



Faculdade de Jussara – FAJ
Curso de Direito

RICARDO ANDRADE BRITO

**JUSTIÇA BRASILEIRA E CRIMES CIBERNÉTICOS: A PROTEÇÃO DOS
DIREITOS FUNDAMENTAIS À INTIMIDADE E À VIDA PRIVADA**

Jussara
2015



Faculdade de Jussara – FAJ
Curso de Direito

RICARDO ANDRADE BRITO

**JUSTIÇA BRASILEIRA E CRIMES CIBERNÉTICOS: A PROTEÇÃO DOS
DIREITOS FUNDAMENTAIS À INTIMIDADE E À VIDA PRIVADA**

Monografia apresentada ao Curso de Direito da Faculdade de Jussara, como requisito parcial à obtenção do grau de Bacharel em Direito, sob orientação do Professor Esp. João Paulo de Oliveira.

Jussara
2015

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, força maior que nos rege e conduz...

À minha família, meu porto seguro...

Aos meus professores, pelo compartilhamento de seus conhecimentos e generosidade em transmiti-los...

Aos colegas, pelo apoio e cumplicidade...

“Se ocorre injustiça em um lugar qualquer,
constitui-se uma ameaça para com a
justiça em todos os lugares”.

Martin Luther King

RESUMO

A sociedade moderna vive um momento em que as evoluções tecnológicas deram lugar à possibilidade de novos crimes, como os cibernéticos ou virtuais. Diante disso, o Direito brasileiro, por sua obsolescência, não se encontra devidamente preparado para lidar com estes tipos de delitos, os quais violam os direitos fundamentais do indivíduo, como os: da personalidade, da privacidade, da intimidade e da honra. Neste sentido, esta monografia tem o intuito de investigar sobre estes crimes digitais e, ao mesmo tempo, apresentar uma análise da lei Carolina Dieckmann (Lei nº 12.737/2012) que, apesar de tipificar algumas condutas criminosas em face do uso da Internet, ainda se mostra insuficiente para atender à demanda específica de crimes cibernéticos. Para que este estudo fosse possível foi realizada uma pesquisa de caráter bibliográfico, na qual foram selecionados autores, como: Moraes (2009), Silva (2011), Bittar (2004), Ferreira (2000), Capellari (2000), Capez (2011), Vianna (2013), entre outros. Buscou-se estabelecer um diálogo entre os autores, para que se chegasse a um consenso plausível diante do objeto de estudo tomado para este estudo monográfico. Concluiu-se que a Legislação brasileira se encontra despreparada para julgar e punir os criminosos que se utilizam da tecnologia de comunicação para cometerem delitos danosos a outrem.

Palavras-chave: Direito. Crimes virtuais. Legislação brasileira. Lei Carolina Dieckmann.

ABSTRACT

Modern society is going through a time when technological developments have led to the possibility of new crimes such as cyber or virtual. Thus, the Brazilian law, in obsolescence, is not properly prepared to deal with these types of crimes, which violate fundamental rights of the individual, such as: personality, privacy, intimacy and honor. In this sense, this monograph aims to investigate these digital crimes and at the same time, present an analysis of Carolina Dieckmann law (Law No. 12,737 / 2012) that although typify some criminal conduct in the face of Internet use, still is insufficient to meet the specific demands of cyber crimes. For this study it was possible to bibliographical survey was conducted, in which authors were selected, as Moraes (2009), Silva (2011), Bittar (2004), Ferreira (2000), Capellari (2000), Capez (2011), Viana (2013), among others. Sought to establish a dialogue between the authors, in order to reach a reasonable consensus on the object of study taken for this monographic study. It was concluded that Brazilian legislation is unprepared to prosecute and punish criminals who use communication technology to commit crimes harmful to others.

Keywords: Right. Cybercrime. Brazilian legislation. Law Carolina Dieckmann.

SUMÁRIO

INTRODUÇÃO	7
CAPÍTULO 1: OS DIREITOS CONSTITUCIONAIS E CIVIS FACE À SOCIEDADE DA INFORMAÇÃO	10
1.1 Os direitos da personalidade	15
1.2 O direito à intimidade	20
1.3 O direito à vida privada	22
1.4 O direito à honra	23
CAPÍTULO 2: O DIREITO DIANTE DA SOCIEDADE TECNOLÓGICA	25
2.1 Princípios da Segurança da Informação e elementos de proteção jurídica	29
2.2 A tutela de proteção digital	32
CAPÍTULO 3: CRIMES CIBERNÉTICOS: ANÁLISE DOS CONCEITOS E PRESSUPOSTOS LEGAIS DIANTE DA LEI CAROLINA DIECKMANN (LEI Nº 12.737/2012)	36
3.1 Crimes virtuais: conceitos e particularidades	37
3.2 Os crimes virtuais e a legislação aplicável	41
3.3 Análise da Lei nº 12.737/2012	43
CONSIDERAÇÕES FINAIS	48
REFERÊNCIAS BIBLIOGRÁFICAS	50

INTRODUÇÃO

É certo que a ciência e a tecnologia se desenvolveram nos últimos tempos e, em consequência disso, a sociedade passou por diversas transformações em seus campos: econômico, político, cultural e social. Desse modo, é comum considerar os avanços científicos e tecnológicos como sendo os motores do progresso, pois, à medida que impulsionaram o desenvolvimento do saber humano, também instituiu novas formas de relacionamento sociocultural.

No entanto, é necessário considerar que além dos benefícios decorrentes destes avanços, a nova sociedade da informação deu origem a novos e complexos conflitos, cujo enfrentamento, por parte da Justiça e da sociedade, apresenta a mesma complexidade.

Tal fato é relevante, pois esta sociedade da informação produz mazelas que envolvem questões pessoais e de caráter privado, como acontece na rede mundial de computadores – a Internet. Neste contexto, muitos usuários apresentem condutas destoantes dos princípios morais e éticos desejados pela sociedade. E, certamente, isso tem acarretado prejuízos para os cidadãos, para as entidades e órgãos públicos, assim como para as organizações privadas.

Assim, o objeto de estudo desta monografia parte da premissa de que os casos nos quais as pessoas utilizam a Internet como ferramenta para cometer atos criminosos, causadores de dolo a outrem, têm aumentado acentuadamente. Em função disso, crê-se relevante que os crimes digitais ou cibernéticos sejam discutidos não apenas por segmentos sociais interessados no tema, mas também pela comunidade acadêmica, em especial pela área de estudos do Direito.

Dessa forma, este estudo se justifica devido ao fato de que tais avanços trouxeram consigo fatores negativos, visto que tornaram possível a existência de crimes que a legislação brasileira não estava preparada para compreender, nem identificar e, muito menos, punir. Isso porque o Código Penal Brasileiro é antigo, data da década de 1940, época em que não se aventava a hipótese de a Justiça ter que lidar com estes tipos de crimes.

Portanto, é clara a necessidade de se criar tipos penais ainda não previstos na legislação para lidar com delitos desta natureza, visto que não é adequado nem permitido utilizar a analogia jurídica. A esse respeito, Fernando Capez assevera que:

Ao aplicar a analogia em norma penal incriminadora se está ferindo o princípio da reserva legal, visto que um fato apenas comparado legalmente como crime, estaria sendo tido como tal. Pode-se imaginar, para efeito de compreensão, o típico o furto de uso (roubo de objeto alheio móvel para o uso), se for usada a analogia do artigo 155 do Código Penal (subtração de coisa alheia móvel com intuito de se apossar definitivamente dele). Assim, um fato não considerado criminoso pela lei passaria a sê-lo, em evidente afronta ao princípio constitucional do art. 5º, XXXIX (reserva legal). Tal analogia in *malam partem*, a priori, não seria possível, uma vez que jamais seria benéfica ao acusado a incriminação de um fato atípico (CAPEZ, 2010, p. 59).

Nesse sentido, o embasamento teórico deste estudo partiu do princípio de que a Constituição Federal de 1988 legitima e garante os direitos fundamentais do cidadão, com a finalidade de protegê-lo de abusos e de excessos, de acordo com o art. 187 do Código Civil, o qual é bastante claro quando estabelece que um indivíduo também comete um ato ilícito se houver constatação do abuso de direito quando excede os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos maus costumes.

Soam-se a isso o que está disposto no artigo 5º, inciso “X” da CF/88, o qual determina que são invioláveis: a intimidade, a honra, a privacidade e a imagem das pessoas, devendo ser assegurado o direito a indenização pelo dano material ou moral que decorrer de tal violação.

Desta maneira, no caso dos crimes cibernéticos, é notória a necessidade de que sejam disciplinadas as diversas situações que se relacionam a esses crimes, que ainda não estão consideradas no ordenamento jurídico brasileiro. Dessa forma, na maioria dos casos, é mais fácil buscar no Código Civil as possibilidades legais de solução das questões relacionadas à proteção de dados.

No entanto, é relevante considerar que nem sempre será possível usar a analogia das normas aplicando-as às especificidades do contrato eletrônico, do comércio eletrônico, do documento eletrônico etc. Surge daí, portanto, a necessidade de o legislador se preocupar em dar segurança jurídica às relações virtuais e, ao mesmo tempo de colocá-las em apreciação crítica.

Para tanto, esta pesquisa será pautada no método de pesquisa dedutivo, visto que o objeto de estudo parte de uma análise geral para uma situação particular, ou seja, a pesquisa abordará uma investigação sobre uma situação geral: a prática de crimes informáticos e suas consequências, convergindo para um estudo particular, ou seja, a análise da Lei Carolina Dieckmann (Lei nº 12.737/12).

Ainda, será utilizada a pesquisa bibliográfica como procedimento técnico, em que serão selecionados estudos referentes ao tema escolhido, para que se tenham fundamentos teóricos suficientes para estabelecer um diálogo entre os autores e se chegar a reflexões coerentes com a realidade que se nos apresenta.

Por fim, deve-se acrescentar que a abordagem da pesquisa será qualitativa, pois serão analisados estudos realizados sobre o objeto investigado, de modo a se proceder a uma análise coerente dos pressupostos que permeiam a legislação pertinente.

Em termos de estrutura, o estudo será dividido em três capítulos, a saber: no primeiro, serão abordados os direitos fundamentais constitucionais e civis que se relacionam ao objeto de investigação; no segundo, será apresentado um estudo sobre a tutela dos direitos fundamentais do cidadão, buscando analisar de que forma a Justiça lida com casos de crimes virtuais ou cibernéticos; e, por fim, será feita uma análise da Lei Carolina Dieckmann, Lei nº 12.737/12, que foi promulgada para lidar com esta matéria jurídica e, que apresenta lacunas importantes, tornando-a parcialmente ineficiente diante da diversidade de crimes decorrentes do uso tecnológico contextualizado.

1 OS DIREITOS CONSTITUCIONAIS E CIVIS FACE À SOCIEDADE DA INFORMAÇÃO

É fato que atualmente a humanidade, em sua grande maioria, está inserida em um mundo paralelo, o qual se apresenta mais cômodo e ágil na realização de afazeres do dia a dia; um mundo em que fronteiras não existem, no qual é possível se comunicar, comprar, instituir relacionamentos, aprender, estudar, enfim, interagir com o mundo de maneiras diversas, desde que se disponha de um computador interligado a outros por meio de uma ferramenta tecnológica denominada: Internet (AZEVEDO JUNIOR, 2014).

É importante salientar que a partir da Internet,

O homem descobriu um novo modo de se relacionar com o mundo – a realidade virtual. Através de dispositivos que transmitem ao usuário as palavras, as imagens, os sons e as sensações dos mundos simulados, é possível atuar, mover-se e comunicar-se através do computador de forma similar com o que se faz na vida cotidiana (MNEMOSYNE, 2014, p. 2)

Assim, a Internet transformou-se em um marco do mundo globalizado, visto que carrega consigo inúmeras possibilidades de se aplicar suas ferramentas para o desenvolvimento das diversas áreas do conhecimento humano. Soma-se a isso, o fato de que a Internet permite uma espécie de interação social muito democrática. Tais reflexões vão ao encontro dos ensinamentos de Nogueira (2009, p.23), quando ele assevera que a Internet “(...) é utilizada por todas as classes sociais, por pessoas de todas as idades, pelos setores públicos ou privados e quase tudo que fazemos passa por um computador”.

É fato que o aumento da utilização da Internet, à medida que possibilita experiências comunicativas rápidas e completas, entre indivíduos de diversos lugares, também abre espaço para a ação de indivíduos desprovidos de boas intenções.

Tais práticas ilícitas ocorrem através do uso da Rede Mundial de Computadores – INTERNET, nas mais variadas formas, como por exemplo, o plágio de trabalhos acadêmicos, a disseminação da pedofilia, episódios de calúnia e de difamação, a clonagem de cartões de crédito, o uso indevido da imagem de outras pessoas, entre outras.

Por isso, ocorreu uma mudança em relação a hábitos e atitudes por parte dos usuários desta rede, originando uma nova forma de viver. Essa nova sociedade é decorrente da terceira revolução tecnológica, que tem na Internet seu maior símbolo, sendo que esta se configura como uma reestruturação do contexto social mundial, tanto que a sociedade hoje parece estar envolta numa rede:

Rede, como espaço, é a palavra chave. Aparece na maioria das disciplinas, alimenta metáforas, perde em precisão o que ganha em extensão. O homem contemporâneo está preso cada vez mais no universo das redes; suas práticas, seu modo de vida são modificados a partir disso, o exterior é introduzido e acolhido pela máquina de comunicar (DUPAS, 2000, p. 56).

É relevante, portanto, frisar que esta nova sociedade está interligada por redes eletrônicas, cujas estruturas e valores estão fundamentados na informação, elemento este que carrega consigo a possibilidade moldar as novas relações sociais e econômicas. Isso estabelece a informação como o paradigma que estrutura a sociedade moderna (MONTEIRO NETO, 2008).

Em função disso, a sociedade contemporânea, devido aos avanços tecnológicos, tem vivenciado uma realidade na qual os direitos fundamentais, dentre os quais citam-se os direitos à vida privada e íntima, estão sendo violados. Tais violações têm originado prováveis traumas pessoais e, conseqüentemente, têm dado margem a sérios problemas tanto no âmbito profissional e financeiro, quanto nas relações sociais das vítimas desses criminosos virtuais.

Tal questão se agrava, pois não há, ainda, um sistema jurídico eficiente capaz de lidar coerentemente com este tipo de situação. Desse modo, as pessoas parecem estar à mercê de criminosos que têm conhecimento suficiente para burlar sistemas de informática, programas de proteção digital, sites de relacionamentos pessoais, enfim, tais indivíduos colocam a todos sob a égide do medo e da insegurança (LIRA, 2014).

Nesse ínterim, se torna relevante impetrar uma discussão sobre os direitos fundamentais do ser humano, partindo do pressuposto de que estes foram aventados no Código Civil de 1916 e legitimados pela Constituição Federal do Brasil, de 1988.

Destaca-se, pois, que a compreensão e análise de tais direitos devem ser uma constante não apenas entre aqueles que têm esses direitos violados, mas por todos os grupos sociais e pelo Governo, visto que todos estão sob a mesma

condição, ou seja, qualquer pessoa pode ser uma vítima dos crimes que violam os direitos essenciais das pessoas, como o são os crimes cibernéticos e/ou digitais (LIRA, 2014).

É cediço destacar que, para compreender o objeto de estudo delineado para esta monografia, necessário se faz apresentar um estudo, mesmo que breve, sobre os direitos fundamentais do indivíduo, para que seja possível compreender melhor a natureza do objeto de estudo delineado para este trabalho monográfico. Assim, a partir do estudo dos direitos fundamentais da pessoa, crê-se que seja possível apresentar argumentos suficientes para discutir acerca dos crimes cometidos por meios digitais.

Historicamente, numa dimensão empírica, considera-se que os direitos fundamentais são, essencialmente, os direitos humanos (GUERRA FILHO, 1997, p. 2). Dessa forma, pode-se afirmar que os direitos fundamentais resultam em posições jurídicas das pessoas enquanto tais, de modo que haja eficácia no que concerne às relações com o Estado ou entre particulares, amparadas ou não pela Constituição.

Sob a mesma perspectiva teórica, Alexandre Moraes (2009, p. 39) define os direitos humanos fundamentais como

(...) o conjunto institucionalizado de direitos e garantias do ser humano que tem por finalidades básicas o respeito à sua dignidade, por meio de sua proteção condições mínimas de vida e desenvolvimento da personalidade humana (MORAES, 2009, p. 39).

Nesta mesma esteira, José Castan Tobeñas (1952, apud MORAES, 2000), também assevera que os direitos humanos são aqueles referentes aos princípios fundamentais da pessoa humana – tanto na esfera individual como coletiva. É relevante, portanto, observar que os direitos humanos estão ligados à garantia de que não há intervenção do Estado na esfera individual e, dessa maneira, é possível vislumbrar a consagração da dignidade humana. Posto assim, é coerente afirmar que, devido ao fato de existirem diversos conceitos sobre os direitos fundamentais, é complexa a tarefa de estabelecer uma única definição que seja capaz de englobar toda a sua hermenêutica.

A esse respeito, para José Afonso da Silva (2011) atesta que

A ampliação e as transformações dos direitos fundamentais humanos, no envolver histórico, dificultam a definição de um conceito sintético e preciso. Tal dificuldade é aumentada se são empregadas

várias expressões para designá-los, tais como: naturais, humanos, individuais, públicos subjetivos, liberdades fundamentais, liberdades públicas e direitos fundamentais (SILVA, 2011, p. 175).

Pelo alcance de sua abrangência, é possível dizer que esses direitos colocam-se em elevada posição hermenêutica, isto é, a interpretação do sentido que apresentam em referência aos outros direitos previstos no ordenamento jurídico brasileiro é complexa. De acordo com Silva (2002, p. 24), os direitos fundamentais se caracterizam por ser imprescritíveis, inalienáveis, irrenunciáveis, invioláveis, universais, efetivos, interdependentes e complementares. É certo que tais fatores tornam a sua interpretação jurídica bastante intrincada.

Cabe aqui destacar que, do prisma material, os direitos fundamentais são variáveis de Estado para Estado, visto que dependem de sua ideologia, o que quer dizer que cada Estado possui sua especificidade de direitos. Contudo, Schmitt (1996), afirma que o autêntico direito fundamental de uma pessoa se caracteriza como absoluto e corresponde ao princípio de distribuição do Estado de Direito. Segundo este, a liberdade do indivíduo não apresenta limites a priori, e a faculdade do Estado limitada em princípio.

Diante disso, é interessante frisar que

Atualmente, é fora de dúvida a superação do individualismo, fonte inspiradora do Código Civil de 1916, face às perspectivas hermenêuticas construídas a partir do advento da Constituição da República Federativa do Brasil de 1988. A partir de então, se tornou indispensável uma releitura de todo o ordenamento jurídico à luz dos novos paradigmas constitucionais, abrigando em seu seio muitas realidades novas devido às transformações sociais contemporâneas (MELLO, 2002, p. 29).

Uma forma de se compreender tais transformações sociais é observar que o *ethos* da sociedade contemporânea, ou seja, o modo de ser e de viver individual ou coletivamente¹, é bem diferente do que se presenciava há algum tempo. Posto assim, é primordial que a hermenêutica do direito seja realizada à luz de um procedimento aberto, buscando enxergar as modificações sofridas pelas pessoas e pela sociedade.

O exercício de interpretação da lei e das normas constituintes do ordenamento jurídico, geralmente reconhecido como hermenêutica, pode ser realizada a partir de procedimentos fechados ou abertos. A hermenêutica fechada é mais comodista, pois que demanda esforço intelectual reduzido do intérprete; assim sendo, a interpretação desenvolve-

¹ Cf. FRANKENA, William. **Ética**. Rio de Janeiro: Zahar, 1969, p. 56.

se segundo perspectiva burocrática e literal do texto legal. Assim, a hermenêutica aberta mostra tendência inovadora, requerendo a capacidade de reflexão do Judiciário ou do Direito, de modo a se tornar viável a adaptação às novas situações e desafios postos pela sociedade (MELLO, 2002, p. 29).

Acrescenta-se a esses ensinamentos, as palavras de Miguel Reale (1995), em sua obra *Lições Preliminares do Direito*, na qual o autor coloca que:

A interpretação de uma lei requer, em primeira instância, que a mesma seja compreendida na plenitude de suas finalidades sociais, para que se possa determinar o sentido de cada um de seus dispositivos. Apenas dessa forma a lei é aplicável a todos os casos que se relacionem aos objetivos delineados para tal. Dessa forma, o cuidado inicial do hermeneuta contemporâneo é o de saber qual a finalidade social da lei, pois é o fim que possibilita a penetração em sua estrutura significativa particular (REALE, 1995, p. 285).

Assim, deve-se considerar que os princípios legais não podem ser interpretados por partes, visto que é imperativo que o processo de interpretação busque uma compreensão do todo. Nesse sentido, o ato de interpretar deve voltar-se para o intuito de atender às contendas sociais para as quais a norma ou princípio foi elaborado.

É nesse sentido que se afirma a necessidade de uma interpretação legal voltada para o atendimento das exigências do novo *modus vivendus* da sociedade moderna. Para Melo (2002), esta sociedade vive sob uma vertente de legitimidade social, de modo que alguns segmentos dos pensadores do Direito têm ansiado pela aplicação de novas abordagens que dêem a possibilidade de respostas às novas demandas sociais.

Ainda, na esteira dos ensinamentos de Melo (2002), pode-se afirmar que é preciso enfrentar a delicada tarefa de uma interpretação uma lei e aplicá-la dentro dos parâmetros estabelecidos pela Constituição Federal do Brasil. Assim, certamente, a Justiça poderá oferecer um tratamento justo às lides decorrentes dessa nova realidade material, real e histórica que se desenha nas inter-relações socioinformatizadas.

Nesta mesma linha de reflexão, é interessante destacar a lição do Professor Paulo Bonavides ao explicar que:

O sistema constitucional apresenta elasticidade e flexibilidade, o que nos permite inferir o sentido dado pela Constituição em face da ambiência social, que ela reflete, e a cujos influxos está sujeita, numa escala de dependência cada vez mais avultante (BONAVIDES, 1999, p. 77).

Depreende-se, destas reflexões, que a hermenêutica, ou seja, a interpretação usada para analisar e decidir sobre os conflitos decorrentes das novas relações sociais, como o são os crimes cibernéticos, deve estar em consonância com a realidade social da qual emerge tal problema. Em razão disso, o sistema constitucional deve ser considerado com flexibilidade, para que possa dar conta da complexidade que envolve as práticas criminosas originárias de ambientes virtuais.

É interessante acrescentar que o Professor Miguel Reale foi Supervisor da Comissão Elaboradora e Revisora do Código Civil, em 1975. Em um dos trechos do documento em questão, Reale aborda a necessidade de se revisar o ordenamento jurídico brasileiro, principalmente no que tange as questões sociais, as quais envolvem os direitos fundamentais do ser humano, tendo como suporte argumentativo o dinamismo sociocultural e político que emergem na linha histórica de um povo.

Superado definitivamente o individualismo, o qual fora condicionador das fontes inspiradoras do código em vigência e reconhecendo mais amiúde que o Direito tem um caráter social em sua essência e em seu destino, correlacionando concretamente os valores coletivos e os individuais, de modo que a pessoa humana seja preservada sem privilégios e exclusivismos, diante de uma ordem global comum e participativa, não pode haver medo, pois é urgente e indispensável que se renovem os códigos atuais, o que configura uma das mais nobres e corajosas metas do governo (REALE, 1975, p. 108).

Diante destas colocações, é coerente afirmar, então, que em face de novas situações, são primordiais também que sejam discutidas e postas em ação novas regulamentações jurídicas, para que as normas que regem o destino de uma nação, não se percam no tempo e deixem de prestar os benefícios para os quais elas foram concebidas.

1.1 OS DIREITOS DA PERSONALIDADE

É mister reafirmar que a Constituição Federal de 1988 implantou novos valores que visam a assegurar e a promover a dignidade da pessoa humana. Assim, é coerente dizer que o aplicador do Direito deve se dedicar ao estudo dos mais variados institutos jurídicos, com a finalidade de adequá-los à ordem constitucional vigente. Trazendo para o escopo dos crimes cibernéticos e sua violação dos direitos da personalidade, é necessário aprofundar o estudo para o campo dos direitos humanos (BOBBIO, 1988).

Tal impressão é relevante, pois a compreensão dos direitos da personalidade, invariavelmente, levam a uma discussão sob o escopo dos direitos humanos. A esse respeito, é fundamental considerar as lições de Norberto Bobbio (1988), o qual sustenta que

(...) os direitos humanos surgem como direitos naturais universais, são desenvolvidos como direitos positivos particulares (ao passo que cada Constituição incorpora declarações de direitos) para, no final encontrarem sua realização total, sendo reconhecidos como direitos positivos universais (BOBBIO, 1988, p. 30).

Portanto, em consonância com a realidade social proveniente da sociedade tecnológica e insegura que se apresenta a todos, podem-se citar as reflexões de Costa (2011), quando o mesmo afirma que os crimes cibernéticos, como a invasão de sites pessoais, extração de informações sigilosas, publicação de imagens íntimas, enfim, todos os crimes ligados à Internet, terminam por violar o direito à privacidade e, devido a isso, o tema tem sido objeto de estudo de muitos juristas, principalmente nos últimos tempos.

A violação da privacidade encontra no texto constitucional remédios rápidos, visto que essa violação já constitui, em alguns casos, um ilícito penal. Ademais, a Constituição foi clara em assegurar à parte lesada, o direito à indenização por dano material ou moral decorrente da violação da intimidade, da vida privada, da honra e da imagem das pessoas, em suma, do direito à privacidade (SILVA, 2009, pg.210).

Posto isso, é relevante discutir, nos moldes constitucionais, o que realmente significa o termo “privacidade”. De acordo com Costa (2011), a privacidade compreende aquilo que é ou está exterior ao Estado, pois pertence à pessoa, sendo-lhe particular ou própria do indivíduo.

Portanto, é coerente inferir que a privacidade pode ser considerada como uma faculdade intrínseca a todo indivíduo e, portanto, diz respeito apenas à própria pessoa ou sobre as suas atividades particulares, devendo ser mantida fora do alcance de terceiros, se for do interesse deste indivíduo.

Ainda é relevante acrescentar que a privacidade, em seu sentido amplo, pode ser compreendida como:

O conjunto de informações sobre o indivíduo, o qual este decide manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito. A privacidade reúne todas as manifestações do âmbito íntimo, privado e da personalidade, consagrados pelo texto constitucional. A esfera de inviolabilidade é ampla e abrange o modo de vida doméstico, as relações familiares e afetivas em

geral, fatos, hábitos local, nome, imagem, pensamentos, segredos, e, bem assim, as origens e planos futuros do indivíduo (SILVA, 1992, p. 188).

Em face de tais considerações, pode-se observar que a privacidade se refere ao modo de ser e viver de cada um, sendo, portanto o direito que a pessoa tem de viver conforme seus princípios, sem que terceiros venham a ter conhecimento de fatos que o próprio indivíduo quer manterem sigilo, visto que é um direito fundamental garantido pela Constituição.

Conforme Celso Ribeiro Bastos:

A evolução tecnológica possibilita uma devassa na vida íntima das pessoas. (...) Na época atual, as lentes teleobjetivas e os aparelhos eletrônicos de ausculta, facilitam uma devassa na vida íntima das pessoas. (...) Por isso, sentiu-se a necessidade de proteger de maneira específica a imagem das pessoas, a sua vida privada, a sua intimidade (BASTOS, apud GUERRA, 1999, p. 48).

Portanto, é de conhecimento geral que é comum o aparecimento de pessoas anônimas em fotos ou filmes propagados pelos meios de informação, que são coletados em eventos públicos, como: atos de posse, eventos beneficentes da classe alta da sociedade, em shows, além de operações policiais, e eventos relacionados ao esporte etc. Daí, tais imagens são postadas na internet e, em questão de pouco tempo, é provável que já haja muitas pessoas a par da situação, desencadeando problemas sérios à vida das pessoas em exposição (GUERRA, 1999).

Filosoficamente, Zavala de Gonzáles discute o tema sugerindo que:

(...) a intimidade se apresenta como uma condição essencial do homem, a qual lhe permite viver dentro de si mesmo e de se projeta no mundo exterior a partir dele mesmo, como único ser capaz de dar-se conta de si e de fazer de si o centro do universo (GONZÁLES, 1993, p. 175)

Percebe-se que tal conceito se apresenta carregado de subjetividade, isto é, está focalizado no indivíduo como o centro do direito, dando ênfase à sua capacidade de autogestão. Portanto, não seria incoerente afirmar que o direito à intimidade se caracteriza por se basear na busca em defender as pessoas dos olhares alheios e da interferência na sua esfera íntima, através da espionagem e da divulgação de fatos obtidos ilegalmente.

No entanto, é fato que, atualmente, a punição de crimes de natureza tecnológica vem sendo feita a partir dos dispositivos legais existentes que se assemelham ou se relacionam com este tipo de matéria jurídica, sendo que os

legisladores estão buscando analogias no Código Penal, no Código Civil para terem respaldo adequado para legislar em casos da natureza digital ou tecnológica. Isso ocorre porque a tipificação dos crimes virtuais na Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que é a única lei específica para esses casos, apresenta falhas, o que será discutido no terceiro capítulo desta monografia.

Na esteira destas reflexões, importante considerar que a garantia da preservação da intimidade e da vida privada, quando estas são colocadas à mostra social, indevidamente ou inadvertidamente, devem ser denunciadas e punidas coerentemente. É nesse sentido que “(...) a Constituição Federal prevê o direito de indenização por dano material, moral e à imagem, consagrando no inciso V, do art.5º, ao ofendido a total reparabilidade em virtude dos prejuízos sofridos” (MORAES, 2006, pg. 44).

Convém destacar também que neste mesmo artigo, no inc. X, a Constituição do Brasil reza que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988).

Portanto, é relevante refletir que os problemas trazidos pela sociedade da informação globalizada, através da Internet, dá possibilidades para que as pessoas usuárias da rede sejam alvos de crimes que lesam o cidadão de várias formas, entre elas podem ser citadas: a exposição de sua vida íntima, violação de sua honra, lesão por danos materiais financeiros, entre outras formas de prejuízos e danos.

Destarte, deve-se considerar que a inclusão no Código Civil de capítulo específico destinado a tratar do tema direitos da personalidade evidencia a sintonia entre o legislador brasileiro e os pressupostos da doutrina moderna. Isso foi muito importante, pois:

O Código Civil brasileiro anterior nada previa a respeito, sendo completamente avesso à filosofia de proteção ao homem, como ser humano, visto que priorizava a proteção aos bens patrimoniais, em detrimento dos bens existenciais, nos quais se inserem aqueles relativos à personalidade do ser humano (OLIVEIRA, 2002, p. 15).

Assim, é certo afirmar que tal inovação foi fundamental por reconhecer tacitamente a existência de direitos extrapatrimoniais decorrentes das relações interprivadas. Isso ainda, fomenta a possibilidade de que a pessoa lesada em qualquer direito relativo à personalidade possa requerer a

reparação dos danos, porventura sofridos em virtude de lesão ou de ameaça de lesão a esses direitos. Vale colocar que “a proteção à pessoa humana se complementa, considerando que a legislação civil passa a prever o que se pode chamar de ‘direitos subjetivos privados’” (TEPEDINO, 1999, p. 33).

Posto assim, a intimidade e a vida privada são consideradas na Constituição Federal, como sendo os valores voltados para a consolidação dos valores humanos, em caráter de direito individual. Dessa forma, de acordo com o Código Civil brasileiro:

Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei.

Parágrafo único. Em se tratando de morto, terá legitimação para requerer a medida prevista neste artigo o cônjuge sobrevivente, ou qualquer parente em linha reta, ou colateral até o quarto grau. (BRASIL, 2002)

Tais disposições legais confirmam o caráter ilícito dos delitos cometidos virtualmente e impõem a necessidade da reparação possível dos danos, porventura sofridos pelas vítimas. É fundamental que isto aconteça realmente, pois o desenvolvimento da tecnologia de comunicação está propiciando que a vida das pessoas seja espionada e sua intimidade sendo exposta ao público.

De acordo com Silva (1998), interceptando correspondências via Internet, pode-se revelar segredos e vigiar os passos das pessoas na Terra. Além disso, as microcâmeras podem expor a vida das pessoas ao público, tornando-a um caos.

Daí surge a necessidade de que o Estado seja competente para assegurar que os direitos à intimidade e à privacidade dos indivíduos, pois, como observa Edson Ferreira da Silva,

(...) em face de uma sociedade na qual diversos estilos e pontos de vista provocam reações negativas quando são conhecidas publicamente, é essencial um substancial grau de liberdade contra as observações, de modo a haver um genuína autonomia (SILVA, 1998, p. 2)

Nesta mesma linha, José de Oliveira Ascensão (1998), assevera que o direito à individualidade pode ser compreendido sob três esferas: a individual, a privada e a secreta. A primeira esfera protege o homem em relação à sociedade, quanto à sua identificação pessoal e sua imagem, assim como quanto ao valor da honra; a

segunda, se concentra na privacidade, como sendo uma forma de defesa da autonomia, o que é necessário para que a vida da pessoa não seja absorvida pela comunidade; por fim, a terceira esfera corresponde àquilo que é de reserva absoluta, àquilo que é inerente ao conhecimento e à consciência de cada indivíduo.

Assim, para colocar em discussão o referido tema, é coerente destacar que o individualismo acentuado, característico da sociedade moderna, deu origem ao reconhecimento de direitos em favor dos grupos sociais e do próprio indivíduo; disso decorre o direito de associação, sendo uma garantia de que a liberdade individual seja respeitada.

Soma-se a isso o fato de que, conforme Silva apud Sarlet (2011), a doutrina constitucional moderna, salvo as exceções, vem afastando a utilização de expressões como liberdades públicas, liberdades fundamentais, direitos individuais, direitos públicos subjetivos, direitos civis e direitos naturais, bem como suas variantes. Isso porque tais termos, de alguma forma, estão sendo dissociados do estágio atual de evolução dos direitos fundamentais, visto que o Brasil é um Estado democrático e social, de Direito.

1.2 O DIREITO À INTIMIDADE

Em princípio, é fundamental observar que a vida íntima de uma pessoa é considerada inviolável. Por isso, a exposição pública de fatos que apenas dizem respeito à própria pessoa é vedada pela Constituição brasileira e deve ser encontrada uma maneira coerente de reparar os danos trazidos por delitos dessa natureza (MORAES, 2009).

Em princípio, cabe colocar que a discussão sobre o direito da intimidade suscita dificuldades: por um lado, é necessário precisar a extensão do seu conteúdo, porque ele tem caráter subjetivo e varia de pessoa para pessoa; por outro lado, deve-se reconhecer que os valores sociais são mutáveis no tempo e no espaço e acompanham a dinâmica das relações sociais.

Neste mesmo sentido, há dificuldade em se estabelecer em quais situações o interesse pela preservação da intimidade deva ser sacrificado em prol de outro interesse juridicamente protegido, quando se encontram antagônicos. É importante destacar que o direito à intimidade e à vida privada não possuía

expressão jurídica antes do final do século XIX. No entanto, pode-se afirmar que os princípios gerais, bem como os direitos consagrados naquela época, protegiam e se relacionavam ao que atualmente discutidos à luz do conceito de intimidade e privacidade (LIRA, 2014).

É relevante, então, destacar que os fatores que oportunizam a regulação dos direitos à intimidade e à vida privada, eram antes tratados à luz de uma hermenêutica clássica e tradicional, a qual não prevê uma proteção específica desses direitos diante de situações de violação dos mesmos.

Deve-se ressaltar que a partir do desenvolvimento da sociedade, com o crescimento indiscriminado das cidades, com a criação das relações de consumo e com o avanço da tecnologia, é certo que a intimidade e a vida privada passaram a apresentar a exigência de um sistema de proteção mais específico, haja vista que tais medidas se tornam essenciais em função das novas formas de perigo que se apresentam nestes novos tempos.

A esse respeito, José Adércio Leite Sampaio, leciona que:

Se julgarmos, em princípio, que a história do direito fundamental à intimidade e à vida privada será a história do homem em busca de realização de sua dignidade, certamente se falará em lutas contra a opressão e a arbitrariedade, é possível confundi-lo com a liberdade, confundindo também com a idealização e posituação dos direitos fundamentais (SAMPAIO, 1998, p. 34).

No estudo do direito à intimidade e à vida privada pode-se encontrar o estudo da própria independência do homem em face do Estado. Isso porque o domínio da privacidade não está submetido ao controle público, de acordo com o Mestre Oliveira Ascensão (1998). Sendo assim, a partir do momento em que se passa a tratá-lo como o direito de decisão livre, o mesmo adquire o status de direito *privatus*, isto é, refere-se ao que é exterior ao Estado, visto que pertence à pessoa ou ao indivíduo.

Nesse sentido, é coerente destacar que o direito à vida privada deve considerar a necessidade da autonomia do sujeito social, o que significa poder decidir sobre assuntos de foro íntimo e mantê-los em segredo, assim como ter garantias de que sua casa e suas correspondências não serão violadas.

1.3 O DIREITO À VIDA PRIVADA

Em princípio, é relevante salientar que a vida privada, como sendo um direito legítimo, é decorrente da personalidade, portanto, participa do direito à vida, constituindo-se em tema de importância atual, visto que há uma crescente preocupação em conseguir maior proteção e efetividade em relação aos direitos individuais.

Assim, é importante colocar que em função de todos os direitos estarem relacionados ao direito à vida, é relevante ter em mente que a Carta Magna atribui a tais direitos, especial atenção jurídica, determinando sua primordialidade nas relações sociais.

Segundo Silva (2011),

(...) a vida humana, que é o objeto do direito assegurado no art. 5º, caput, da Constituição Federal de 1988, integra-se de elementos materiais (físicos e psíquicos) e imateriais (espirituais). Isso faz com que a vida tenha intimidade conosco mesmo (caracterizado no dar-se conta de si mesma, no assistir a si mesma e no tomar posição sobre si mesma). Por isso, a vida humana constitui a fonte primária de todos os outros bens jurídicos. No conteúdo do seu conceito encontra-se o direito à existência, à dignidade da pessoa humana, ao respeito, à integridade físico-corporal e moral, e à privacidade (SILVA, 2011, p. 198).

Somam-se a estas palavras, os ensinamentos de Silva (2011) quando ele lança mão da expressão “direito à privacidade” em sentido amplo, pois, de acordo com o autor, engloba todas as manifestações de âmbito íntimo, da personalidade e da vida privada.

Assim, pode-se definir privacidade como um

(...) conjunto de informações sobre o indivíduo, o qual pode ele decidir manter sob seu exclusivo controle, ou pode comunicar, restando a ele decidir a quem, quando, onde e em que condições isso será feito. Portanto, a esfera de inviolabilidade tem caráter amplo, abrangendo o ponto de vista doméstico, relações familiares e afetivas em geral, assim como fatos, hábitos, localização, identificação pessoal, imagem, segredos, e, inclusive, as origens e planos futuros do indivíduo (SILVA, 2009, pg. 206).

Esse seria o traço característico da tutela à privacidade das pessoas, em seu sentido essencial. De acordo com Bittar (2004), é necessário garantir a supressão de qualquer atentado a perspectivas particulares ou íntimas da pessoa, o que

compreende o lar, a família e a correspondência e, em determinados casos, inclusive o patrimônio.

O direito à vida privada, como espécie dos direitos da personalidade, requer a compreensão destes. Dessa forma, a hermenêutica acerca dos direitos da personalidade se mostra essencial para que se legitime o que o Código Civil, em concomitância com a Constituição Federal, determina: a garantia de proteção da vida privada e da intimidade da pessoa, dando veracidade à condição de inviolabilidade, permitindo a qualquer pessoa que estejam disponíveis os dispositivos legais adequados de defesa e proteção de sua privacidade e de sua intimidade (BARROS, 2009).

1.4 O DIREITO À HONRA

Há doutrinadores que encontram no direito à honra a origem do direito à intimidade e à vida privada (SAMPAIO, 1998). Conforme os ensinamentos do Mestre Oliveira Ascensão:

A dignidade da pessoa humana implica no fato de que a cada homem sejam atribuídos direitos, por ela justificados e impostos, que assegurem esta dignidade na vida social. Esses direitos, portanto, devem representar um mínimo, que crie o espaço no qual cada homem poderá desenvolver sua personalidade. Mas devem representar também um máximo, pela intensidade da tutela que recebem (ASCENSÃO, 1998, p. 64).

No direito da personalidade a pessoa é o fundamento e o fim do direito sendo assim, pois, defendida a reserva sobre a intimidade da vida privada como fator essencial ao desenvolvimento da personalidade humana.

Dessa maneira, partindo da noção de que a personalidade humana é inviolável é que inicia a construção do direito à intimidade, podendo definir seus aspectos particulares e revelando-o como um direito autônomo.

Destarte, pode-se afirmar que o direito à honra, à reputação ou consideração social, abrange a honra externa ou objetiva e a honra interna ou subjetiva, constituindo-se num direito de personalidade. Isso está atrelado ao âmbito do direito civil e, devido ao fato de ter sido disposto pela Constituição Federal (inciso X, do art. 5º, CF), como sendo inerente aos direitos fundamentais, há a exigência de sua observância diante de casos particulares e também diante da esfera pública (MARQUES, 2010).

Posto assim, deve-se observar que a honra se refere à dignidade da pessoa, por isso tem um caráter subjetivo, mas igualmente a todos os outros direitos fundamentais, como a privacidade, a vida privada e a intimidade, o direito à honra é protegido pelo artigo 220 da Constituição Federal do Brasil.

2 O DIREITO DIANTE DA SOCIEDADE TECNOLÓGICA

É indiscutível que os avanços tecnológicos no campo da intercomunicação têm possibilitado a propagação e o compartilhamento de informações de forma muito rápida e ampla, de modo que é possível vislumbrar hoje uma sociedade informacional e globalizada. Tal fato certamente contribui para a consolidação do conhecimento, além do fato de promover o estreitamento das relações entre as pessoas.

No entanto, o que se percebe é que estas novas tecnologias, como é o caso da Internet, vêm acarretando sérios problemas a um número elevado de usuários da rede, visto que certos direitos legítimos das pessoas, como o direito à privacidade e à intimidade, estão sendo violados por criminosos virtuais que se enaltecem por considerar que estão imunes à Justiça (LIRA, 2014).

Dessa forma, surge um ambiente tomado pela insegurança e pela incerteza por parte de todos aqueles que estão conectados a esta sociedade da informação, visto que são vítimas em potencial de criminosos que conhecem a “rede” muito mais profundamente que a grande maioria dos usuários.

Em decorrência disso, é fundamental que o Direito esteja em consonância com as novas perspectivas sociojurídicas que se apresentam diante dessa sociedade digital.

É inerente ao Direito, como ciência adaptável às transformações sociais, mostrar preocupação em relação às mudanças trazidas pela “virtualização” do cotidiano social. É claro que não poderia ser diferente, visto que a realidade informática/virtual se impõe de maneira imperativa, como acontece nas revoluções. A tecnologia transpõe os preconceitos e os temores, estabelecendo-se de forma independente da adesão de seus destinatários (PIMENTEL, 2000, p.139).

Diante disso, é fundamental dialogar com Auriney Brito (2013) quando o mesmo afirma que

(...) o Direito Penal na Sociedade da Informação “não sugere um novo direito, mas o estudo do Direito clássico, que vigora sob a influência dos conflitos sociais fomentados, incrementados ou criados na sociedade da informação (BRITO, 2013, p. 26).

Por isso, é imprescindível ter em consideração que a análise da dinâmica social pós-moderna, deve passar pelo crivo de que a evolução indiscriminada

decorrente da globalização, certamente deu origem a riscos sociais provenientes das novas formas de relacionamento entre os cidadãos.

Dessa forma, é possível observar que, apesar de a Internet se apresentar como uma ferramenta essencial o desenvolvimento econômico e cultural da sociedade, a mesma se tornou responsável pelo estabelecimento de novos modelos de relacionamentos sociais, os quais têm possibilitado o surgimento de novos conflitos e, conseqüentemente, de uma nova zona criminológica.

Conforme Moraes (2007), é preciso considerar que os novos riscos oriundos da era da informática passaram a provocar conflitos ignorados pelo Direito. Devido a isso, apresenta-se urgente a tomada de novas providências, as quais devem estar voltadas não apenas para a proteção de bens jurídicos clássicos e palpáveis, como a vida e o patrimônio dos cidadãos, mas também observando a subjetividade dos direitos fundamentais inerentes à personalidade.

Nesse sentido, Alexandre de Moraes (2004) acrescenta a importância de se buscar a proteção dos direitos fundamentais junto ao poder judiciário, quando estes são violados:

A constitucionalização dos direitos humanos fundamentais não significa mera enunciação formal de princípios, mas a plena positivação de direitos, com base nos quais qualquer indivíduo poderá exigir sua tutela perante o Poder Judiciário, para a concretização da democracia. É absolutamente indispensável a garantia de proteção jurídica, de modo a se tornar efetiva a aplicação e o respeito aos direitos humanos fundamentais previstos na Constituição Federal e no ordenamento jurídico, de modo genérico (MORAES, 2004, p. 99).

Sobre isso, é importante destacar que Auriney Brito (2013) considera o surgimento da sociedade da informação, como uma possibilidade de riscos e incertezas, que aumentam, visto que a utilização da rede mundial de computadores, por parte da população mundial, tem crescido de forma vertiginosa.

Dessa forma é exigível que sejam tomadas atitudes de proteção por parte do Estado, o qual certamente tem recebido um número de demandas criminais cada vez mais crescentes. Por isso, torna-se essencial a ampliação do horizonte de proteção do Direito Penal aos usuários do sistema de informação globalizado.

A este contexto podem ser acrescentadas as palavras da professora Ivette Senise Ferreira, quando a mesma afirma que:

O crescimento da informatização das várias atividades desenvolvidas de maneira individual ou coletiva na sociedade trouxe instrumentos novos para as mãos dos criminosos. Este alcance ainda não foi corretamente avaliado,

pois surgem cotidianamente novas modalidades que lesam os mais variados bens e interesses, cuja tutela é incumbida ao Estado, possibilitando a formação de uma criminalidade específica da informática, cuja tendência é aumentar quantitativamente e, qualitativamente, aperfeiçoar os seus métodos de execução (FERREIRA, 2000, p. 207).

Na esteira destas reflexões, Zygmunt Bauman (2008) considera que a sociedade se tornou desprotegida em decorrência dos avanços da tecnologia, visto que esse contexto deu origem a riscos, incertezas e à prática de crimes. Com isso surgiu a “sociedade da incerteza”, na qual novos perigos são descobertos e anunciados cotidianamente, tornando as pessoas vulneráveis a riscos que nem podem prever.

Assim, é possível considerar que:

Como na Sociedade da Informação a internet representa um importante meio de comunicação, os relacionamentos que exercitam outras liberdades, ou a livre-iniciativa devem estar devida e juridicamente resguardados. O Direito agora não se resume mais ao acesso à internet, mas principalmente, ao acesso a uma internet segura. (BRITO, 2013, p. 43).

Conforme Gonçalves (2013, p. 46), “a privacidade pode ser considerada como um dos bens da vida mais importantes ao ser humano, uma vez que, sem ela, o homem expõe-se de modo a violar a sua própria personalidade”. Assim, é lógico afirmar que nem tudo que o homem pensa, deve ser compartilhado.

Logo, é coerente colocar que a partir dos avanços da tecnologia e da difusão de informação, é possível perceber que a sociedade pós-moderna tem se apresentado vulnerável, visto que ninguém escapa à vigilância e à privacidade.

Dessa forma, as palavras de Gonçalves (2013), permitem aludir à ideia de que nesta era digital as possibilidades de proteção dos direitos fundamentais dos indivíduos, como a vida privada e a intimidade, estão em situação frágil. Isso pode ser percebido a partir dos meios de informatização, os quais constituem a sociedade da informação, e esta exerce um forte poder sobre os indivíduos, passando a controlar a vida dos indivíduos e deixando os seus dados e informações vulneráveis e à mercê de criminosos virtuais.

Também é importante observar que uma das bases constituintes da formação da Sociedade Informacional existente hoje, é certamente, o desenvolvimento acelerado das telecomunicações. Sobre isso, Eduardo Capellari (2000) assegura que:

A sociedade de informação (...) é resultado do crescimento de investimentos nas tecnologias de informação – destaque-se recentemente a rede mundial

de computadores – os quais originam uma nova divisão social do trabalho e constituem, por conseguinte, uma nova sociedade (CAPELLARI, 2000, p.39).

Considerando as reflexões do referido autor, é possível afirmar que a informação tornou-se a mola propulsora de transformação da sociedade pós-moderna, visto que a combinação de satélites, televisão, telefone, fibra ótica e microcomputador aproximou o mundo, e derivou disso um sistema unificado de conhecimento que

(...) supera as estruturas administrativas hierarquizadas e verticalizadas, direcionado-as de forma horizontal quanto às relações de poder, que tem na figura da rede, propriamente, a expressão da nova realidade” (CAPELLARI, 2000, p.39).

Pode-se, portanto, observar que surge uma nova era, a qual tem provocado a ruptura das barreiras territoriais, devido à minimização do tempo de processamento de volumes inacreditáveis de informações. Esta é, portanto, “a era informacional ou a era digital, em que sociedade internacional tem a possibilidade de “navegar” em outra dimensão: a do ciberespaço” (VALLE, 2005, p.18).

Neste íterim, é importante observar que o indivíduo pertencente a esta sociedade da informação e que se encontra conectado a este ciberespaço, está cada vez mais dependente das comodidades e facilidades que os meios de intercomunicação globalizada permitem.

Vendo por outro prisma, não seria um disparate afirmar que essa comodidade oferecida pela sociedade da informação, ao mesmo tempo em que traz benefícios diversos, também se torna uma fonte de riscos, deixando os usuários dos meios digitais de informação expostos aos “olhos” dessa sociedade.

A esse respeito, Stefano Rodotà (2008) faz uma reflexão interessante ao afirmar que:

Assediados por computadores, espiados por olhos furtivos, filmados por telecâmeras invisíveis, os cidadãos da sociedade da informação correm o risco de parecerem homens de vidro: uma sociedade que a informática e a telemática estão tornando totalmente transparente. (RODOTÀ, 2008, p. 4).

Esta transparência de que o autor fala, pode se referir à falta de segurança que os usuários da era digital experimentam, quer estejam conscientes disso, quer sejam realmente ignorantes sobre os riscos oferecidos pelo sistema. Na verdade, o que importa é que neste contexto social o direito à privacidade está sendo violado,

fazendo com que os dados pessoais dos usuários sejam coletados, estimulando a prática dos crimes digitais.

Assim, é coerente afirmar que a sociedade pós-moderna vêm avançando muito em termos tecnológicos, visto que se vive o momento da criação de um ambiente eletrônico, computacional e virtual.

No entanto, pode-se perceber que, se de um lado há o desenvolvimento dos meios de comunicação, por outro lado, esses mesmos meios podem contribuir para a insegurança do meio digital. Emerge daí a urgência em se modernizar a legislação penal brasileira no tocante à segurança digital.

2.1 PRINCÍPIO DA SEGURANÇA DA INFORMAÇÃO: ELEMENTOS PARA A PROTEÇÃO JURÍDICA

De acordo com Patrícia Peck Pinheiro (2013, p. 311) “o maior estímulo aos crimes virtuais é dado pela crença de que o meio digital é um ambiente marginal, um submundo em que a ilegalidade impera”. Tais impressões corroboram com as ideias de Rodotà (2008), quando este alude à transparência a que a era digital expôs os indivíduos conectados na sociedade da informação.

É nesse sentido que o Direito deve se aperfeiçoar, visto que no contexto em que o usuários dos sistemas de informação se encontram, “o direito digital obriga toda corte que atua no processo judiciário: juízes, procuradores, advogados, delegados, investigadores, peritos e demais, a realizar uma atualização tecnológica” (LIRA, 2014, p. 29).

Esta atualização é, portanto, necessária para que seja atingido um patamar de uma sociedade digital mais segura. E se isso não acontecer, é provável que o ordenamento jurídico, ao invés de proteger os cidadãos e cuidar da legitimação de seus direitos, estará prejudicando estes cidadãos e colocando a sociedade em risco.

Posto isso, é coerente afirmar que a existência de um conjunto de normas e de sanções no mundo digital, que seja capaz de abarcar os mais variados tipos de delitos decorrentes do uso da rede de computadores, se apresenta como algo primordial e, caso o Estado não seja eficaz ao punir os criminosos cibernéticos, poderá se assistir a um retrocesso das relações e dos negócios virtuais, em virtude da insegurança dos ambientes virtuais.

Neste diapasão, Spencer Toth Sydow (2013) assevera que:

(...) o fenômeno da modernização (científica e tecnológica) traz para a sociedade transformações, grande parte das vezes de proporções muito superiores à capacidade de adaptação e de controle jurídico (SYDOW, 2013, p. 53).

Assim, é possível inferir que, se por um lado a modernização é aparentemente vantajosa por trazer a maximização de valores, por outro lado, certamente, há o fenômeno do descontrole da harmonia social. Esse fenômeno, a cada violação dos direitos fundamentais do indivíduo, vai gerando conflitos entre as pessoas e, com isso, dá-se início à criação de novos riscos, os quais precisam ser previstos e tratados à luz de uma legislação penal digital séria e voltada para a solução dos embates decorrentes do mau uso da tecnologia.

Isso se justifica pelo fato de que:

A sociedade informática, pois, deve ainda ser vista como uma sociedade de risco *sui generis*, uma vez que, além dos riscos previsíveis, controláveis e mitigáveis da sociedade comum, ainda possui a variante da gigantesca capacidade de mudança inerente à tecnologia da informação. (SYDOW, 2013, p. 53).

A esse respeito, as reflexões de Sydow (2003) coadunam com as palavras de Alamiro Velludo Salvador Neto, quando ele expõe que na sociedade de risco

(...) o legislador tipifica criminalmente as mais diversas e pensáveis condutas como apelo à voz de cidadãos inseguros. O aplicador utiliza-se irrefutavelmente deste mesmo e incessante apelo para subsumir aqueles tipos de modo severo sem qualquer comprometimento com os âmbitos de proteção estabelecidos através dos instrumentos coerentes da dogmática penal. E o jurista, por sua vez, corre desesperadamente atrás de um entendimento possível da calamitosa situação, na busca da construção de um sistema razoável para o Direito Penal da modernidade. Eis aí o fenômeno da sociedade de risco. (SALVADOR NETO, 2006, p.85).

Assim, é possível depreender que nesta sociedade de risco, os indivíduos que utilizam os meios digitais de comunicação, estão propensos a terem seus direitos constitucionais violados e sem a certeza de que os danos sofridos serão ressarcidos de alguma forma. Para que isso não se torne uma realidade calamitosa, é tempo de o Direito Penal ser repensado, com vistas a compreender e atuar positivamente diante desta nova forma de interação social, pautada na informatização.

Neste contexto, é interessante destacar que, devido a estes avanços tecnológicos, os conceitos como soberania, território, tempo e espaço acabam por perder o sentido e, justamente por isso, a sociedade necessita de uma tutela penal que abarque esse novo bem jurídico: a “Segurança Informática” (SYDOW, 2003).

Então, usando as palavras de Sydow (2013, p. 70), pode-se entender, atualmente, que por segurança “compreende-se a condição de algo ou alguém encontrar-se livre de perigo, perdas ou proteção”. Por isso, é fundamental que se proceda a uma revisão e reformulação da legislação penal brasileira, com o intuito de rever o termo “segurança”, buscando compreender mais minuciosamente os riscos *sui generis* que a sociedade da informação oferece aos seus usuários.

Esta a condição *sine qua non* é possível lidar com estes novos delitos de maneira mais adequada e eficaz. Por isso, é essencial que esta deficiência da Legislação penal brasileira seja combatida, de modo a prevenir a ocorrência destes crimes violadores da subjetividade do cidadão.

Dessa forma, para iniciar uma análise do tema em questão, é relevante colocar em discussão os fatores que contribuem para a existência desta realidade. Dentre tais fatores podem ser apontados o despreparo da Legislação brasileira para lidar satisfatoriamente com estes casos e a falta de informação dos usuários da rede a respeito das políticas de proteção deles mesmos (LIRA, 2014).

Em relação ao primeiro fator citado, pode-se afirmar que os crimes virtuais parecem estar se tornando comuns no Brasil. Isso vem ocorrendo em virtude de vários fatores, entre eles podem ser citados: a morosidade do poder legislativo em tipificar essas modalidades de crimes e o despreparo dos legisladores diante de tais delitos. Tal fato tem dado origem a uma atmosfera de “terra sem lei” na Internet.

Deve-se considerar que as práticas ilícitas cometidas por pessoas de má fé, que usam a Internet para invadir a vida privada dos outros para benefício próprio, parecem decorrer de oportunidades que os próprios usuários dão àqueles que já têm a intenção de cometer um crime cibernético (LIRA, 2014).

Assim, certos direitos fundamentais do indivíduo estão sendo violados com a prática de modismos, como os sites de relacionamentos sociais, os quais abrem ao público, fatos e informações que deveriam ficar em sigilo.

É provável que isso ocorra porque nem sempre as pessoas têm conhecimento ou não têm noção dos malefícios que o uso indiscriminado da tecnologia pode acarretar em suas vidas. De acordo com Costa (2011), um exemplo disso é que, por meio desses sites de relacionamento, é possível saber de coisas consideradas pessoais e que, então são tornadas públicas, tornando o usuário da rede vulnerável ao ataque de criminosos virtuais.

Portanto, parece ser coerente afirmar que os usuários da Internet também devem procurar se informar melhor sobre as formas de ele mesmo se proteger eletronicamente, evitando que seus dados pessoais e informações sobre sua intimidade não sejam coletados com tanta facilidade pelos criminosos virtuais.

É fato que a modernidade requer do Direito uma atenção especial às mudanças e transformações sociais, particularmente, as que se relacionam com o ramo da informática, visto que este se encontra em pleno desenvolvimento, mas também é fundamental que o cidadão se mantenha informado sobre as formas de proteção no ambiente da Internet.

Entretanto, Gatto (2011) alerta que, em meio a essa onda digital de informações, tornou-se possível o armazenamento de dados industriais e individuais, dados relativos a contas bancárias, números de cartões de crédito, senhas de acesso, trocas de experiências interpessoais, criação e difusão do comércio eletrônico e, conseqüentemente, certo comodismo, deixando o usuário vulnerável a ataques virtuais criminosos.

2.2 A TUTELA DE PROTEÇÃO DIGITAL

Diante do cenário de exposição e insegurança sugerido pela sociedade da informação, é importante destacar o que a Constituição Federal brasileira determina a respeito:

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

(...)

XXXV - a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito (BRASIL, 1988).

Assim, em face do que a Carta Magna determina, é garantido a todas as pessoas que residem em território brasileiro, quando estas se sentirem violadas em relação a qualquer direito fundamental, que procurem a Justiça, pois todos têm o direito de acessar uma atividade jurisdicional do Estado, assim como o direito a uma adequada resposta do Poder Judiciário.

É importante salientar, a esse respeito, que a Constituição é taxativa quando estabelece que o direito de acesso ao Poder Judiciário, com a finalidade de requerer

não apenas a tutela jurisdicional em face da violação de direito, mas também em virtude da ameaça de sua violação.

Em referência a essa tutela jurídica imposta pela Constituição Federal do Brasil, deve-se refletir que

(...) o dispositivo constitucional garante não apenas um devido processo legal tendente a uma tutela jurisdicional repressiva, atuada após o direito ser violado, com o fim de reparar os danos causados ou a sua reintegração, mas também, o acesso a um processo que visa evitar a violação do direito, ou seja, uma tutela jurídica preventiva, que haja enquanto ainda existe apenas a ameaça de violação do direito e não a sua consumação (MALTINTI, 2008, p. 179).

Portanto, é coerente afirmar que o Estado-juiz deve estar preparado para atuar antes da ocorrência da prática da lesão, a partir da adoção de medidas que impeçam que o criminoso concretize sua ação ou a continue. Isso é um tratamento jurídico em termos de tutela cautelar e tutela antecipada (THEODORO JR., 2014).

A legitimação desta tutela jurídica aos usuários das mídias digitais é fundamental, pois a sociedade da informação funciona, basicamente, por meio da Internet. Por isso, é preciso que tais indivíduos estejam a par de que

(...) a internet proporcionou conflitos capazes de atingir dimensões imprevisíveis: por um lado, existe o direito à liberdade de informação e de imprensa, garantidos pela Constituição Federal de 1988, que é um direito fundamental do homem e serve como referência de todas as liberdades reconhecidas na Carta das Nações Unidas, o que garante a livre expressão do pensamento, da atividade intelectual, artística, científica, etc. Por outro lado, existe o direito à intimidade, à vida privada, à honra e à imagem, também assegurado pela mesma Constituição Federal de 1998 (TOMIZAWA, 2008, p. 18).

Conforme o autor, esse conflito ocorre no instante em que o mercado é capacitado por esta era da informação a rastrear a vida das pessoas, a conhecer os hábitos e preferências destas, assim como conhecer também suas finanças, suas posses, o que gosta de comprar, enfim, o mercado passa a saber muito sobre a vida do cidadãos e, por isso podem criar um banco de dados que possibilita o envio de propagandas e afins.

Então, o mercado, passa a agir unilateralmente, isto é, não considera que o usuário não autorizou esta coleta de dados e, portanto, o mercado passa a violar direitos fundamentais do indivíduo, não o deixando em paz.

Soma-se a isso, o fato de que nesta sociedade digital insegura, o usuário da rede também está exposto e vulnerável a ataques de criminosos cibernéticos, cujo intuito é o lesar os direitos que são legitimados pelo Estado.

A esse respeito, Guilherme Tomizawa alerta que

(...) observa-se, cotidianamente, que no meio navegável eletrônico, são livremente veiculados dados pessoais, propagandas ou imagens não autorizadas, o que pode denegrir e macular a intimidade e a vida privada de outrem (TOMIZAWA, 2008, p. 19).

Nesse contexto, diante das mudanças provocadas pela Sociedade da Informação, é urgente que direito regule as novas relações jurídicas advinda desse processo, de modo que haja eficiência jurídica no que tange às novas exigências e necessidades do ser humano moderno.

Fundamentando-se na análise empírica dos crimes mais comuns que se relacionam ao uso de novas tecnologias, Sydow (2003) relata que é possível limitar os componentes que tornam o sistema informático inseguro. A esse respeito, o Preâmbulo da Convenção de Budapeste acerca de *Cibercrime* e o Comitê Gestor da Internet no Brasil, salientam a imprescindibilidade de se considerar os três pilares ou princípios da proteção jurídica diante desses casos:

Convictos de que a presente Convenção é necessária para impedir os atos praticados contra a **confidencialidade, integridade e disponibilidade de sistemas informáticos**, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados, assegurando a incriminalização desses comportamentos tal como descritos na presente Convenção, e da adoção de poderes suficientes para combater eficazmente essas infrações, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infrações, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável. (SYDOW, 2013, p. 70, grifo nosso).

Diante destas reflexões é importante que o Estado possa atuar de maneira transparente e eficaz, resguardando os princípios da segurança da informação, que também são chamados de elementos da proteção jurídica.

Ainda, de acordo com Sydow (2013), estes elementos são: a) confidencialidade – garantia de que seus dados e informações, armazenadas em dispositivos de comunicação, não serão violados por outrem; b) integridade – compreendida como a incolumidade de dados ou informações na origem, no trânsito ou no destino; c) disponibilidade – refere-se à facilidade de recuperação ou acessibilidade de dados e informações.

Diante do que foi explanado acerca da necessidade de uma revisão urgente dos pressupostos legais relacionados aos crimes oriundos desta sociedade da informação, no capítulo que segue será apresentada uma análise do conteúdo da Lei n. 12.737/12, conhecida como a Lei Carolina Dieckmann, na qual se pretende observar de que forma a referida lei garante o tratamento jurídico adequado em face dos delitos virtuais.

3 CRIMES CIBERNÉTICOS: ANÁLISE DOS CONCEITOS E PRESSUPOSTOS LEGAIS DIANTE DA LEI CAROLINA DIECKMANN – LEI Nº 12.737/2012

Em conformidade com o Superior Tribunal de Justiça (STJ)², devido à universalização da Internet, os “crimes contra a honra (injúria, calúnia e difamação), furtos, extorsão, ameaças, violação de direitos autorais, pedofilia, estelionato, fraudes com cartão de crédito, desvio de dinheiro de contas bancárias”, têm aumentado paulatinamente.

Conforme Gimenez (2013), o Direito Penal vem se deparando com muitos percalços para se adaptar a este contexto, visto que este ramo do Direito não consegue lidar adequadamente com esta nova realidade social e acompanhar o gradativo e rápido avanço das novas tecnologias.

Neste ambiente livre e absolutamente sem fronteiras se desenvolveu uma nova forma de crimes, ordinariamente denominada de criminalidade virtual, a qual é fomentada por agentes delituosos que se valem do aparente anonimato e também da não existência de regras na rede mundial de computadores (GIMENEZ, 2013).

A esse respeito, é fundamental considerar que o Direito se deparou com uma nova realidade, decorrente dos avanços tecnológicos que tornaram a comunicação entre as pessoas muito mais rápida e eficiente, constituindo um ciberespaço, no qual o índice de crimes tem crescido paulatinamente, enquanto o Direito se encontra estagnado ou caminhando a passos muito lentos para dar conta de estar preparado para enfrentar as lides cibernéticas.

Tal realidade virtual se apresenta completamente distinta da realidade do mundo físico regulamentado pelo ordenamento jurídico brasileiro vigente. Desse modo, é coerente observar que emerge desse cenário social informatizado, a necessidade de se voltar os olhares para uma nova realidade jurídica (PINTO, 2001). Isso é pertinente devido ao fato de que a incidência de crimes cometidos em ambientes virtuais tem aumentado significativamente nos últimos tempos.

Logo, é imperativo que haja uma revisão dos dispositivos legais que versam sobre a possibilidade de crimes de natureza tecnológica, para que os usuários destes sistemas sejam amparados legalmente. Isso é coerente, pois

² Informações extraídas de: <http://stj.jusbrasil.com.br/noticias/234770/justica-usa-codigo-penal-para-combater-crime-virtual> Acesso em: 20/09/2015.

O Direito Penal é o segmento do ordenamento jurídico cuja finalidade é a de eleger os comportamentos humanos mais graves e prejudiciais à coletividade, os quais colocam em risco os valores essenciais à boa convivência social, e apontá-los como infrações penais, atribuindo-lhes as respectivas sanções, assim como estabelecer todas as regras complementares e gerais, necessárias à sua correta e justa aplicação (CAPEZ, 2011, p. 19).

Então, parece coerente afirmar que é função do Direito Penal acompanhar as dinâmicas sociais, de modo a intervir em determinado contexto delituoso para que as sanções e penas cabíveis sejam aplicadas, pois assim é possível restabelecer o bom convívio entre as pessoas, sobretudo, os usuários da Internet e dos novos produtos tecnológicos disponíveis à sociedade (GIMENEZ, 2013).

Nesse sentido, os crimes cibernéticos, informáticos, virtuais, etc., devem ser combatidos pelo Direito tanto Penal como Civil, com vistas a reparar os danos, porventura sofridos pelos usuários desses ambientes virtuais.

Assim, neste capítulo será apresentada uma análise da legislação pertinente aos crimes de natureza tecnológica elencados pela Lei Carolina Dieckmann, Lei nº 12.737/12, que trata especificamente de crimes cibernéticos que violam direitos fundamentais dos cidadãos, iniciando pela definição de crimes desta natureza, abordando os aspectos legais que são usados no tratamento destes casos e, finalmente, investigando as premissas da lei em questão.

3.1 CRIMES VIRTUAIS: CONCEITOS E PARTICULARIDADES

É possível conceituar genericamente que os crimes cibernéticos, virtuais ou informáticos são: “qualquer conduta ilegal, antiética, ou não autorizada que envolva processamento de dados e/ou transmissão de dados” (ROSA, 2002, p. 53).

Em termos mais específicos, Guimarães; Neto (2003) dividem os crimes cibernéticos como:

- a) Crime virtual puro – compreende qualquer conduta ilícita, em relação ao hardware e/ou ao software de um computador, isto é, a parte física e a parte virtual do microcomputador;
- b) Crime virtual misto – aquele que usa a Internet para se conduzir ilicitamente e, cujo objetivo é diferente do citado anteriormente. Por exemplo, podem ser citadas as transações ilegais de valores de contas correntes;

c) Crime virtual comum – é utilizar a Internet apenas como forma de instrumento para realizar um delito que se enquadra no Código Penal, como a distribuição de conteúdo pornográfico infantil por diversos meios, tais como *messengers*, *e-mail*, *torrent* ou outras formas de se compartilhar dados (GUIMARÃES; NETO, 2003, p. 67-70).

Já, nas reflexões de Vianna, os crimes cibernéticos se classificam em:

- a) crimes informáticos impróprios – aqueles nos quais o computador é utilizado para se executar o crime, porém sem ofender o bem jurídico ou a violar a informação automatizada, ou seja, os dados;
- b) crimes informáticos próprios – aqueles em que o bem jurídico protegido pela norma penal, violando as informações automatizadas (dados);
- c) delitos informáticos mistos – são crimes complexos em que, além da proteção da inviolabilidade dos dados, visam tutelar a norma do bem jurídico de natureza diversa;
- d) crimes informáticos mediatos ou indiretos – é o delito-fim de natureza não informática, herdando esta característica do delito-meio informático realizado para permitir a sua consumação (VIANNA, 2003, p. 170).

Aos ensinamentos de Guimarães; Neto (2003), os crimes denominados cibernéticos, que também são conhecidos como eletrônicos ou virtuais, são classificados conforme o modo como são praticados e que elementos físicos o infrator utiliza para tal. Já para Vianna (2013), é pertinente dividi-los em puros (ou próprios), ou impuros (ou impróprios).

Os primeiros são praticados por computador e se realizam ou se consomem também em meio eletrônico, sendo a informática o objeto jurídico tutelado; já os segundos, são aqueles em que o agente se vale do computador como meio para produzir um resultado que ofenda o mundo físico ou o espaço real, ameaçando ou lesando outros bens diversos da informática (VIANNA, 2013).

É interessante destacar que este contexto deu origem ao surgimento, de um número muito alto de casos de crimes envolvendo tecnologias de comunicação, como a Internet e, desse cenário, emergem os hackers e os crackers.

Portanto, deve-se considerar que

Os primeiros registros de crimes cibernéticos datam da década de 70, momento em que surge a figura do Hacker e do Cracker que são indivíduos com profundo conhecimento de informática, contudo o primeiro usa seus conhecimentos para melhorar a segurança de sistemas informático, enquanto o segundo busca quebrar essa segurança a fim de obter vantagens pessoais incorrendo conseqüentemente na prática de ilícitos com a realização de invasão de sistemas e furto de dados (FREITAS; SILVA, 2013, p. 5).

O histórico dos crimes cibernéticos reporta à década de 1970, quando o termo “hacker” foi definido como sendo a pessoa detentora de vastos conhecimentos

técnicos e, devido às suas habilidades, pode invadir sistemas operacionais privados e disseminar pragas virtuais.

(...) é fundamental compreender a distinção entre hacker e cracker. Em princípio, ambos são detentores de conhecimentos profundos de informática, porém o que difere os dois é a forma de utilização destes conhecimentos: ao passo que o hacker invade os sistemas computacionais para provar que há falhas a corrigir, não causando danos aos seus proprietários; já o cracker invade os computadores com o intuito de causar danos e cometer atos ilícitos, assim como se aproveitar das falhas existentes no sistema para obter vantagem indevida. Assim, o cracker cria um problema para os usuários, o hacker procura solucioná-lo (COSTA, 2011, p. 180).

Assim, a possibilidade de usar os sistemas informacionais para cometer delitos, certamente, passou das mãos de hackers e crackers para usuários menos conhecedores da área, que usam a Internet para obter vantagens sobre pessoas em particular ou de empresas, constituindo um cenário de insegurança e vulnerabilidade.

Sendo assim, para se combater e punir os delitos virtuais, deve-se considerar que a consecução desses crimes ultrapassa a disciplina disposta no ordenamento jurídico brasileiro. Dessa maneira, é imprescindível que haja uma especialização técnica nas investigações, a fim de facilitar a identificação dos agentes delituosos e compreender melhor como o crime acontece, pois assim é possível combater e punir tais criminosos.

Assim, a identificação dos criminosos virtuais é uma das tarefas mais complexas por parte das autoridades policiais, visto que os autores destas práticas, majoritariamente, são dotados de conhecimentos específicos que permitem seu anonimato por certo tempo (ROCHA, 2013).

Outro ponto importante a ser considerado é o *locus delicti*, ou lugar onde ocorre o crime, que determina o local em que o crime está sujeito à lei penal de determinado país. De acordo com Damásio de Jesus, “como cada Estado é soberano, ocorre a problemática da delimitação do espaço de ação da legislação penal” (JESUS, 2003, p. 120).

A respeito deste tema, é conveniente salientar que o Código Penal, reza em seu art. 6º a adoção da teoria da ubiquidade, a qual consiste no fato de que o território de um país pode abarcar qualquer dos momentos do crime, quer sejam os atos executórios, quer sejam os atos consumativos do delito.

Art. 6º - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado (BRASIL, 2008).

Assim, depois de esclarecido em qual território vigora a lei penal brasileira, é fundamental investigar quando nele se deve considerar cometida a infração. De acordo com Fernando Capez (2011):

No caso de um crime ser praticado em território nacional e o resultado ser produzido no estrangeiro (crimes à distância ou de espaço máximo): aplica-se a teoria da ubiquidade, prevista no art. 6º do Código Penal, isto é, o foro competente será tanto o do lugar da ação ou omissão quanto o do local em que se produziu ou deveria produzir-se o resultado (CAPEZ, 2011, p. 123).

Nessa esteira, as ideias de Capez (2011) vão ao encontro das reflexões de Jesus (2003), quando este afirma que:

(...) quando o crime se inicia em território estrangeiro e é consumado no Brasil, considera-se que o mesmo foi praticado no Brasil. Assim, aplica-se a lei penal brasileira ao fato de um indivíduo, em território boliviano, atirar na vítima que está em nosso território, vindo a falecer; assim como o caso de um estrangeiro expedir a pessoa que viva no Brasil um pacote de doces envenenados, ou uma carta injuriosa. De modo semelhante, tem eficácia a lei penal nacional quando os atos criminosos são praticados em nosso território e o resultado se produz em país estrangeiro (JESUS, 2003, p. 129).

Assim, é coerente afirmar que essas novas práticas delituosas cometidas na esfera da Internet, devem ser combatidas à luz da doutrina supracitada, com o intuito de adaptar a legislação a essa nova modalidade delituosa que se apresenta. Isso é fundamental porque o surgimento do denominado mundo virtual, rompeu com a noção de espaço, transcendendo o ambiente físico e instituindo um novo *locus delicti*, conhecido atualmente por ciberespaço.

Acerca da competência forense, faz-se necessário perceber que a problemática em torno da territorialidade da internet está no caráter internacional que a rede apresenta. É fato que na Internet as fronteiras não existem, portanto, aquilo que é publicado na “rede”, certamente estará disponível para qualquer um que tenha acesso. Por isso, é coerente questionar de que forma deve proceder o juízo competente ao analisar casos referentes aos crimes cometidos na “rede”? (ARAS, 2001)

Em função do que foi discutido, é cediço constatar que a primeira problemática instaurada no tratamento desses tipos de crimes é realmente a identificação do local em que o crime foi cometido.

3.2 OS CRIMES VIRTUAIS E A LEGISLAÇÃO APLICÁVEL

De acordo com Silveira (2015), antes do ano de 2012, devido à falta de uma legislação específica, era muito complexa a investigação dos crimes virtuais, visto que a legislação em vigor ainda estava voltada para os crimes de uma maneira genérica, ou seja, não se considerava o meio utilizado para a sua prática.

Nesse escopo, é relevante destacar que os dispositivos legais de que se dispunham e eram usados para combater e punir crimes cometidos por meio de sistemas de informática:

- a) Código Penal (CP);
- b) Estatuto da Criança e do Adolescente (Lei n. 8.069/90), o qual determina no art. 241-A que é crime:

Art. 241-A: Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente (BRASIL, 1990).

- c) A Lei dos crimes de software (ou Lei Antipirataria, Lei n. 9.609/98), o qual se refere à proteção da propriedade intelectual de programas de computador, assim como sua comercialização no País (BRASIL, 1998).
- d) A Lei de Segurança Nacional (Lei nº 7.170/83), que traz a definição sobre os crimes contra a segurança nacional e contra a ordem política e social, bem como estabelece o processo e julgamento desses casos (BRASIL, 1983).

Dessa forma, diante da não especificidade da legislação, o enfrentamento de lides desta natureza se tornava e, ainda se torna muito complexo. Isso se deve, parcialmente à falta de condições de identificar os agentes criminosos e, consequentemente, a obtenção de provas suficientes para que os mesmos sejam julgados dentro dos princípios que regem a Legislação brasileira.

Entretanto, por ocasião do mês de maio de 2012, a mídia noticiou a divulgação de imagens da intimidade da atriz Carolina Dieckmann. Tais imagens foram veiculadas em vários sites da Internet, causando uma repercussão social muito significativa. Isso abriu um campo para a edição da Lei n. 12.737, de 30 de novembro de 2012, que foi publicada no Diário Oficial em 03 de dezembro de 2012,

com *vacatio legis* de 120 (cento e vinte) dias, a qual recebeu a alcunha de “Lei Carolina Dieckmann”.

A esse respeito, Tavares (2013) reflete que a referida legislação entrou em vigor carregando em seu bojo vários pontos obscuros, os quais merecem atenção, visto que a sua aplicabilidade e sua eficiência poderão não ocorrer devido a falhas e preciosismo em excesso por parte do legislador.

Para Flávia Penido:

Muito se tem discutido sobre a Lei de Crimes praticados na Internet (Lei nº 12.737/2012), projeto do deputado federal Paulo Teixeira (PT-SP), mais conhecida como “Lei Carolina Dieckmann”. Há os que criticam a rapidez com que o projeto caminhou depois que a atriz Carolina Dieckmann teve suas fotos íntimas, que estavam arquivadas em seu computador pessoal, divulgadas na internet, partindo da afirmativa de que se tratava de um “casuísmo”; já, outros louvam a iniciativa. A verdade é que antes da Lei 12.737/2012, os especialistas da área de direito penal eletrônico afirmavam que a quase totalidade dos crimes cibernéticos já estavam previstos, havendo necessidade de se preencher os espaços em branco. Apenas o tempo poderá dizer se a lei atingiu seu objetivo (PENIDO, 2013, p. 01).

Assim, é possível afirmar, em conformidade com as ideias de Tavares (2013), que a promulgação da referida lei, mesmo apresentando lacunas ou falhas, constitui-se como um avanço por parte da legislação brasileira, pois tais delitos promovem danos e prejuízos consideráveis para as pessoas ou instituições atingidas.

Soma-se a isso, o fato de que a lei em questão se apresenta como um importante passo em direção a um tratamento jurídico coerente, em face dos delitos virtuais. E isso é primordial, pois esses crimes, majoritariamente, desrespeitam os direitos fundamentais do cidadão e violam princípios constitucionais indispensáveis para uma vida digna.

Nessa esteira, Celso Antônio Bandeira de Mello assevera que:

A violação de um princípio é muito mais séria do que a transgressão de uma norma. A desatenção ao princípio implica ofensa não apenas a um específico mandamento obrigatório, mas a todo o sistema de comandos. É a mais grave forma de ilegalidade ou inconstitucionalidade, conforme o escalão do princípio atingido, porque representa ingerência contra todo o sistema, uma espécie de subversão dos valores fundamentais e corrosão de sua estrutura mestra (MELLO, 1994, p. 451).

Assim, a Lei nº 12.737/12 se apresenta como um dispositivo legal que merece ser discutido, visto que as denúncias de crimes cibernéticos tendem a crescer, conforme aumentam os usuários.

3.3 ANÁLISE DA LEI Nº 12.737/12

Conforme publicado no Diário Oficial, em 30 de novembro de 2012, a presidenta Dilma Roussef sancionou a Lei nº 12.737/2012. A referida legislação em seu artigo 1º dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

No artigo 2º, esta lei reza que o Decreto-Lei nº 2.848, datado de 7 de dezembro de 1940 (CP), está acrescido dos artigos 154-A e 154-B, que tipificam a invasão de dispositivo informático, determinando que:

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.

Deve-se acrescentar este artigo estabelece que o indivíduo que se ocupa da produção, da oferta, da distribuição, da venda ou da difusão de dispositivos ou programas de computador, também estará incorrendo no mesmo crime definido no caput desta lei. Ainda, é fundamental destacar que se houver danos financeiros, a pena será aumentada de um sexto a um terço.

No parágrafo terceiro encontra-se determinado que:

§ 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.

Percebe-se que, de acordo com o que está definido nesta lei, o criminoso poderá ter sua pena acrescida conforme o grau de gravidade dos danos causados. Por isso, é válido destacar que:

§ 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.”

Deve-se salientar que, conforme prescrito na referida lei, há uma preocupação maior com os possíveis danos causados às autoridades governamentais.

Destaca-se também a ação penal referente ao artigo 154-B, conforme disposto na lei:

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.

A Lei em questão também modifica o Decreto-Lei nº 2.848/1940, estabelecendo o seguinte:

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.

Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial (BRASIL, 2012).

Analisando o texto da Lei Carolina Dieckmann, pode-se perceber que o art. 154-A, do Código Penal, que foi inserido através da Lei nº 12.737/12, tem o objetivo de proteger a privacidade do indivíduo em relação aos dados e informações pessoais ou profissionais que ficam armazenados em dispositivo de informática e que, de alguma maneira, teve a sua segurança violada sem que titular tenha dado autorização. Dessa forma, o novo diploma legal, além de buscar a proteção do dispositivo informático, também enseja evitar a violação do mesmo.

Assim, é coerente colocar que o art. 154-A, mesmo tendo um tom repressivo, ainda é merecedor de esclarecimentos por parte do legislador, visto que ficaram obscuros os seguintes elementos para caracterização do crime:

a) o núcleo invadir; b) dispositivo informático alheio; c) conectado ou não à rede de computadores; d) mediante violação indevida de mecanismo de segurança; e) com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo; f) ou instalar vulnerabilidades para obter vantagem ilícita (DIWAN, 2015, p. 2).

Isso é relevante, pois o crime de invasão pode ser classificado, de acordo com os ensinamentos de Fernando Capéz (2011, p. 286-292), como: a) delito comum, visto que pode ser praticado por qualquer indivíduo; b) plurissubsistente, pois se consome por meio de vários atos; c) comissivo, uma vez que é decorrente da prática de “instalar”, “invadir”, configurando uma ação; d) formal, porque a consumação independe de resultado; e) instantâneo, haja vista que sua ocorrência se dá concomitante ao momento da violação do dispositivo.

Deve-se observar que, para a caracterização das condutas definidas no tipo penal em estudo, é seguro afirmar que há o dolo, com o fim específico de agir na intenção de obter, adulterar ou destruir dados ou informações pertencentes a outrem. De acordo com Diwan (2015), é preciso observar que o dispositivo de informática deve dispor de mecanismo de segurança, pois constatando a ausência do mesmo, ou o não acionamento deste, surge o impedimento da configuração do tipo penal.

Contudo, é de se questionar que, se o dispositivo de informática não dotado de algum mecanismo de segurança também vai encontrar proteção jurídica nesta nova Lei. Isso se justifica pelo fato de que o legislador se referiu expressamente aos aparelhos digitais que contenham softwares de antivírus, de firewall, de senhas e de outras defesas no campo digital (DIWAN, 2015).

Deve-se considerar também o § 1º do referido artigo, no qual há uma equiparação da conduta do agente responsável pela produção, oferta, distribuição, venda ou difusão de dispositivo ou programa de computador, à conduta do agente invasor. Com isso, percebe-se a busca pela sanção da conduta do agente que desenvolve, difunde, distribui de forma gratuita ou onerosa o software malicioso ou vídeos com imagens e informações sigilosas e de foro íntimo de outras pessoas.

Já o § 2º do art. 154-A, determinou o aumento da pena do delito de 1/6 a 1/3, caso a invasão ao equipamento informático provoque prejuízo econômico à vítima. Com isso, a Lei pune, com mais severidade, quando a prática delituosa atingir a esfera patrimonial.

Em relação ao § 3º do mesmo artigo dispõe que, caso a invasão resultar na obtenção de conteúdo de comunicações eletrônicas privadas, contendo segredos comerciais ou industriais e informações sigilosas, assim definidas em Lei, bem como o controle remoto não autorizado do dispositivo invadido, a pena será a de reclusão, de seis meses a dois anos, e multa; isso se a conduta não representar maior gravidade criminal (DIWAN, 2015).

Ressalta-se que a intenção do legislador foi a de punir com eficácia o agente capaz de controlar de forma remota o dispositivo informático, assim como quando o mesmo consegue obter conteúdo de comunicação eletrônica privada, segredo comercial ou industrial e informações sigilosas. Portanto, faz-se necessário destacar que é irrelevante quando se tratar de segredo temporário.

O § 4º, por sua vez, prevê o aumento da pena nos casos em que as informações que foram obtidas por meio das ações previstas no § 3º forem divulgadas, transmitidas a terceiros ou comercializadas.

É importante salientar que a Ação Penal é prevista no Art. 154-B, quando traz em seu bojo que a regra estabelecida é a da ação penal pública condicionada, exceto quando se tratar de crime praticado contra a administração pública direta ou indireta dos poderes da União, Distrito Federal, Estados ou Municípios, além de empresas concessionárias de serviços de caráter público. Ainda, pelas pessoas citadas no § 5º, ocasião em que excepcionalmente será ação penal pública incondicionada (DIWAN, 2015).

É válido ressaltar que a Lei dos Crimes Cibernéticos deu amplitude à redação do art. 266 do Código Penal, intitulado de “Crimes Contra a Incolumidade Pública”, quando aborda a interrupção ou perturbação de serviço telegráfico, informático, telefônico, telemático ou de informação útil ao público.

Sendo que tal alteração se explica a partir da inserção do § 1º, a qual infere que incorre na mesma pena do caput o indivíduo que interromper serviço telemático ou de informação de utilidade pública, ou ainda, impedir ou dificultar o restabelecimento destes serviços (BITENCOURT, 2012).

Deve-se acrescentar, de acordo com Diwan (2015) que é possível entender por serviço telemático como sendo a união dos serviços de telecomunicações e informática, isto é, referem-se ao serviço realizado por operadoras com o intuito de transmitir informações digitais; no entanto, os serviços de informação de utilidade

pública podem ser compreendidos como os que estão à disposição dos cidadãos por meio da telefonia, informática, telegrafia e telemática.

Para Bitencourt (2012), a referida lei trouxe acréscimo do parágrafo único ao artigo 298, do Código Penal (CP), quando equipara o cartão de crédito ou débito a documento particular. Esta nova redação, ao fazer isso, demonstra um avanço importante, visto que tem a intenção de evitar danos patrimoniais provocados pelo uso inadequado das novas tecnologias.

De acordo com Oliveira (2012), a lei tem pena bastante branda no que se refere à pena máxima, o que termina por limitar o poder do julgador, visto que existem casos nos quais a extensão pode ser muito grande e com a pena máxima em até um ano. Além disso, caberão muitas benevolências trazidas lei penal, como o regime aberto, transação penal, entre outros. Além disso, é possível o não cabimento de prisão preventiva ou temporária.

Posto assim, é possível afirmar que a entrada em vigor da Lei nº 12.737/12, a Lei Carolina Dieckmann, mesmo apresentando lacunas que merecem e precisam ser preenchidas coerentemente, traz consigo uma forma de evolução da legislação brasileira. Isso porque trata de um tema contemporâneo à nossa sociedade e, por isso, se apresenta hábil para complementar os dispositivos jurídicos existentes, podendo tornar o ordenamento legal pátrio mais condizente com as necessidades jurídicas decorrentes das novas relações que se estabelecem e dos problemas que surgem com a disseminação e legitimação de uma sociedade informatizada.

CONCLUSÃO

Os estudos realizados para a elaboração desta monografia possibilitaram observar e conhecer diversos pormenores relacionados aos direitos fundamentais de uma pessoa, como o direito à honra, à privacidade, à preservação da imagem e da intimidade. Ressalta-se que estes direitos são essenciais para que haja uma vida harmoniosa entre os sujeitos sociais.

Assim, é urgente e necessário disciplinar as inúmeras situações que podem decorrer do mau uso da tecnologia de comunicação, em especial a Internet. Isso porque, para que sejam solucionadas questões referentes à proteção de dados, nem sempre será possível a aplicação analógica das normas que agora existem como, por exemplo, do contrato eletrônico, comércio eletrônico, documento eletrônico etc. Por isso, é urgente que o legislador se preocupar com a segurança jurídica das relações virtuais.

Pode-se argumentar que há a Lei nº 12.737/2012, a qual regulamenta os crimes cibernéticos propriamente ditos. No entanto, os estudos realizados demonstram que esta lei apresenta diversas deficiências e confrontos com os sistemas penal e processual penal em voga. Tal afirmação é coerente, pois os crimes cibernéticos são a porta de entrada para outras condutas criminosas, o que facilita o uso do computador como instrumento para cometer vários delitos.

Destaca-se que o legislador não contemplou na referida lei, a invasão de sistemas, visto que optou por restringir o objeto material àquilo que denominou dispositivo informático, mas não o define, deixando lacunas para interpretações inadequadas.

Ainda, é importante salientar que, além de se perceber as imperfeições na redação dos tipos penais, é fato que as penas imputadas na nova lei são ínfimas, pois se for considerada a real gravidade das condutas incriminadas, as punições constantes no referido texto legal, não punem o infrator com nenhum rigor. Portanto, isso pode levar à criação de uma atmosfera de impunidade, que só aumentará o número de casos desta natureza.

Em suma, os tipos e penas da Lei nº 12.737/2012 não são eficientes para dar as respostas que a Sociedade espera e precisa, nem para desestimular aqueles que têm o intuito de usar as facilidades tecnológicas para obterem benefícios e/ou

causar dolo a outras pessoas. Assim, é necessário que esta lei seja revista e reformulada, de modo a garantir às pessoas um ambiente seguro para que gozem dos benefícios que os avanços tecnológicos podem oferecer a quem deles se serve.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAS, Vladimir. **Crimes de informática. Uma nova criminalidade**. Jus Navigandi, ano 6, n. 51, 1 out. 2001. Disponível em: <<http://jus.com.br/revista/texto/2250>>. Acesso em: 20/07/2015.

ASCENSÃO, José de Oliveira. **Direito Civil: Teoria Geral**. vol 1, Coimbra: Coimbra, 1998.

AZEVEDO JUNIOR, Jamil Gomes de. **Cyberbullying**: análise das consequências da falta de legislação penal federal sobre o tema e da recusa do Brasil em aderir à convenção de Budapeste sobre o cibercrime. 2014. Disponível em: http://www.jurisway.org.br/v2/dhall.asp?id_dh=9828 Acesso em: 04/09/2015.

BARROS, Alice Monteiro de. **Proteção à intimidade do empregado**. 2. ed. São Paulo: LTr, 2009.

BAUMAN, Zygmunt. **Medo Líquido**. Rio de Janeiro: Jorge Zahar, 2008.

BITENCOURT, Cesar Roberto. **Invasão de dispositivo informático**. 2012. Disponível em: <http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico> Acesso em: 08/09/2015.

BITTAR, Carlos Alberto. **Os Direitos da Personalidade**. 4. ed. São Paulo: Saraiva, 2000.

BOBBIO, Norberto. **Era dos direitos**. Trad. Carlos Nelson Coutinho, Rio de Janeiro: Campus, 1988.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 8. ed. São Paulo: Malheiros Editores, 1999.

BRASIL. Código Penal. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Vade Mecum**. São Paulo: Saraiva, 2008.

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

_____. **Lei n. 8.069**, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8069.htm>. Acesso em: 20/08/2015

_____. **Lei n. 9.609/98**, de 19 de fevereiro de 1998. Lei dos Crimes de Softwares/Lei Antipirataria. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L9609.htm Acesso em: 08 de setembro de 2015.

_____. **Lei n.º 12.737, de 30 de novembro de 2012**, que traz a tipificação criminal de delitos informáticos. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm >. Acesso em: 20/09/2015.

_____. **Lei nº 10.406**, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, Brasília, DF, 11 jan. 2002. Disponível em <http://www.planalto.gov.br>. Acesso em 23 de maio de 2006.

_____. **Lei nº 7.170**, de 14 de dezembro de 1983. Define os crimes contra a segurança nacional, a ordem política e social, estabelece seu processo e julgamento e dá outras providências. Brasília, DF, 1983.

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

CAPELLARI, Eduardo. Tecnologias de informação e possibilidades do século XXI: por uma nova relação do estado com a cidadania. In: ROVER, Aires José (org.). **Direito, Sociedade e Informática**: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000.

CAPEZ, Fernando. **Curso de Direito Penal, volume 1, parte geral**. São Paulo; Saraiva, 2010.

_____. **Curso de Direito Penal**. 15. ed., vol. 1, parte geral (arts. 1º a 120), São Paulo: Saraiva, 2011.

COSTA, Fernando José da. **Locus delicti nos crimes informáticos**. São Paulo: USP, 2011. Disponível em: <<http://www.teses.usp.br/teses/disponiveis/2/2136/tde-24042012-112445/pt-br.php>>. Acesso em: 17/07/2015.

COSTA, Givago Richard Braga Carneiro da. **Uma reflexão sobre o direito à intimidade, à vida privada, à honra e à imagem das pessoas nas redes sociais da internet**. Revista Âmbito Jurídico. 21/jul/2011. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artig. Acesso: em: 20/09/2015.

DIWAN, Alberto. **O crime de invasão de dispositivo de informática - Art. 154-A do Código Penal**: uma análise do delito introduzido pela Lei 12.737/2012. 2015. Disponível em: <http://albertodiwan.jusbrasil.com.br/artigos/199631200/o-crime-de-invasao-de-dispositivo-de-informatica-art-154-a-do-codigo-penal> Acesso em: 08/09/2015.

DUPAS, Gilberto. **Ética e poder na sociedade da informação**: de como a autonomia das novas tecnologias obriga a rever o mito do progresso. São Paulo: UNESP, 2000.

FERREIRA, Ivete Senise. A criminalidade informática. In: Newton de Lucca; Adalberto Simão Filho. (Org.). **Direito e Internet**: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

FILHO, Willis S. Guerra (Coord). Direitos Fundamentais, processo e princípio da proporcionalidade. In: **Dos Direitos Humanos aos Direitos Fundamentais**. Porto Alegre: Ed. Livraria do Advogado, 1997.

GATTO, Victor Henrique Gouveia. Tipicidade penal dos crimes cometidos na internet. In: **Âmbito Jurídico**, Rio Grande, XIV, n. 91, ago 2011.

GIMENEZ, Emanuel Alberto Sperandio Garcia. Crimes virtuais. **Revista Doutrina TRF4**. nº 67, ago/2013. Disponível em: http://www.revistadoutrina.trf4.jus.br/index.htm?http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html Acesso em: 28/08/2015.

GONÇALVES, Andrey Felipe Lacerda et al. O direito fundamental à privacidade no cenário brasileiro na perspectiva de um direito à proteção de dados pessoais. In: **Revista de Direito Privado**, Nelson Nery Jr. (Coord.), v. 14, n. 54, p.45-62, abr./jun. 2013.

GUERRA, Sidney César Silva. **A liberdade de imprensa e o direito à imagem**. Biblioteca das teses. Rio de Janeiro: Renovar, 1999.

JESUS, Damásio E. de. **Direito Penal**. 27. ed. São Paulo: Saraiva, 2003.

LIRA, Leide de Almeida. **Lei Carolina Dieckmann**: (in)eficácia na proteção dos direitos fundamentais à intimidade e à vida privada em face da pena cominada aos delitos informáticos. Monografia. Curso de Direito, Centro Universitário do Distrito Federal – UDF. Brasília, 2014.

MARQUES, Andréa Neves Gonzaga. **Direito à honra**. Disponível em: <http://www.tjdft.jus.br/institucional/imprensa/artigos/2010/direito-a-honra-andrea-neves-gonzaga-marques> Acesso em: 18/07/2015.

MELLO, Celso Antônio Bandeira de. **Curso de Direito Administrativo**. 5. ed. São Paulo: Malheiros, 1994.

MELLO, Cleyson de Moraes. Hermenêutica Jurídica e a Filosofia do Novo Código Civil Brasileiro. In: BARROS, Ana Lúcia Porto de. (org) **O novo código civil: comentado**. Rio de Janeiro: Freitas Bastos, 2002.

MNEMOSYNE, Tenessy et al. **Globalização e Sociedade da Informação: Perspectivas Ético-Políticas**. Universidade Federal da Bahia. 2014. Disponível em: http://www.cinform-anteriores.ufba.br/vi_anais/docs/TennessyMnemosyne.pdf

Acesso em: 21/08/2015.

MONTEIRO NETO, João Araújo. **Aspectos constitucionais e legais do crime eletrônico**. 2008. Dissertação (mestrado). Universidade de Fortaleza, 2008.

MORAES, Alexandre de. **Direito Constitucional**. 19. ed. São Paulo; Atlas, 2006

_____. **Direitos Humanos Fundamentais**. 3. ed. São Paulo: Atlas, 2009.

_____. **A Constituição do Brasil Interpretada**. 4. ed. São Paulo: Atlas, 2004.

NETO, Mário Furlan; GUIMARÃES, José Augusto Chaves. **Crimes na internet: elementos para uma reflexão sobre a ética informacional**. R. CEJ, Brasília, n. 20, p. 67-73, jan./mar. 2003.

NOGUEIRA, Sandro D´amato. **Crimes de informática**. 2. ed. Leme: BH editora, 2009.

OLIVEIRA, William César Pinto de. Lei Carolina Dieckmann. **Revista Jus Navigandi**, Teresina, ano 18, n. 3506, 5 fev. 2013. Disponível em: <<http://jus.com.br/artigos/23655>>. Acesso em: 20/07/2015.

PENIDO, Flávia. **Os crimes previstos na Lei Carolina Dieckmann**. 2013. Disponível em: <<http://www.tiespecialistas.com.br/2013/04/os-crimes-previstos-na-lei-carolina-dieckmann/>> Acesso em: 23/08/2015.

PIMENTEL, Alexandre Freire. **O direito cibernético: um enfoque teórico e lógico-aplicativo**. Rio de Janeiro: Renovar, 2000.

PINHEIRO, Patricia Peck. **Direito digital**. 5. ed. São Paulo: Saraiva, 2013.

PINTO, Marcio Morena. **O Direito da internet**: o nascimento de um novo ramo jurídico. Jus Navigandi, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <<http://jus.com.br/revista/texto/2245>>. Acesso em: 8 fev 2012.

REALE, Miguel. **Lições preliminares de direito**, 22. Ed., São Paulo: Saraiva, 1995.

ROCHA, Carolina Borges. Evolução dos crimes cibernéticos. **Revista Jus Navigandi**, Teresina, ano 18, n. 3706, 2013. Disponível em: <<http://jus.com.br/artigos/25120>>. Acesso em: 16/09/2015.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**. Rio de Janeiro: Renovar, 2008.

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

SALVADOR NETO, Alamiro Velludo. **Tipicidade penal e sociedade de risco**. São Paulo: Quartier Latin, 2006.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada**. Belo Horizonte: Del Rey, 1998.

SARLET, Ingo Wolfgang. Dignidade da pessoa humana. In: BARRETO, Vicente de Paulo (org.). **Dicionário de Filosofia do Direito**. São Leopoldo: Usininos; Rio de Janeiro: Renovar, 2006.

_____. **A Eficácia dos Direitos Fundamentais**. 6. ed. Porto Alegre: Livraria do Advogado Editora, 2006.

SCHMITT, Carl. Teoría de la constitución. Madrid: Alianza Universidad Textos, 1996.

SILVA, Edson Ferreira da. **Direito à Intimidade**. São Paulo: Oliveira Mendes, 1998.

SILVA, José Afonso da. **Aplicabilidade das normas constitucionais**. 7 ed. São Paulo: Malheiros, 2011.

_____. **Curso de Direito Constitucional Positivo**. 33. ed. São Paulo: Malheiros, 2009.

_____. **Manual da constituição de 1988**. São Paulo: Malheiros, 2002.

SILVA, Paulo Domingos Pereira da; FREITAS, Cláudia Regina Miranda de. Crimes virtuais: há algo de novo? **Revista Pensar**. 2013. Disponível em: http://revistapensar.com.br/direito/pasta_upload/artigos/a211.pdf Acesso em: 19/07/2015.

SILVEIRA, Artur Barbosa da. Os crimes cibernéticos e a Lei nº 12.737/2012. **Conteúdo Jurídico**. Brasília-DF. 2015. Disponível em: <<http://www.conteudojuridico.com.br/?artigos&ver=2.52253&seo=1>>. Acesso em: 17/09/2015.

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

TAVARES, Tarcísio Alves. **Análises iniciais e críticas à Lei 12.737/2012 – Lei Carolina Dieckmann**. Universidade Presidente Antônio Carlos – Unipac / Faculdade de Ciências Jurídicas e Sociais de Barbacena – MG. Graduação em Direito. 2013.

TEPEDINO, Gustavo. **Temas de Direito Civil**. Rio de Janeiro: Editora Renovar, 1999.

THEODORO JR., Humberto. **Curso de Direito Processual Civil**. Vol. II. Rio de Janeiro: Forense, 2004.

TOBEÑAS, José Castan. **Los Derechos de la Personalidad**. Madri : Reus. 1952.

TOMIZAWA, Guilherme. **A Invasão de Privacidade através da Internet**. Curitiba: JM Livraria Jurídica, 2008.

VALLE, Regina Ribeiro do. Direitos Cibernético é uma realidade? In: VALLE, Regina Ribeiro do (org.). **E-dicas: O Direito na Sociedade da Informação**. São Paulo: Usina do Livro, 2005.

VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático**. Rio de Janeiro: Forense, 2003.

ZAVALA DE GONZÁLEZ, M. **Derecho a la intimidad**. Apud: MORENO, Hernández Moisés. El deber Del prófesional frente a la intimidad de su cliente. **Revista da Facultad de Derecho de México**, tomo XLIII, enero-abril de 1993, ns. 187,188.