade. No direito digital prevalecem os princípios em relação às regras, pois o ritmo de evolução tecnológica será sempre mais veloz que o da atividade legislativa. Por isso a disciplina jurídica tende a auto-regulamentação, pela qual o conjunto de regras é criado pelos próprios participantes diretos do assunto em questão com soluções práticas que atendem ao dinamismo que as relações de direito digital exigem[17].

No direito digital deve haver a publicação das "normas digitais" no formato de disclaimers, como já fazem os provedores, ou seja, estar publicada na pagina inicial, a norma a qual se está submetido, senda ela um principio geral ou uma norma – padrão para determinada atuação. Desse modo, a publicidade das regras possibilita maior conhecimento do publico e conseqüentemente aumenta sua eficácia.

O direito digital não se limita a internet, sendo a própria evolução do Direito onde a Internet é um novo recurso que deve ser juridicamente atendido, como todas as outras inovações que estejam por vir. Nesse sentido a autora conclui:

> Em tal realidade, o maior compromisso dos operadores do direito é evitar qualquer ripo de arbitrariedade. Por isso, a discussão dos projetos de lei sobre temas que envolvem informática, Internet, e e-commerce, crimes virtuais deve ser feita com a sociedade civil, envolvendo empresas e organizações sociais, para não cometermos o erro de desmoralizar a lei, desacreditando o Direito. (PINHEIRO, 2009, P. 66).[18]

Segundo Pinheiro, não se pode achar que o Direito Digital é totalmente novo. Ao contrario, tem ele suas guaridas na maioria dos princípios do Direito atual alem de aproveitar a maior parte da legislação em vigor. A mudança, segundo a autora, está na postura de quem interpreta e faz sua aplicação. "é errado pensar que a tecnologia cria um grande buraco negro, no qual a sociedade fica a margem do Direito, uma vez que as leis em vigor são aplicáveis a matéria, desde que com sua devida interpretação".

---

[17] PINHEIRO, Patrícia Peck. Direito digital. 4ª edição. Saraiva, 2009. Vitalbook fille.
[18] PINHEIRO, op. cit., p.66.

2 DIREITO A INTIMIDADE E A DIVULGAÇÃO DE INFORMAÇÕES NA INTERNET.

A violência cometida via internet, tem tomado rumos imensuráveis, e muitos tem sido os danos por ela causados. Têm sido calorosas as discussões sobre os limites da liberdade de imprensa, a divulgação de informações, em relação aos direitos a intimidade, a vida privada, a imagem e a honra.

Com o advento da constituição de 1988, que consagrou em seu art. 5º, X, a inviolabilidade dos direitos fundamentais a intimidade, a vida privada, a honra e a imagem das pessoas, o constituinte deixa claro que, a proteção desses direitos não buscam apenas punir na esfera penal, aos que se aventuram a confrontar a norma maior. É o que se depreende da leitura da parte final do dispositivo, "assegurado o direito a indenização pelo dano material ou moral, decorrente de sua violação".

Nesse sentido, esclarecedora é a lição de Mendes:

> Se a constituição assegura, não só a inviolabilidade do direito, mas também a efetiva proteção judiciária contra lesão, ou ameaça de lesão a direito (CF, Art. 5º, XXXV), não poderia o judiciário intervir para obstar a configuração da ofensa definitiva, que acaba acarretando danos efetivamente irreparáveis? Que significaria a garantia da proteção judiciária efetiva contra lesão ou ameaça a lesão a direito se a intervenção somente pudesse se da após a configuração da lesão? Pouco, certamente muito pouco! (MENDES, 1994).[19]

Segundo o autor, a carta maior concebeu a liberdade de expressão como direito absoluto, não podendo ele sofrer limites, seja pelo poder judiciário, seja pelo legislativo. Ademais, o art. 220 da constituição é enfático ao dizer que, "a manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo, não sofrerão qualquer restrição, observado o disposto nessa constituição". Não obstante, o texto constitucional não excluiu a possibilidade de que se introduzissem limitações a liberdade de expressão e de comunicação, estabelecendo expressamente que essa liberdade se daria em conformidade com o disposto na constituição.

---

[19] MENDES, Gilmar Ferreira. Direitos e garantias individuais/Direito de personalidade/Liberdade de expressão. Revista de informação Legislativa: v. 31, n 122, p. 297-301, abr. / jul 1994.

O autor enfatiza que a liberdade de informação jornalística, é ainda mais expressiva, com relação a cláusula contida no art. 220, parágrafo 1º, senão vejamos: "nenhuma lei conterá dispositivo que possa constituir embaraço a plena liberdade de informação jornalístico em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV,V, X, XIII, XIV".

Nessa esteira o autor explica que o que parece ser negativo, na verdade é uma forma que o legislador encontrou para impor limites ao direito de liberdade de informação jornalística e da livre manifestação do pensamento:

> Como se vê, a formulação aparentemente negativa, contem, em verdade, uma autorização para o legislador disciplinar o exercício da liberdade de imprensa tendo em vista sobre tudo a proibição do anonimato, a outorga do direito de resposta e a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas. Do contrario não haveria razão para que se mencionassem expressamente esses princípios como limites para a liberdade de imprensa. (MENDES, 1994).

Para Mendes, existe uma reserva legal qualificadora, que impõe limites a liberdade de expressão, objetivando preservar outros direitos fundamentais e individuais não menos significativos, como a dignidade da pessoa humana.

Por outro lado o autor esclarece que existe um conflito entre a liberdade de informação e os direitos amparados pelo art. 5º, X, que tratam especificamente da proteção da vida privada e da intimidade:

> Como se vê, há uma inevitável tensão na relação entre a liberdade de expressão e de comunicação, de um lado, e os direitos da personalidade constitucionalmente protegidos, de outro, que pode gerar uma situação conflituosa, a chamada colisão de direitos fundamentais. (MENDES, 1994)

Deste modo, essa garantia à inviolabilidade da intimidade e da vida privada está diretamente ligada ao direito da dignidade da pessoa humana, sendo este o principio basilar constitucional, tendo o legislador assegurado tal princípio no art.1º, inciso III da Carta Magna.

Nas palavras de Santos (2014, p. 9-10), citado por Oliveira (2015) no que se refere à dignidade da pessoa humana, aduz que:

> Em que pese o criticismo quanto aos efeitos do positivismo na perspectiva democrática, ressalta-se uma manifesta realidade: o acolhimento do ser humano, como valor supremo dos ordenamentos jurídicos, é uma tendência. Daí a noção de que a Dignidade Humana seria, segundo alguns autores, o princípio valorativo máximo do Estado Democrático de Direito[20].

[20] SANTOS, 2008, apud OLIVEIRA, Claudio Roberto de Almeida. A extimidade da sociedade digital e a eficácia da lei 12.737/12 – invasão de dispositivo informático. Conteúdo jurídico, Brasília – DF: 30 abr. 2015.

Segundo o autor, a dignidade da pessoa humana não é uma criação constitucional mas é fruto de erros e acertos impingidos a humanidade num contexto de lutas pelos movimentos sociais marcados por momentos específicos da história.

2.1 O caso Carolina Dieckmann

Segundo reportagem de Guilherme Sardas, citada por Lira, em Maio de 2012 "36 fotos íntimas da atriz Carolina Dieckmann, em que a atriz aparece em cenas de nudez e poses sensuais, vazaram na internet" o computador pessoal da atriz foi invadido por dois Ckackers, um deles do estado de São Paulo e outro de Minas Gerais.

A reportagem cita que a atriz estava sendo chantageada a pagar o valor de 10.000,00 (dez mil reais) para não ter as imagens divulgadas na internet. Os criminosos efetuaram 03 ligações, bem como enviaram 05 emails, mostrando as fotos para o secretário da atriz, Alisson Oliveira, e seu empresário Alex Lerner.

A autora cita trecho extraído da reportagem de Guilherme Sardas, de como se deu a divulgação das imagens da atriz, diante da recusa do pagamento pedido pelos Ckackers:

> Os criminosos pediram 10.000,00 (dez mil reais) para não devassarem as curvas da atriz ao grande público, que ironicamente, figura na lista das musas ainda sonhada 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.**

A autora explana o entendimento de Marcelo Crespo, no qual explica em qual tipificação serão enquadrados os criminosos, na ação penal movida pela atriz, considerando a falta de legislação específica para a invasão de dispositivo informático:

> A ação judicial promovida por Carolina deparou-se, porem, com um **obstáculo jurídico**, o mesmo que vem atenuando a punição em casos semelhantes que ocorreram há mais de uma década no Brasil. "**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, difamação.** (LIRA, 2015)

Autora finaliza, argumentando que a partir de agora, quem invadir dispositivo informático, terá tratamento diferente, uma vez que o caso da atriz foi determinante e propulsor

para que uma nova lei especifica sobre crimes virtuais fosse promulgada, objetivando tutelar um novo direito: a intimidade na internet.

2.2 Lei dos crimes virtuais: análise da lei 12.737/12

Túlio Viana, (Apud, Lira 2014) explana que a lei 12.737 veio dispor sobre a tipificação criminal dos crimes cibernéticos e alterou o código penal brasileiro para incluir os artigos 154A e 154B, criando o tipo penal "invasão de dispositivo informático". A referida lei trouxe pequenas modificações nos artigos 266 e 298 do CP para tipificar a interrupção ou perturbação de serviço informático, telemático ou de informação de utilidade publica, bem como a falsificação de cartões de débito e crédito.

Trata-se de uma análise preliminar sobre a lei "Carolina Dieckmann" que acrescentou ao código penal, dois dispositivos legais que tipificam delitos informáticos.

Embora os arts. 154ª e 154B está inserido na seção referente aos crimes contra a inviolabilidade dos segredos profissionais, esses dispositivos são colocados como delitos e não como crimes.

Segundo (PESSINA 2006) Citada por Abimael Borges, existe uma diferença entre delitos e crimes:

> A diferença básica é que delito (*a deliquendo*) se refere às transgressões legais de natureza leve, essa definição vem desde a Idade Média, as escolas clássicas francesas admitiam a divisão tripartite em que crime é transgressão legal de natureza grave, delito é a transgressão legal de natureza leve e contravenção tem natureza levíssima.

Tem-se que, a edição de determinada lei, é criada para atender os anseios e necessidades da sociedade, necessitando para tanto que, o legislador perceba a necessidade da tutela de novos direitos, que outrora não eram importantes. Carolina Dieckmann foi apenas uma das inúmeras vítimas de invasão de dispositivo informático, mas que devido ao fato de ser pessoa publica, o caso ganhou maior visibilidade e foi fundamental para a aprovação da lei.

Desta feita, após inúmeras ocorrências de fatos que levaram a exposição de pessoas, expondo a intimidade, em evidente violação da intimidade e da vida privada, o legislador

infraconstitucional, editou a lei que trata de crimes cibernéticos e a invasão de dispositivo informático.

Vejamos o que diz a lei "*in verbis*"

> **"Invasão de dispositivo informático"**
>
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
>
> § 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa se a conduta não constitui crime mais grave.
>
> § 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
>
> § 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos;
>
> II - Presidente do Supremo Tribunal Federal;
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
>
> **"Ação penal**
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."
>
> Art. 3º. Os arts. 266 e 298 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal passam a vigorar com a seguinte redação:
>
> "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública
>
> Art. 266. .....

> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
>
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.” (NR)
>
> **“Falsificação de documento particular**
>
> Art. 298. .....
>
> **Falsificação de cartão**
>
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.” (NR)
>
> Art. 4o Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.
>
> Brasília, 30 de novembro de 2012; 191o da Independência e 124o da República.

A sociedade digital é assim reconhecida em virtude do rápido e ininterrupto desenvolvimento tecnológico-digital. Com a tecnologia da informação a sociedade tornou-se conectada, deste modo, seguramente, tudo de uma forma ou de outra, está conectado. Todavia, Os criminosos também se modernizaram, desenvolvendo um novo patamar criminal, o cybercrime, ou seja, os crimes informáticos.

2.3 Invasão de dispositivo informático

Oliveira (2015) esclarece que prática criminosa a dispositivos informáticos se dá através da utilização do computador bem como da internet, portanto se faz imprescindível conhecer os tipos de crimes informáticos tutelados por nosso ordenamento jurídico, pois ao praticá-los o autor não terá como se beneficiar da inocência legal, ou seja, afirmar não saber da existência de lei punitiva.

Para tanto, uma conduta só pode ser considerada crime se houver previsão legal que a tipifique, assim demonstrado no art. 5º, inciso XXXIX, da Constituição Federal de 1988 (CF/88) - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal.

Neste sentir, com o intuito de tipificar mais uma conduta, no dia 30 de novembro de 2012, a presidente Dilma Rousseff sancionou a Lei 12.737/12, que torna criminosa a prática de Invasão de Dispositivo Informático, apelidada pela mídia, vulgo “Lei Carolina Dieckmann”, que vigora desde o dia 02 de abril de 2013.

Sanches conceitua dispositivo informático como qualquer aparelho (notebook, netbook, tablet, smartphone etc.) capaz de armazenar e processar automaticamente informações e programas.

O autor explica que a objetividade jurídica, recai na tutela penal sobre a privacidade individual ou profissional, armazenada em dispositivo informático.

Quanto ao sujeito passivo e ativo, o autor explica que toda e qualquer pessoa pode ser autor e ou vítima do crime de invasão de dispositivo informático. Rogério Sanches ilustra esse entendimento, citando a lição de Andre Lopes Cavalcante:

> "Em regra, a vítima é o proprietário do dispositivo informático, seja em pessoa física ou jurídica. No entanto, é possível também identificar, em algumas situações, como sujeito passivo, o indivíduo que, mesmo sem ser o dono do computador, é a pessoa que efetivamente utiliza o dispositivo para armazenar seus dados ou informações que foram acessados indevidamente. É o caso por exemplo, de um computador utilizado por vários membros de uma casa ou no trabalho, onde cada um tem perfil e senha próprios. Outro exemplo é o da pessoa que mantém um contrato com uma empresa para armazenagem de dados de seus interesses em servidor para acesso por meio da internet (computação em nuvem, mais conhecida pelo nome em inglês, qual seja, cloudcomputing) (primeiros comentários a lei 12.737;12 que tipifica a invasão de dispositivo informático" disponível em www.dizerodireito.com.br, acesso em 21/12/2012. (CUNHA, P. 396)[21]

Nessa linha Greco (2014, p. 471) explica:

> Exige o art. 154-A que esse dispositivo informático seja alheio, isto é, não pertença ao agente que o utiliza. Assim, por exemplo, se alguém coloca informações em um computador de outra pessoa e esta acessa os dados ali inseridos, não se caracterizará o delito em estudo[22].

Greco explica que esse dispositivo informático pode estar conectado ou não a rede de computadores. Diz respeito às estruturas físicas e lógicas, que possibilitem que dois ou mais computadores compartilhem suas informações entre si.

Abimael Borges esclarece:

> O verbo desse artigo é "invadir" dispositivo informático alheio, trata-se da conduta do agente. É uma conduta tipicamente dolosa, pois a ação de invadir depende da vontade, da determinação consciente e livre do agente. A invasão é só o meio pelo qual o agente se serve para tirar proveito. Fica evidente que quando alguém possui a capacidade técnica para invadir um sistema de informática, ele quer o resultado (Art. 18, I, CP). Quem invade um sistema ou instala uma vulnerabilidade, sabe exatamente do resultado que quer obter. Invadir pressupõe a utilização de força, artimanha, violação indevido de mecanismo de segurança, desrespeito à vontade do proprietário do equipamento, ultrapassar o limite de autorização fornecida pelo titular do

[21] CAVALCANTE, apud, CUNHA, Rogério Sanches, p. 396.
[22] GRECO, Rogério. Código penal comentado. 9ª edição. Ver., ampl. E atual. Janeiro 2014. Niterói RJ: Impetus, 2014.

> equipamento. É o tipo comissivo, em que o agente realiza a conduta proibida. Imagine uma situação em que você encosta a porta de sua casa, quem chega, não deve ir entrando só porque você não passou a fechadura, a violação do lar se configura do mesmo jeito. Se a lei não for interpretada dessa forma, ela perde o sentido de existir. O fato de se colocar uma placa "APENAS PESSOA AUTORIZADA" ou "CONFIDENCIAL" já deve ser considerado como mecanismo de segurança. Não precisa colocar cadeado ou esconder num cofre para tipificar a invasão ou violação do sigilo. Se não houver nenhuma forma de resistência, a invasão não pode ser caracterizada. Perceba que o delito em tela é a invasão ou instalação de vulnerabilidade, o que se faz após ela não interessa, pois a invasão já consuma o delito. O resultado normativo da invasão poderá ser o de obter, adulterar ou destruir dados ou informações. Podem surgir resultados naturalísticos, aqueles que permeiam o mundo físico, como foi o caso da divulgação de fotos íntimas da atriz Carolina Dieckmann, pois feriu a honra, a dignidade, a liberdade pessoal da vítima, mas sua existência não é exigível na consumação do fato, mas o caráter formal do tipo independe do resultado, a consumação do delito se dá com a mera invasão, o resultado da invasão pode determinar a qualificação do tipo e o mero exaurimento da conduta delitiva.

Deste modo, nas palavras de Oliveira, a lei não inovou, tanto na condição para que ocorra o crime, quanto nas penas a serem aplicadas aos invasores, o legislador deveria ter associado uma pena que pudesse ser aplicada em caráter pedagógico, ou seja, as penas poderiam ser mais agressivas.

Neste sentir, muitas críticas em torno de sua eficácia surgiram, dentre elas pode-se destacar as palavras de Gomes (2013, apud Oliveira 2015), proferidas ao participar de um evento na cidade de São Paulo, em março de 2013, assim comentou:

> [...] tive a oportunidade de externar meu pessimismo em relação à eficácia penal da lei acima referida. A crença de que a lei penal possa ter efeito preventivo está cada vez mais discutida. [...]. O problemático é esperar que isso seja feito pela lei penal. Eu, particularmente, confio mais em medidas civis (determinadas por juiz civil, como remoção de uma notícia ofensiva), Confio mais em indenizações. (OLIVEIRA, 2015).[23]

Santos (2014) citado por Oliveira (2015) acrescentam:

> Quem conhece minimamente o funcionamento da justiça criminal no Brasil não pode se iludir: ela está, em geral, sucateada. Porque sucateada está a polícia civil (investigativa), que conta com incontáveis cadáveres nas suas portas, o que já é suficiente para sugar todos os seus recursos materiais e pessoais. Medidas civis urgentes são mais eficazes nessa área. [...]. Numa rápida olhada assinalei 104 conceitos dados pela lei, todos dependentes de interpretação. As penas são baixas (em regra, até dois anos), logo, a chance de prescrição é muito grande. Por todos esses motivos, não confio na eficácia preventiva dessa lei. A tutela civil teria condições de ser mais eficiente (GOMES, 2013)[24]

---

[23] GOMES, 2013, apud, OLIVEIRA Claudio Roberto Almeida de. A extimidade da sociedade digital e a eficácia da lei 12.737/12 – invasão de dispositivo informático. Conteúdo jurídico. Brasília – DF: 30 abr. 2015. Disponível em: HTTP://www.conteudo jurídico.com.br/artigos&ver=253339&seo=17.

[24] *Ibidem.*

O autor, ao externar seu pessimismo quanto a lei Carolina Dieckmann, demonstra também sua descrença na aplicabilidade da lei, uma vez que, via de regra a pena será de 02 anos, e existe uma grande probabilidade de ocorrer a prescrição, razão pela qual, Gomes acredita que será mais eficaz a busca na seara civil, confiando mais nas indenizações.

2.4 Avanços e criticas

Para o prof. Rony Vanzof, citado por Liliana Minard Paesani, a lei representa um considerável avanço, pois se introduziu a uma forma de tipificar a conduta lesiva. Entretanto, o autor pondera que as penas poderiam ser maiores, com o fito de desestimular os criminosos a prática de tal conduta, uma vez que, cabe ao juizado especial o tramite do processo. Nesse caso, se não existir condenação anterior ou se esse juizado não foi utilizado durante cinco anos, e a pena maior do crime não ultrapassar dois anos, o réu terá direito a substituir a pena cominada por prestação de serviço a comunidade e ao pagamento de cestas básicas (PAESANI, 2013).

Vanzof explica que a lei veio preencher algumas lacunas, como exemplo, a produção e distribuição de código malicioso e obtenção de conteúdo de comunicação eletrônica privada, bem como de sua divulgação.

Nesse sentir, Ranzof observa:

> O titulo em que estão previstos (esses delitos) é o de crimes contra a pessoa , ou seja, crimes contra a vida, contra a honra, lesão corporal. É um titulo que combate o perigo da violação da privacidade da pessoa e a inviolabilidade de seus segredos. Entretanto, a lei em discussão, deixa numerosas brechas para os criminosos. Entre elas a lei estabelece o crime de interrupção ou perturbação de serviços telemáticos nestes termos: “interrupção de serviço telemático ou de informação de utilidade publica”. A indagação necessária: porque a limitação a utilidade publica, e os demais casos de interrupção igualmente lesivos, mas não considerados de utilidade publica. (PAESANI, 2013, P.27).

O autor destaca que os ataques a organizações privadas não estão amparados pela legislação.

2.4.1 projeto de lei criminaliza divulgação de fotos intimas e vídeos na internet.

Em março de 2014, foi divulgado um artigo de autoria de Vitor Fraga, que traz noticias de casos de divulgação não autorizados de fotos e vídeos na internet, que comprometeram seriamente a intimidade e privacidade das vítimas, levando em alguns casos ao cometimento de suicídio, por não suportarem conviver com a humilhação a que foram submetidas. Vejamos o que diz a reportagem:

> No final do ano passado, o tema da divulgação não autorizada de vídeos e fotos íntimas via internet ganhou manchetes em todo o país por conta, principalmente, do caso de Francielly, uma vendedora de 19 anos, de Goiânia, que em outubro teve um vídeo, em que aparece nua, compartilhado na internet sem sua autorização. Embora seja vítima, Fran, como ficou conhecida, teve que abandonar o trabalho em uma loja e mudar toda a sua rotina. Em novembro, outros casos também foram noticiados em seqüência, como o da aluna da Faculdade de Letras da Universidade de São Paulo (USP) Thamiris, 21 anos, que também passou a viver de forma mais reclusa após ter uma foto nua divulgada na rede. Porém, dois exemplos acabaram dando um tom ainda mais trágico às denúncias: o de Júlia, 17 anos, em Parnaíba (PI) e de Giana, 16, de Veranópolis (RS), que cometeram suicídio após a divulgação dos vídeos em que foram expostas. Embora as vítimas nunca tivessem se conhecido e vivessem a quilômetros de distância umas das outras, o fato de as denúncias ocorrerem em um espaço de poucas semanas ajudou a fomentar o debate, que não é novo, sobre a criminalização da divulgação de fotos e vídeos íntimos nas redes**. Ainda em outubro de 2013, o deputado Romário (PSB/RJ) apresentou o Projeto de Lei (PL) 6.630/13, que altera o Código Penal tipificando "a conduta de divulgar fotos ou vídeos com cena de nudez ou ato sexual sem autorização da vítima"**. **Segundo ele, a iniciativa foi motivada por um anseio social. "Houve grande avanço tecnológico nos últimos dez anos e as pessoas mudaram a forma de se relacionar e de se comunicar, com a popularização de smartphone, redes sociais, aplicativos de celular. Novos tipos de crime surgiram e ouvíamos delegados dizendo em entrevistas como era difícil tipificá-los. Como legislador, me senti no dever de apresentar o projeto com penas mais duras para estas conduta.** (FRAGA, 2014).[25]

Segundo o autor, o presidente da comissão de segurança publica Breno Melarango, da OAB/RJ apóia o projeto, sobre a argumentação de que a divulgação de fotos intima e vídeos na internet, sem a devida autorização, não afetam somente a honra e a imagem, mas principalmente o direito a privacidade. Breno argumenta que essa conduta viola um dos aspectos mais íntimos e valorosos da pessoa, que é a sexualidade e a privacidade sexual. Termina enfatizando que essa é uma conduta que expõe as vítimas a conseqüências psicológicas e sociais devastadoras.

Além do projeto proposto por Romário, existem quatro propostas semelhantes que tramitam na câmara, todas apresentadas em 2013, sendo a principal a PL 5.555/13 que cria mecanismos para o combate a condutas ofensivas contra a mulher na Internet ou em outros meios de propagação da informação. Os outros projetos apensados são os PLs 5.822/13, que Inclui a violação da intimidade da mulher na internet entre as formas de violência doméstica e

[25] FRAGA, Vitor. PL Criminaliza divulgação de fotos íntimos e vídeos na internet, 2014. Disponível em: www.oabrj.org.br/materia-tribuna-do-advogado/18053-intimidade-que-fere.

familiar constantes na Lei Nº 11.340, de 7 de agosto de 2006, Lei Maria da Penha, PL 6.713/13 que Dispõe sobre punição a quem praticar a chamada vingança pornográfica e por derradeiro o projeto de lei 6.831/13, que dispõe sobre o crime de exposição pública da intimidade física ou sexual.

O ensaísta Vitor Fraga traz a baila o esclarecimento feito pelo deputado Romário, referente aos projetos em comento:

> No início de 2014, Romário apresentou requerimento para desapensação de sua proposta. "Quando um projeto é apensado, a análise dele pode ficar prejudicada, perdendo, talvez, algum artigo que julgo importante. Por exemplo, o PL 6.630/13, de minha autoria, não discrimina gênero. As punições são para homens e mulheres que divulgarem o material íntimo, enquanto o do deputado João Arruda altera a Lei Maria da Penha, que se aplica unicamente às mulheres", explica Romário. Enquanto o PL 5.555/13 amplia a quantidade de delitos abrangidos pela Lei Maria da Penha (a violação da intimidade, pela internet ou qualquer outro meio, sem consentimento, passa a ser considerada violência doméstica e familiar contra a mulher), o PL 6.630/13 acrescenta um artigo ao Código Penal, considerando crime a conduta de divulgar fotos ou vídeos com cena de nudez ou ato sexual sem autorização da vítima. Na opinião de Melarango, a desapensação poderia facilitar a tramitação, mas é preciso evitar desproporcionalidades no conjunto de leis penais. "Se um mesmo tema tem o condão de modificar diversos conjuntos de normas jurídicas e há vários projetos direcionados a modificar cada um deles, é mais seguro que tramitem juntos para evitar situações jurídicas penais desequilibradas e irracionais". (FRAGA, 2014)

2.5 Pornografia de revanche

De acordo com Fraga, as denuncias apontam que as mulheres são, maioria absoluta dos casos, as principais vítimas de *reveng porn* "pornografia de revanche" nome dado as publicações sem autorização de imagens e vídeos íntimos na internet. O autor menciona o caso de uma estudante da universidade de são Paulo que teve sua imagem divulgada na internet, na qual aparecia com os seios nus:

> Em novembro de 2013, a estudante de Letras da USP Thamiris também foi vítima da divulgação de uma foto sua com os seios nus, sem autorização. Ela acusou o ex-namorado, o búlgaro e estudante da mesma faculdade Kristian Krastanov - quase um mês antes, ela o havia denunciado à polícia por ameaças de morte via redes sociais. O acusado publicou nota em sua página no Facebook negando ser responsável pelo vazamento das imagens e admitindo que fez as ameaças, mas "jamais cogitou concretizá-las". A universitária afirmou na época, em entrevista ao site G1, que a humilhação foi tão grande que pensou em mudar de cidade e até mesmo em cometer suicídio. Mas decidiu enfrentar a situação, e publicou um texto no Facebook sob o título Meu desabafo como vítima de "revengeporn", que teve cerca de 3 mil compartilhamentos. Thamiris foi criticada pela família do ex-namorado, mas obteve apoio entre colegas e professores da faculdade.

O autor aponta que, logo após o caso de Thamires, aconteceram dois casos mais graves que levaram as vítimas a cometerem suicídio:

> No mesmo mês, com uma diferença de quatro dias, aconteceram os casos com as conseqüências mais graves. No dia 10, Júlia, de 17 anos, se enforcou depois de receber pelo celular um vídeo no qual ela aparecia fazendo sexo com uma amiga e um rapaz, todos menores de idade, na cidade de Parnaíba, no litoral do Piauí. No dia 14, na cidade de Veranópolis, a estudante Giana foi avisada por uma colega de escola que circulava na internet uma foto em que ela aparecia nua. Três horas depois, a adolescente foi encontrada morta em seu quarto pelo irmão - segundo a polícia, ela também se enforcou. Em ambos os casos, os familiares só souberam dos vídeos após as mortes. E também nos dois casos, as adolescentes publicaram mensagens de despedida no Twiter. "Hoje à tarde eu dou um jeito nisso. Não vou ser mais estorvo para ninguém", escreveu Giana no dia de sua morte. "Eu te amo, desculpa não ser a filha perfeita, mas eu tentei", escreveu Júlia à mãe, também antes de se enforcar.
>
> No caso de Júlia, a Polícia Civil do Piauí informou que vai acionar a Polícia Federal para investigar a venda do vídeo íntimo, que estaria disponível por R$ 4,90 em um site internacional, que prometia o envio do link para o e-mail do comprador sem identificação na fatura do cartão de crédito. O mesmo site também teria disponibilizado o vídeo de Fran. (FRAGA, 2014).

O autor lembra que, devido às tecnologias, e o fácil acesso a internet por meio de redes sociais e aplicativos para trocas de mensagens para celular, ficou fácil o compartilhamento de todo tipo de conteúdo, e basta apenas um clique para repassá-los a todos os contatos, e dessa maneira expor as pessoas causando danos imensuráveis.

O deputado Romário esclarece que esse projeto de lei, é diferente da lei Carolina Dieckmann, uma vez que esta criminaliza a invasão de dispositivo informático para obter vantagem ilícita, o PL 6.6630/13 não trata de roubo, mas sim da divulgação de imagens intimas vídeos na internet sem autorização.

3 **INEFICACIA NA PROTEÇÃO A INTIMIDADE NA LEI 12.737/12**

3.1 **Pontos negativos**

Segundo Loes (2013), a promulgação da lei, criada para regular os crimes digitais no Brasil, foi apenas o primeiro passo, pois as lacunas no texto e a infraestrutura deficitária da policia podem atrapalhar, tendo em vista o lapso de tempo para prescrição dos crimes. O autor elucida que a lei dependera de jurisprudência para funcionar.

Muitos operadores do direito têm questionado a brandura das penas cominadas aos delitos informáticos ora consubstanciados na lei Carolina Dieckmann. Misael Bispo Neto (2013) atesta que sem o mínimo de força dissuasória não previne a ocorrência e a recorrência de condutas criminosas, pelo contrario, ao invés de coibir, pode estimular a pratica criminosa.

Greco (2014, P.608) alude que a lei 12.737/12, inserindo o art. 154-A ao código penal, exigiu a presença dos seguintes elementos, para efeitos de caracterização do delito de invasão de dispositivo informático, a saber: a) o núcleo invadir, b) dispositivo informático alheio, c) conectado ou não a 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.

Para Rogério Greco, o núcleo invadir tem o sentido de violar, penetrar, acessar.

Informática na definição de Pablo Guillermo e Alejandro Andrés Konhen, citado por Greco (2014) é:

> A ciência aplicada que trata do estudo e aplicação do processamento automático da informação, mediante a utilização de elementos eletrônicos e sistemas de computação. O termo informatique é um acrônimo das palavras francesas information e automatique, o qual foi utilizada pelo engenheiro Frances Philipe Dreyfus no ano de 1962 para sua empresa Societé d'Informatique Appliquée.
>
> Posteriormente, esse termo começou a ser utilizado pelas diferentes línguas quando se desejava contemplar a questão do processamento automático da informação, sendo assim que ao ingressar no mundo castelhano, se conceitualizou a palavra informática. Para que se possa considerar um sistema informático se deve verificar, necessariamente, a realização das seguintes tarefas básicas: entrada: aquisição de dados. Processo: tratamento dos dados. Saída: transmissão dos resultados. (GRECO, 2014, P.608)[26]

[26] GRECO, Rogério. Código Penal comentado. 9ª.edição. Revista, ampliada e atualizada até janeiro de 2015. Impetus. Niterói: RJ 2015.

De acordo com a conceituação e requisitos acima apontados, o dispositivo informático seria todo aparelho capaz de receber os dados, tratá-los, e transmitir os resultados, a exemplo do que ocorre com os computadores, smartphone, tablet, etc.

O autor explica que o art.154-A exige que esse dispositivo informático seja alheio, isto é, não pertença ao agente que o utiliza. Assim, por exemplo, se alguém coloca informações em um computador de outra pessoa e se esta última acessa os dados ali inseridos, não se caracterizará o delito em estudo.

Dessa forma, presente os demais elementos exigidos pelo tipo, poderá ocorrer a infração penal em estudo com a invasão de um dispositivo informático, alheio, como ocorre com um computador, que pode não está ligado a qualquer rede e ser acessado via internet. Assim, se alguém percebendo que seu vizinho esqueceu o computador que havia levado para a festa em que ambos participavam invadir o equipamento, mediante violação de mecanismo de segurança, com a finalidade de destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, poderá ser responsabilizado pelo tipo penal previsto pelo caput do art. 154-A do código penal. O autor explica que, para que ocorra a infração penal sub exame, o tipo penal exige que a conduta seja levada a efeito mediante violação indevida de mecanismo de segurança. Por mecanismo de segurança, entendem-se todos os meios que visem garantir que somente determinadas pessoas terão acesso ao dispositivo informático, a exemplo do que ocorre com a utilização de login e senhas que visem identificar a autenticar o usuário, impedindo que terceiros não autorizados tenha acesso as informações nele contida.

Logo entende-se que essa exigência, isto é, a violação indevida de mecanismo de segurança, impede que alguém seja punido pelo tipo penal previsto no art. 154-A do diploma repressivo, quando, também, mesmo indevidamente, ingresse em dispositivo informático alheio sem que, para tanto, viole mecanismo de segurança, pois inexistente.

Nesse sentido, o autor explica que não raras vezes, pessoas evitam colocar senhas de acesso, por exemplo, em seus computadores, permitindo assim, que qualquer pessoa que a eles tenha acesso, possa conhecer o seu conteúdo. Entretanto, mesmo sem a existência de senha de acesso, a ninguém é dado invadir computador alheio, a não ser que ocorra a permissão expressa ou tácita de seu proprietário. No entanto para fins de configuração típica, tendo em vista a exigência contida no dispositivo legal em análise, somente haverá a infração penal se houver, por parte do agente invasor uma violação indevida do mecanismo de segurança.

Segundo o autor, aquele que tem conhecimento e habilidades suficientes para violar mecanismos de segurança, invadindo dispositivo informático alheio, é chamado de hacker, conforme lição de Sandro D'amara Nogueira, citado por Greco:

> Este indivíduo, em geral, domina a informática, é muito inteligente, adora invadir sites, mas, na maioria das vezes, não com a finalidade de cometer crimes, costumam se desafiar entre si, para ver quem consegue invadir tal sistema ou página na internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual.[27]

Por outro lado, também existe a figura do cracker que, ainda de acordo com os ensinamentos de Sandro D'amaro, é aquele que:

> Usa a internet para cometer crimes, fraudes bancárias e eletrônicas, furto de dados, golpes e grandes estragos. São verdadeiras quadrilhas de jovens que não se contentam apenas em invadir um sistema, usam sua inteligência e domínio da informática para causar prejuízos de milhares de reais, tanto contra pessoas físicas, como jurídicas, órgãos públicos etc.

Na lição do autor, a conduta do agente, ou seja, o ato de invadir dispositivo informático alheio, conectado ou não a rede de computadores, mediante violação indevida de mecanismo de segurança, deve ter sido levado a efeito com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo.

Sendo assim, não é a simples invasão, pela invasão, mediante violação indevida de mecanismo de segurança, que importa na prática da infração penal tipificada no caput do art.154-A do diploma repressivo, mas sim, aquela que possui uma finalidade especial, ou seja, aquilo que denominamos de especial fim de agir, que consiste na obtenção, adulteração ou destruição de dados ou informações sem a autorização expressa ou tácita do titular do dispositivo. Greco explica que, obter tem o significado de adquirir, alcançar o que desejava conseguir; destruir quer dizer aniquilar, fazer desaparecer, arruinar.

Nesta toada, Haikal citado por oliveira, comenta:

> Uma das vulnerabilidades da "Lei Carolina Dieckmann" é condicionar o crime a uma eventual obtenção ou instrução ou modificação de dados. Nesse contexto, existem formas de obter dados sem a criminalização, já que o invasor pode espionar dados sem ser punido. "A menos que o espião divulgue uma informação para terceiros, considerada sigilosa, ele será punido". (OLIVEIRA, 2015)[28]

---

[27] NOGUEIRA, apud, GRECO, 2015, P. 608-610.

[28] OLIVEIRA, Claudio Roberto de Almeida. A extimidade da sociedade digital e a eficácia da lei 12.737/12 – invasão de dispositivo informático. Conteúdo Jurídico, Brasília – DF: 30 abr. 2015. Disponível em: <HTTP://www.conteudojuridico.com.br/2artigos & ver + 253339 e seo = 1>

De acordo com o art. 154-A a conduta de invadir dispositivo informático alheio, conectado ou não a rede de computadores, mediante violação indevida de mecanismo de segurança, pode ainda, alem da finalidade de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ser dirigida no sentido de instalar vulnerabilidades para obter vantagem ilícita.

Segundo o centro de estudos, respostas e tratamentos de incidentes de segurança no Brasil, citado por Greco (2014, P.611):

> Uma vulnerabilidade é definida como uma condição que , quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede. Um ataque de exploração de vulnerabilidade ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.

De acordo com o centro de estudos, resposta, e tratamento de incidentes de segurança no Brasil, pode o agente instalar vulnerabilidades através dos chamados códigos maliciosos:

> Código malicioso (malwares) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são:
>
> - Pela exploração de vulnerabilidades existentes nos programas instalados;
> - Pela auto-execução de mídias removíveis infectadas, como pen- drives;
> - Pelo acesso a páginas web maliciosas, utilizando navegadores vulneráveis;
> - Pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
> - Pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em paginas web ou diretamente de outros computadores (através de compartilhamento de recurso)
>
> Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador de podem executarem ações em nome dos usuários, de acordo com as permissões de cada usuário. Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Alem disso, os códigos maliciosos são, muitas vezes, usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de spam.

Rogério Greco explica quais são os principais tipos de códigos maliciosos: a) vírus – programa malicioso que possui, basicamente, dois objetivos: atacar e replicar automaticamente.

O vírus depende da execução dos arquivos hospedeiros para que possa se tornar ativo e continuar o processo de infecção; b) worm – writer once read many- tem como característica fundamental replicar mensagens sem o consentimento do usuário, disseminando propagandas, arquivos maliciosos ou congestionando a rede. Sua propagação se dá através da exploração de vulnerabilidades existentes, ou falhas na configuração do software instalada em computadores; trojam horse (cavalo de tróia) – literalmente, é um presente de grego, pois é um programa que se passa por um presente, a exemplo do que ocorre com álbuns de fotos, jogos, cartões virtuais, algum aplicativo útil etc., mas, no entanto abre portas remotas para invasão dos hackers; spyware – são programas espiões, a exemplo do keylogger, que captura a armazena as teclas digitadas pelo usuário no teclado, ou ainda, o screenlogger, capaz de capturar telas da área de trabalho do usuário, inclusive armazenando a posição do cursor; boot – que é um programa que dispõe de mecanismo de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores; boot net – é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos boots et.

São inúmeros os códigos maliciosos através dos quais pode ser praticado o delito de invasão de dispositivo informático.

3.1.1 Divergência entre juristas e doutrinadores quanto ao termo invasão mediante violação indevida de mecanismo de segurança.

Flavia Penido, advogada e professora de direito digital, citada por Lira, relata a discussão de alguns juristas a cerca do art. 154-A do diploma legal, o qual preconiza:

> Invadir dispositivo informático alheio, conectado ou não a 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 vulnerabilidade para obter vantagem ilícita. (LIRA, 2014)

Para a autora o texto é claro, mas existem polêmicas instauradas. Alguns juristas entendem que o verbo invasão, requer medida violenta para que se configure o crime; outros questionam a necessidade de mecanismo de segurança. Segundo alguns especialistas, em não

havendo senha, tela de bloqueio ou anti vírus não há ocorrência do crime previsto no art. 154-A.

Auriney Brito (2013, P.69) ressalta a importância de se observar cada elementar do crime para que se tenha total noção dos limites da imputação penal. No caso o verbo núcleo do tipo 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 ele seja.

O autor ressalta que se o dispositivo estiver completamente desprotegido, não há que se falar em punição pelo crime de invasão, uma vez que não está presente a violação indevida de mecanismo de segurança.

Haikal, apud Oliveira, pondera:

> Se o computador estiver ligado e os dados estiverem expostos, não necessariamente haverá uma tipificação de crime. No caso do computador estar desprotegido pode não ser considerado crime [...]. Para a invasão ser considerada crime, é preciso transpor um mecanismo de segurança como a senha. [...] se trata de uma "aplicação míope do tipo penal, que irá atingir quem estiver despreparado". A redação da lei não especifica punição para a disseminação de vírus, mas para ataque de serviço DDS (como os ataques do Grupo Anonymus) aplicável somente para o serviço público, e não para o setor privado. (OLIVEIRA 2015)[29]

No dizer de Wanderley Jose dos Reis (2013, P.34), a redação do caput do dispositivo foi duramente criticada no seio doutrinário tendo em vista que o verbo nuclear do art. 154-A, qual seja, invadir, exprime, consoante definição do dicionário Aurélio: "Entrar a força, apoderar-se violentamente e a julgar pela redação do novel artigo, somente se configuraria o crime se o agente acessasse o sistema de informática a força*"(*REIS, 2013).*[30]*

O autor explica que só há duas formas de se ter acesso ao banco de dados de forma indevida: "quando o agente acessa fisicamente o dispositivo, ou quando o usuário de forma inadvertida, permite que seja instalado em seu computador os chamados malwares, que aparecem na forma de arquivos enviados por e-mail, links na internet ou em dispositivos móveis como pen-drive"

---

[29] HAIKAL, apud, OLIVEIRA, Claudio Roberto de Almeida. A extimidade da sociedade digital e a eficácia da lei 12.737/12 – invasão de dispositivo informático. Conteúdo jurídico, Brasília – DF: 30 abr. 2015

[30] REIS, Vanderley Jose dos. Delitos cibernéticos: implicação da lei 12.737/12. In Revista jurídica Consulex v. 17, n 405, p.32-35, dez 2013.

Segundo o autor, o legislador pecou no aspecto técnico do art. 154-A, sendo que ao invés do termo "invadir" correto seria usar o termo "acessar" uma vez que não haveria necessidade do autor operar com violência, mas tão somente por meios ardil para a obtenção dos dados.

Na lição de Auriney Brito, (2013) o legislador deixou claro que é imprescindível que haja uma lesão ou ameaça concreta a bem jurídico tutelado, para que se atenda ao principio da lesividade, pois só a ação do agente não é suficiente para configurar o crime.

3.1.2 A **mera "espiadinha" não configura crime.**

Para o especialista em crimes de internet Renato Opice Blum (2012, Apud Lira 2014)), existe uma brecha também na parte final do art. 154-A, pois não prevê punição para quem invade um computador alheio e não rouba nada, o faz apenas por curiosidade, ou não o faz por circunstancias alheia a sua vontade.

Desta maneira, Flavio Penido Expõe a parte final do mencionado art. e aponta dúvidas entre os especialistas no que se refere a mera "espiadinha", se não vejamos: "com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, ou instalar vulnerabilidade para obter vantagem ilícita"

Analisando o verbo "obter" gera dúvida em alguns especialistas quanto a configuração do crime de obtenção de dados, uma vez que é possível, entrar e sair do dispositivo com o fim apenas de "espiar".

França (2013, P.4) traz uma possibilidade de invasão de computadores com o mero fito de descobrir vulnerabilidades, sendo exercida por um profissional, razão pela qual não se configura crime:

> É o que fazem os Hackers, que se distinguem dos Crakers por não intentarem causar qualquer dano ao proprietário das informações violadas. Aqueles indivíduos, em virtude da expertise que demonstram, são, inclusive, contratados por grandes empresas que se valem do seu trabalho para corrigir as falhas dos seus sistemas.[31]

[31] FRANÇA, Misael Neto Bispo da. Crimes informáticos e lei "Carolina Dieckmann". Mais do mesmo. Direito penal contemporâneo. In Revista Consulex, v. 27, n 39, p.3-5, set 2013.

O autor conclui que será necessária jurisprudência para sanar a dúvida, tendo em vista a divergência de opiniões entre doutrinadores quanto a interpretação do texto normativo.

3.2 Classificação doutrinaria

Analisando a figura típica fundamental, prevista no art. 154-A do código penal, Rogério Greco explicar que se trata de crime comum, tanto com relação ao sujeito ativo, quanto ao sujeito passivo; formal (uma vez que a simples violação indevida de mecanismo de segurança , com a finalidade de obter, adulterar ou destruir dados ou informações sem autorização tácita ou expressa do titular do dispositivo, ou instalar vulnerabilidades para obter vantagem ilícita, já configura o crime, independentemente desses resultados); de dano; de forma vinculada (pois que somente poderá ser praticado mediante violação indevida de mecanismo de segurança); instantâneo; monossubjetivo; plurissubsistente; transeunte ou não transeunte (dependendo da hipótese concreta).

3.2.1 Objeto material e bens juridicamente protegidos.

Segundo o autor, bens juridicamente protegidos são a liberdade individual e o direito a intimidade, configurados na proteção da inviolabilidade dos dados e informações existente em dispositivo informático.

Objeto material é o dispositivo informático alheio, conectado ou não a rede de computadores, bem como os dados e as informações nele armazenadas.

3.2.2 Sujeito ativo e sujeito passivo

Qualquer pessoa pode ser sujeito ativo do delito de invasão de dispositivo informático, haja vista que o tipo penal em estudo não exige qualquer condição especial.

Sujeito passivo é o proprietário (pessoa física ou jurídica) do dispositivo informático invadido, ou mesmo qualquer outra pessoa que nele tenha arquivados dados ou informações.

3.2.3 Consumação e tentativa

Para Rogério Greco, em se tratando de crime formal, o delito tipificado no caput do art. 154-A se consuma no momento em que o agente consegue, efetivamente, invadir o dispositivo informático alheio, conectado ou não a rede de computadores, mediante violação indevida de mecanismo de segurança, 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.

O autor enfatiza que a obtenção, adulteração ou destruição dos dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou a instalação de vulnerabilidades para obtenção de vantagem Ilícita, caso venha a ocorrer, devem ser consideradas como mero exaurimento do crime.

Segundo o autor, considerando a natureza plurissubsistente, será possível o raciocínio correspondente a tentativa. Assim, por exemplo, a hipótese em que o agente é descoberto quando procurava invadir dispositivo informático alheio, durante suas tentativas de violar indevidamente o mecanismo de segurança, para os fins previstos no tipo penal em estudo. Nesse caso, estaria caracterizado o crime tentado.

Acentua o autor, que, no que diz respeito a modalidade equiparada, ocorrerá a consumação quando o agente produzir, oferecer, distribuir, vender ou difundir dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput do art. 154-A do código penal. Não há necessidade, portanto, que o invasor efetivamente utilize dispositivo ou programa de computador produzido, oferecido, distribuído, vendido ou difundido pelo agente, tratando também aqui, de crime formal, em que a simples prática dos comportamentos previstos pelo tipo, tem o condão de consumar a infração penal.

O autor explica que se o dispositivo ou programa de computador produzido, oferecido, vendido, distribuído ou difundido pelo agente for utilizado para a invasão de dispositivo informático, esse ultimo comportamento será considerado como exaurimento do crime tipificado no parágrafo 1 do art. 154-A do código penal.

3.2.4 E**lemento subjetivo**

O dolo é o elemento subjetivo previsto pelo tipo penal sub exame, não havendo previsão para a modalidade de natureza culposa. Rogerio Greco explica que há ainda, o que doutrinariamente é reconhecido como *especial fim de agir,* configurado nas expressões *com o fim,* prevista no caput do art. 154-A do código penal, e *com o intuito de,* existente no $1 do mesmo artigo.

Explica o autor que o delito de invasão de dispositivo informático só pode ser praticado comissivamente, entretanto, poderá ser levado a efeito o raciocínio correspondente ao crime omissivo impróprio se o agente, garantidor, nos termos do art. 13 $ 2 do código penal, devendo e podendo agir para impedir o resultado, nada fizer.

3.3 Pena, suspensão condicional do processo, competência para julgamento, ação penal.

Segundo Misael Neto Bispo da França, (2013) a falta de dignidade penal, atestada pela insignificância do quantum da reprimenda cominada a tal conduta da previsão do art. 154-A, aponta para sua pouca relevância, uma vez que se configura pena de três meses a um ano.

O autor explica que a ciranda despenalizante do diploma legal, uma vez que a pena máxima é apenas um ano, cuja competência é dos juizados especiais, onde se estimulará a conciliação, a composição dos danos civil e a transação penal. Senão vejamos:

> A pena mínima, abaixo de um ano favorece a suspensão condicional do processo, se não houve condenação, ou se não existe processo por outro crime. [...] Daí porque dizer que a reprimenda, associada ao comportamento delitivo, tem de ser idônea, isto é, deve fazer jus a gravidade da sua efetivação em face da liberdade do indivíduo, sob pena de, desnaturando suas próprias funções, da azo a inevitável autofagia. Noutras

> palavras, penas insignificantes não atendem aos princípios clássicos do direito penal, sobretudo o da lesividade (FRANÇA 2013 p.5)[32]

O autor esclarece que a função da pena é evitar a recorrência da conduta criminosa, entretanto se a pena não atribuir o mínimo de força dissuasória esta meta dificilmente será alcançada.

4 A CONVENÇÃO DE BUDAPESTE

[32] FRANÇA, Misael Neto Bispo Da. Crimes informáticos e lei "Carolina Dieckmann". Mais do mesmo. Direito penal contemporâneo. In Revista Consulex, v. 27, n 39, p.3-5, set 2013.

Criada em 2001, na Hungria, pelo Conselho da Europa, e em vigor desde 2004, após a ratificação de cinco países, a Convenção de Budapeste, ou Convenção sobre o cybercrime, engloba mais de 20 países, e tipifica os principais crimes cometidos na Internet, segundo (EDERLY, 2008) citado por Dalliana Vilar Pereira.

A autora elucida que, Segundo seu Preâmbulo, a Convenção prioriza uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional e reconhece "a necessidade de uma cooperação entre os Estados e a indústria privada". Ademais, ainda em seu escopo inicial, ressalta o obrigatório respeito: (i) à Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa (1950); (ii) ao Pacto Internacional sobre os Direitos Civis e Políticos da ONU (1966); à (iii) Convenção das Nações Unidas sobre os Direitos da Criança (1989); e (iv) à Convenção da Organização Internacional do Trabalho sobre as Piores Formas do Trabalho Infantil (1999).

O Tratado de 2001 possui quatro Capítulos (Terminologia, Medidas a Tomar a Nível Nacional, Cooperação Internacional e Disposições Finais, respectivamente) e 48 artigos encorpados num texto de fácil compreensão, sobretudo porque não traz informações deveras técnicas. O principal destaque da Convenção é que ela define (Capítulo I) os cibercrimes, tipificando-os como infrações contra sistemas e dados informáticos (Capítulo II, Título 1), infrações relacionadas com computadores (Capítulo II, Título 2), infrações relacionadas com o conteúdo, pornografia infantil (Capítulo II, Título 3), infrações relacionadas com a violação de direitos autorais (Capítulo II, Título 4). Todos dentro do Direito Penal Material. Matérias do Direito Processual são as que se seguem: âmbito das disposições processuais, condições e salvaguardas, conservação expedita de dados informáticos armazenados, injunção, busca e apreensão de dados informáticos armazenados, recolha em tempo real de dados informáticos e interceptação de dados relativos ao conteúdo.

Dalliana Villar esclarece que a competência e Cooperação Internacional são vistas no Artigo 22º, o qual aponta quando e como uma infração é cometida, além de deixar a critério das Partes a jurisdição mais apropriada para o procedimento legal.

Tal acordo parte da premissa de que o combate ao cybercrime deve ser realizado através de um Regime Internacional. Segundo Castells citado por Dalliana Vilar Pereira, Desse princípio, pode se partir para outro:

> A prática do crime é tão antiga quanto à própria humanidade. Mas o crime global, a formação de redes entre poderosas organizações criminosas e seus associados, com atividades compartilhadas em todo o planeta, constitui um novo fenômeno que afeta profundamente a economia no âmbito internacional e nacional, a política, a segurança e, em última análise, as sociedades em geral. (CASTELLS, 2007, p. 203).[33]

A autora explica que é notório que, com o fenômeno da globalização e da popularização da Internet, as fronteiras indelimitáveis do ciberespaço abrigaram não apenas criações em prol da cidadania e da participação universal (por exemplo: leitores de telas para cegos, teclados e aparelhos especiais para deficientes físicos, fóruns de discussão etc.), como também facilitaram que crimes, comumente praticados no "mundo real", se moldassem ao ciberespaço.

Nesse diapasão, Castells colaciona que a "internacionalização das atividades criminosas faz com que o crime organizado (...) estabeleça alianças estratégicas para cooperar com as transações pertinentes a cada organização, em vez de lutar entre si" (CASTELLS, 2007, p. 205).

Hoje, há um leque de ferramentas on-line que, em sinergia e bem orquestrado, pode colocar em risco não apenas indivíduos específicos, mas também Estados. Por exemplo, uma organização terrorista pode planejar um atentado e, para tal, utilizar-se dos seguintes meios:

- troca de mensagens criptografadas via: bate-papos, correio eletrônico, mensageiros instantâneos, redes sociais etc.

- escolha do local, através de programas GPS, mapas on-line, previsão meteorológica, tráfego da malha rodoviária através de câmeras ao vivo etc.

- obtenção/compra de artefatos através de sítios virtuais que vendam produtos de "segunda-mão" e/ou que não declaram impostos.

Sob esse prisma, a Internet parece ser um celeiro propício para a proliferação do que há de pior na humanidade. Porém, esses perigos reais são as grandes exceções do mundo virtual, que a convenção em estudo visa combater.

4.1 Possível ingresso no ordenamento jurídico brasileiro

[33] CASTELLS, 2007, P.203 apud, PEREIRA, Dalliana Vilar. A convenção de Budapeste e a lei penal Brasileira. Disponível em: <HTTP://www.academia.edu/786458/A_CONVENÇÃO_DE_BUDAPESTE_E_AS_LEIS-_BRASILEIRAS

Dalliana Vilar explana que, tendo em vista o relativismo da Convenção de Budapeste, bem como a flexibilidade do seu texto em, sobretudo, apontar caminhos e não propor soluções rígidas no que tange às controvérsias e resolução de litígios, surgem, então, algumas dúvidas: por que o Brasil não adere à Convenção de Budapeste? O fato de o Brasil não fazer parte da Convenção o impede de criar suas próprias leis de combate ao cybercrime ?.

Como não foi um dos signatários do Tratado e como bem lembrou o Secretário-Geral do Ministério das Relações Exteriores/Itamaraty, Samuel Pinheiro Guimarães, o Brasil não pode simplesmente aderir à Convenção, e, sim, ser convidado pelo Comitê de Ministros do Conselho Europeu. No texto original, em seu Artigo 37º – Adesão à Convenção é possível se constatar o sobredito: "(...) O Comitê de Ministros do Conselho da Europa pode(...) convidar qualquer Estado não membro do Conselho e que não tenha participado na sua elaboração, a aderir à presente Convenção" (CONVENÇÃO SOBRE O CIBERCRIME, p. 23).

Nesse Sentido, Dalliana Vilar aponta que apesar de a adesão ter de ser unânimes entre os Estados membros, e como as relações multilaterais entre o Brasil e os principais países europeus não estão desgastadas, é praticamente certa uma provável aceitação ao ingresso brasileiro. Porém, o fato de ele ainda não ser membro, não exclui – respondendo à segunda questão – existe possibilidade de se criar legislação própria para tipificar e combater o cybercrime.

4.2. **A convenção de Budapeste e a legislação penal brasileira**

Auriney brito (2013 p.59) esclarece que uma das condutas sugerida pela convenção é o *acesso ilegal* a qualquer parte de um sistema de computador sem a devida permissão, desde que seja de maneira intencional, ou seja, a convenção nessa espécie de delito não prevê a tipicidade pela modalidade culposa.

De acordo com o autor, o dolo requerido pela convenção seria a intenção de obter dados de computador, ou outra desonesta, quebrando medidas de segurança sem autorização daquele que detém o poder de permitir o acesso.

A convenção sugere no art. 5º a criminalização de interferência de sistema, que recomenda punição para o ato que, de maneira intencional, cause sério atraso, sem permissão, de funcionamento de sistema de computador, por meio de inserção, transmissão, danificação, deleção, deterioração, alteração ou supressão de dados de computador. O fato descrito, já possuía um tipo penal no Brasil, trata-se dos arts. 265 e 266 do cp., que tipifica como crime a conduta de "atentar contra a segurança ou funcionamento de serviço de água, luz, força ou calor, ou qualquer outro de utilidade publica" e 266 "interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar o restabelecimento. Nesse sentido, vejamos o que diz o autor:

> Com a alteração promovida pela lei 12.737/12 no código penal, foi acrescentado ao art. 266 §1º com redação mais específica: "incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta o restabelecimento." (BRITO, 2013, P.59)[34]

O artigo 6º da convenção considerou de muita relevância, e atribuiu pena, quanto ao mal uso de equipamento, sugerindo que os países signatários, adotem medidas legislativa para criminalizar a conduta de produção, venda, compra para uso, importação, distribuição, ou disponibilização de dispositivos, que incluem programas de computador projetados ou adaptados primariamente , com o propósito de cometer o acesso ilegal, interceptação ilegal, interferência de dados e interferência de sistema, ou ainda, a disponibilização de código de acesso, ou dados similares, por meio dos quais, todo ou qualquer parte de sistema de computador possa ser acessado com a intenção de praticar essas condutas.

Sobre a prática de phishing Auriney (2013) colaciona:

> Atualmente a prática de phishing, que tem como principal meio de execução a remessa de milhares de mensagens eletrônicas (spam) com o objetivo de captar informações sigilosas que facilitem o acesso a determinadas vantagens, foi tipificada neste artigo, importante inovação que, se não vier acompanhada de vantagem patrimonial indevida, não constitui fato típico no Brasil[35].

[34] BRITO and Auriney. Direito Penal informático, 1ª edição. Saraiva, 2013. Vitalbook fille
[35] *Ibidem*, p. 59-62

De acordo com o autor, a falsificação computacional, encontra sua previsão no art. 7º da convenção, que objetiva estabelecer como ofensa penalmente relevante, a inserção, a alteração, a deleção o supressão de dados de computador, transformando-os em falsos com a intenção de serem considerados ou terem sidos realizados para propósitos legais como se autênticos fossem. Nesse sentido esclarecedor a lição de Auriney Brito (2013 p. 62):

> Atualmente a falsificação de qualquer documento, seja ele publico ou particular, encontra tipificação na legislação penal brasileira, o que não acontece com o dado eletrônico ou de computador. Se o dado for um documento publico ou particular, não há necessidade de alteração legislativa.[36]

O autor pondera que a fraude relacionada a computador, diferentemente da falsificação de dados eletrônicos, prevê as práticas de inserção, alteração, deleção, supressão de dados de computador ou qualquer interferência no funcionamento no sistema de um computador com intenção fraudulenta, de compra, para si ou para outrem, visando benefício econômico. Segundo o autor a discussão sobre essa conduta é grande na doutrina e na jurisprudência, pois se amolda ao crime previsto nos arts. 155 § 5º (furto mediante fraude) e 171 (estelionato), caput do código penal.

Corroborando com esse entendimento o autor explana:

> Sobre a problemática já existe um ponto específico no congresso nacional brasileiro que visa a criação de uma modalidade peculiar do crime previsto no art. 171 do código penal, denominado estelionato eletrônico, o que, apesar de boa intenção, pode trazer conseqüências inesperadas e desastrosas. (BRITO, 2013, p. 62)

A convenção também recomendou a punição para tentativa, ajuda ou encorajamento para o cometimento das condutas de acesso ilegal, interceptação ilegal, interferência de dados, mal uso de equipamentos, falsificação relacionada a computador, fraude relacionada a computador, danos relacionados a pornografia infantil, ofensas a transgressões de direitos autorais e direitos correlatos, e responsabilidade corporativa.

Essas condutas já se encontram tipificadas no ordenamento jurídico brasileiro nos arts. 14,II, 29 e 286, todos do código penal brasileiro**.**

---

[36] *Ibidem,* p.62

Auriney Brito, colaciona que, a convenção prevê a possibilidade de responsabilização penal do provedor de acesso, hipótese não contemplada pela constituição federal de 1988 e tampouco pela legislação infraconstitucional.

Para que haja a responsabilidade penal do provedor de acesso, a convenção elenca alguns requisitos como que aquela conduta seja praticada em seu beneficio, por qualquer pessoa física, que haja individualmente ou como parte integrante de um órgão de pessoa jurídica, quando atue em uma posição de liderança nessa empresa. É necessário que se verifique um poder de representação e autoridade para tomar decisões em beneficio dessa pessoa jurídica para que ambos (pessoa física e jurídica) sejam responsabilizados pela conduta criminosa.

4.3 O marco civil da internet

O Marco Civil da Internet foi discutido no Brasil por meio de audiências públicas e com participação de inúmeras plataformas como Twiter, Face book, etc., e através do portal e-democracia, este último, mantido pela Câmara dos Deputados, cuja finalidade é estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil, tendo a Lei 12.965/14 - Marco Civil da Internet, sido sancionada pela presidente Dilma Rousseff em 23 de abril de 2014. (OLIVEIRA, 2015).

Segundo (Oliveira, 2015, apud Pinheiro, 2014) o documento é considerado uma "Constituição da internet", já que estabelece regras e conceitos básicos da rede, aonde se apoiarão projetos e leis futuras sobre o mundo digital. O texto indica a liberdade de expressão, a proteção da privacidade e o estabelecimento da neutralidade da rede como princípios básicos das internet, além de definir os atores e quais responsabilidades de cada um no ambiente online.

De fato, o Brasil demonstra com o referido Marco, um significativo avanço no que se refere à regulamentação da internet no Brasil. Deste modo, o usuário deverá ficar atento ao que muda em sua vida online, afinal em todo regramento imposto, é lógico afirmar que haverá perdas e ganhos, principalmente no tocante à liberdade digital, esse seria o retrocesso.

Referida Lei estabelece princípios, garantias e deveres para o uso da Internet no Brasil. Vejamos o que diz a lei *in verbis:*

> Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros;
>
> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário;
>
> [...]
>
> Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

No que concerne à proteção constitucional da honra, imagem e reputação do indivíduo, a ser tutelada pelo Marco Civil, a remoção do conteúdo junto ao provedor da página, somente será de forma direta e imediata, se envolver nudez, cena de sexo, infração de direitos autorais ou exposição de menor de idade. Entretanto, para outros casos, a remoção do conteúdo, se dará por meio de ordem judicial, podendo, ainda, a remoção ocorrer parcialmente (OLIVEIRA, 2015).

A Lei 12.965/14 deixou claro que o acesso a internet é essencial ao cidadão, e qualquer comportamento contrário aos bons costumes, que vise denegrir a imagem, honra e privacidade do indivíduo, será punida. Vejamos os arts. a seguir elencados:

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

Oliveira (2015) explica que quanto a descobrir quem foi o autor do dano, do ilícito, para coibir crimes e punir infratores, tornou-se difícil, pois a forma como está disciplinada no Marco Civil, os provedores de conexão e aplicação não podem saber quais são os dados que estão armazenados no outro. Logo, é grande a possibilidade de não conseguir associar o fato, a conduta, a uma identidade real e válida. E tais provas somente são apresentadas pela via judicial. Senão vejamos:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> §1º - O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art.

Pinheiro (2014), citado por Oliveira (2015) explica que na tentativa de acelerar o processo, há previsão de que as demandas, via de regra, tramitem nos Juizados Especiais. Isto é lamentável, pelo fato de que as demandas consumeristas ficarão na fila, priorizando-se os casos de difamação, o que não serão poucos. Assim, o Poder Judiciário, sofrerá acúmulo de processos, gerando morosidade e conseqüentemente, danos sociais. É o que se depreende da leitura do artigo seguinte, da referida lei:

> Art. 19. [...]
>
> §3o - As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.

O Marco Civil estabelece como regra que um conteúdo só pode ser retirado do ar após uma ordem judicial, e que o provedor não pode ser responsabilizado por conteúdo ofensivo postado em seu serviço pelos usuários. Com isso, o projeto pretende evitar a censura na internet: para se provar que um conteúdo é ofensivo, o responsável deve ter o direito ao contraditório na Justiça (VARELLA, 2014, Apud OLIVEIRA, 2015).

Varella (2014) explana que o texto, porém, prevê exceções. Um conteúdo pode ser retirado do ar sem ordem judicial desde que infrinja alguma matéria penal (como pedofilia, racismo ou violência, por exemplo). Isso evita que um material que possa causar riscos a algum usuário fique no ar enquanto aguarda decisão da Justiça. O que se pretende com isso, segundo

Varella, é que a internet ganhe mais segurança jurídica na retirada de conteúdo. A regra é que os conteúdos têm que continuar funcionando, a não ser que firam a lei.

Segundo Pinheiro (2015) o Marco Civil não deixa de ser um grande passo, mas ao se tirar do texto o que já tinha previsão na Constituição Federal, no Código de Defesa do Consumidor, no Código Civil, no Código de Processo Civil, no Código Penal, avançamos ainda de forma singela para dar um tratamento adequado a esta nova realidade que independe de territórios e ordenamento jurídico.

CONCLUSÃO

As comodidades e benefícios trazidos pela internet não podem ser negados a população, em razão dos riscos que os usuários correm, razão pela qual, a busca pela segurança no ciberespaço, tornou-se uma preocupação global. O Brasil passou a reconhecer o surgimento de novos bens jurídicos e passou a tutelá-los ainda que de maneira tímida, com a criação da lei 12.737/12.

Com o surgimento da sociedade digital, as autoestradas da informação se encontram em rápido desenvolvimento. A internet tem provocado avanços em praticamente todos os aspectos da sociedade e em cada canto do globo, uma vez que permite uma melhora no comercio, promove a democracia participativa, facilita a comunicação entre familiares e amigos, entre outros pontos importantes.

Com a crescente necessidade da sociedade pela interação social, e o uso sob diversos aspectos da internet, surge uma cobiçada zona criminógena, para a realização de fraudes, ofensas a pessoa, danos ao sistema financeiro, exploração sexual infantil e varias outras condutas indesejadas no denominado ciberespaço.

Verificou-se que elementos contidos na delinqüência informática, trouxeram varias preocupações para o direito penal. São condutas que levam a um sentimento de desconforto e de deficiência legislativa.

O presente estudo investigou as implicações ensejadas pela manipulação de dados pessoais, sejam através de imagens, sons, vídeos, buscando demonstrar hipóteses em que o apoderamento de informações pessoais por terceiros, e sua combinação com outras informações, podem desnudar a pessoa e funcionar como ato invasivo de aspectos pessoais.

A investigação partiu-se da análise do direito a intimidade, privacidade, honra e imagem, visando identificá-los como direito fundamental, e a proteção desses direitos sobre o aspecto privatísticos das pessoas, e os limites desses direitos, visto que nenhum direito é absoluto, e até que ponto a divulgação de informações sobre determinadas pessoas poderiam ser abusivas ou aceitáveis. Verificou-se que a intimidade pode ser extraída de instrumentos internacionais, como a Declaração Universal dos Direitos do Homem, e outros instrumentos internacionais.

A lei Carolina Dieckmann foi um marco importante para a sociedade, que incorporou ao ordenamento jurídico brasileiro com a missão de combater delitos informáticos e evitar a

impunidade dos criminosos virtuais. O objetivo da referida lei, foi importante, porem deixou a desejar.

Foram identificados mais pontos negativos do que positivos, uma vez que o texto é ambíguo e provocou dissensões entre juristas e doutrinadores, como é o caso do termo "invadir" que em outras palavras significa entrar a força. Se por outro lado, um dispositivo informático for deixado ligado e terceira pessoa se apropria de informações contidas naquele dispositivo, não configura o crime de invasão, uma vez que o agente não precisou invadir o dispositivo, já que ele estava "disponível". Já o termo "mecanismo de segurança" nos remete a idéia de proteção quanto à invasão, que se concretiza a partir da instalação de hardware como antivírus, spyware, firewall, senhas de segurança etc. a ausência desses mecanismos de segurança, faz com que o dispositivo esteja desprotegido e conseqüentemente não há que se falar em crime, uma vez que não houve a violação de mecanismo de segurança. Alguns doutrinadores entendem que o legislador infraconstitucional, pecou na qualidade técnica do artigo, e que a solução seria trocar o verbo "invadir" pelo verbo "acessar" visto que nessa modalidade o agente não opera com violência, mas tão somente com habilidades para a obtenção de dados. A segunda crítica estar em torno do verbo "obter". Se o agente não tem a intenção de obter dados, mas tão somente por curiosidade, invade dispositivo informático, ou tenta fazê-lo, essa conduta não caracteriza crime, segundo a leitura do dispositivo legal, art. 154-A.

Juristas e doutrinadores questionaram sobre a brandura da pena, que não desestimula e nem impede a recorrência dos atos criminosos. A pena varia de 03 meses a 03 anos, sendo que o código de processo penal permite a suspensão condicional do processo nos casos em que a pena mínima não seja superior a um ano, desde que o acusado não esteja sendo processado ou não tenha sido condenado por outro crime. E se a pena máxima não foi superior a dois anos, o código de processo penal permite a transação penal, que é a garantia de não ser aplicada pena privativa de liberdade, o que livra o agente de responder a uma ação penal e, sem admitir culpa, cumpre penas alternativas, tais como prestação de serviço a comunidade, pagamento de determinado valor para instituição de caridade, entre outras. Ademais, as penas por serem insignificantes, prescrevem rapidamente, inviabilizando a punição.

Existe ainda a crítica quanto ao art. 266 da mesma lei, no que concerne a interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de "utilidade pública". Se a interrupção ou perturbação não for de utilidade publica, mas de instituição privada, então o agente não terá cometido crime algum.

A preocupação com a criminalidade informática, portanto, não é completamente imprescindível, mas, cabe aos cientistas do Direito a continuação das incursões doutrinárias, principalmente no direito comparado, afim de, atingirmos um maior grau de eficácia na aplicação da lei penal, preservando os princípios e fundamentos do estado democrático de Direito.

REFERENCIAS

BRASIL. Constituição Federal, Out. 1988. Disponível em: HTTP://www.planalto.gov.br/ccivil_03/constituição/constituiçãocompilado.htm. Acesso em 20 de Mar 2015.

BRASIL. Lei 12.737, Nov 2012. Disponível em: HTTP://www.planalto.gov.br/ccivil_03/ato2011-2014/2012/lei/l12737.htm>. Acesso em 2 de Abr 2015.

BRASIL. Lei 12.935, abr 2014. Disponível em: HTTP://www.planalto.gov.br/ccivil_03/-Ato2011-2014/Lei/L12935.htm. Acesso em: 2 de abr 2015.

BRASIL.Código penal, dez, 1940. Disponível em HTTP://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em 23 de Marc 2015.

BRITO., and Auriney. Direito penal informático, 1ª edição.. Saraiva, 2013. VitalBook file.
CANOTILHO, J.J.Gomes. et al. Comentários a constituição do Brasil. – São Paulo: Saraiva 2013.

CASTELLS, 2007, P.203 apud, PEREIRA, Dalliana Vilar. A convenção de Budapeste e a lei penal brasileira. disponível em: <HTTP://www.academia.edu/786458/A_CONVENÇÃO_DE_BUDAPESTE_E_AS_LEIS-_BRASILEIRAS.

FARIAS, Edilson Pereira. Colisão de Direitos, 3 edição. Sergio Antonio Fabris Editor, 2009.

FRAGA, Vitor. Pl criminalizada divulgação de fotos intimas e vídeos na internet. Disponível em: <http://www.oabrj.org.br/materia-tribuna-do-advogado/18053-Intimidade-que-fere> Acesso em 7 de Mar de 2015.

FRANÇA, Misael Neto Bispo da. Crimes informáticos e lei "Carolina Dieckmann": mais do mesmo no direito penal contemporâneo. In Revista Juridica Consulex, v. 27, n 39, p.3-5, set 2013.

LIRA, Leide de Almeida. Lei Carolina Dieckmann: *(in) eficácia na proteção dos direitos fundamentais a intimidade e a vida privada em face da pena cominada aos delitos informáticos.* Conteúdo Juridico, Brasilia-DF: 01 Jul. 2014. Disponível em: HTTP:/www.conteudojuridico.com.br/:artigos&ver=1055.48868&seo=1.Acessp em: 31 out. 2015.

MENDES, Gilmar Ferreira. Curso de Direito Constitucional. 8.ed ver.e atual.-São Paulo: Saraiva 2013.

MENDES, Gilmar Ferreira. Direitos e garantias individuais/Direito de Personalidade/ liberdade de expressão. Revista de informação legislativa: v.31, n. 122, p. 297-301, abr./jun. 1994. bDisponível em: http://www2.senado.leg.br/bdsf/item/id/176193.

MENDES, Maria Gilmaíse de Oliveira. Direito a Intimidade e Interceptações telefônicas. Livraria Mandamentos, 1998.

OLIVEIRA, Claudio Roberto de Almeida. A extimidade da sociedade digital e a eficácia da Lei 12.737/12 - invasão de dispositivo informático. Conteudo Juridico, Brasilia-DF: 30 abr. 2015. Disponivel em: <http://www.conteudojuridico.com.br/?artigos&ver=2.53339&seo=1>. Acesso em: 11 set. 2015

PAESANI, and Liliane Minard (coord). O Direito na Sociedade da Informação III: A Evolução do Direito Digital, (v.3). Atlas, 2013. Vitalbook fille.

PEREIRA, Dalliana Vilar. A convenção de Budapeste e as leis Brasileiras. Disponível em: <HTTP://www.charlieoscatango.com.br/imagesA%convenção%20de%20budapeste%20e%20as%20leis%20brasileiras.pdf. Acesso em 11 de set 2015.

PINHEIRO., and Patricia Peck. Direito Digital, 4 edição. Saraiva, 2009. Vitalbook fille.

SAMPAIO, Jose Adércio Leite. Direito a intimidade e a vida Privada. Del Rey.1998.

VIANNA, Tulio; MACHADO, Felipe. Crimes informáticos. Belo Horizonte: Ed. Forum, 2013.