Centro Universitário do Distrito Federal – UDF
Coordenação do Curso de Direito

LEIDE DE ALMEIDA LIRA

LEI CAROLINA DIECKMANN: (IN) EFICÁCIA NA PROTEÇÃO DOS DIREITOS FUNDAMENTAIS À INTIMIDADE E À VIDA PRIVADA EM FACE DA PENA COMINADA AOS DELITOS INFORMÁTICOS

Brasília - DF
2014

LEIDE DE ALMEIDA LIRA

LEI CAROLINA DIECKMANN: (IN) EFICÁCIA NA PROTEÇÃO DOS DIREITOS FUNDAMENTAIS À INTIMIDADE E À VIDA PRIVADA EM FACE DA PENA COMINADA AOS DELITOS INFORMÁTICOS

Trabalho de conclusão de curso apresentado à Coordenação de Direito do Centro Universitário do Distrito Federal - UDF, como requisito parcial para obtenção do grau de bacharel em Direito Orientador: Valdinei Cordeiro Coimbra.

Brasília -DF
2014

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 / Leide de Almeida Lira. – Brasília, 2014.

118 f.

Trabalho de conclusão de curso apresentado à Coordenação de Direito do Centro Universitário do Distrito Federal - UDF, como requisito parcial para obtenção do grau de bacharel em Direito. Orientador: Valdinei Cordeiro Coimbra.

1.Delitos Informáticos. 2.Privacidade. 3.Invasão. 4.Interrupção. 5.Penas Brandas. I. Lei Carolina Dieckmann: (in) eficácia na proteção dos direitos fundamentais à intimidade e à vida privada em face da pena cominada aos delitos informáticos

CDU 343.2

LEIDE DE ALMEIDA LIRA

LEI CAROLINA DIECKMANN: (IN) EFICÁCIA NA PROTEÇÃO DOS DIREITOS FUNDAMENTAIS À INTIMIDADE E À VIDA PRIVADA EM FACE DA PENA COMINADA AOS DELITOS INFORMÁTICOS

Trabalho de conclusão de curso apresentado à Coordenação de Direito do Centro Universitário do Distrito Federal - UDF, como requisito parcial para obtenção do grau de bacharel em Direito Orientador: Valdinei Cordeiro Coimbra.

Brasília, 30 de maio de 2014.

Banca Examinadora

_____

Valdinei Cordeiro Coimbra
Orientador
Centro Universitário do Distrito Federal - UDF

_____

Marcelo Ferreira de Souza
Membro da Banca
Centro Universitário do Distrito Federal - UDF

_____

Amaury Santos de Andrade
Membro da Banca
Centro Universitário do Distrito Federal - UDF

Nota: 10,0 (dez)

Dedicatória

Dedico este trabalho à minha querida família, aos amigos e professores que contribuiram de forma significativa para a construção deste conhecimento. Que esta tese represente a retribuição do apoio, carinho e compreensão indispensáveis à elaboração e êxito.

AGRADECIMENTO

Agradeço primeiramente a Deus, que me ajudou a superar os obstáculos e a vencer mais um desafio "A Ele toda honra e toda glória". Aos meus familiares que me deram amor, força, incentivo, e sobretudo, compreenderam que a ausência momentânea faz parte da vida de quem busca o sucesso duradouro. Ao meu esposo Edenildo Lira da Silva que é mais que um companheiro, é meu amigo e meu amor. À minha querida amiga Maria Ioneide Maciel dos Santos que é exemplo de luta e superação. Ao Mestre Valdinei Cordeiro Coimbra que cumpriu com louvor o papel de orientador neste trabalho, vez que rompeu as barreiras do desconhecido e impulsionou-me para conhecer a vitória. Por fim, agradeço a todos que indiretamente contribuiram e acreditaram na realização desta conquista.

“Privacidade não é algo que eu mereça, é um requisito absoluto”.

Marlon Brando

RESUMO

O presente trabalho aborda a Lei Carolina Dieckmann e sua ineficácia no que tange à proteção dos direitos fundamentais à intimidade e à vida privada, uma vez que as penas cominadas aos delitos informáticos são ínfimas frente aos danos causados às vítimas - que variam de superação ao suicídio. Infere-se que o grande avanço tecnológico da era digital, contribuiu para o cometimento de crimes e o surgimento de um novo bem jurídico a ser tutelado “a segurança da informação”, oportunidade em que passou-se a discutir se o direito penal continua sendo a *ultima ratio* considerando o princípio da lesividade ou se deve acompanhar as mudanças da sociedade de risco *sui genere* sob pena de se transformar em um mero argumento de retórica. Elucida-se que a referida lei recebeu este nome devido ao vazamento de 36 (trinta e seis) fotos íntimas da atriz na rede, razão pela qual houve grande divulgação na mídia, ocasionando pressão sobre o legislador e promulgação do diploma legal. Embora a lei tenha trazido avanços ao ordenamento jurídico pátrio, também trouxe várias lacunas em seu texto – foram expostas nove - que ao invés de coibir pode estimular a prática delituosa, razão pela qual é importante buscar o direito comparado e exemplificar a discrepância entre as punições. Por derradeiro, propõe possibilidades de melhoria junto à legislação brasileira no combate aos crimes cibernéticos a nível nacional e internacional, bem como conscientiza e orienta os usuários para que possam proteger sua intimidade na rede, mediante a manutenção preventiva de seus dispositivos informáticos e de suas atitudes.

Palavras-chave: Delitos Informáticos. Intimidade e Vida Privada. Segurança. Lei. Avanços. Lacunas. Possibilidades de Melhoria.

ABSTRACT

This paper addresses the law Carolina Dieckmann and his ineffectiveness with regard to the protection of fundamental rights to intimacy and privacy, since the feathers and propriety to the computer offenses are tiny compared with the damage caused to the victims-ranging from resilience to suicide.Infers that the great technological advancement of the digital age, contributed to the Commission of crimes and the emergence of a new legal right to be safeguarded "information security", opportunity in which was discussing whether the criminal law remains the last ratio considering the principle of lesividade or whether to accompany the changes risk society sui genere under penalty of becoming a mere rhetorical argument. Clarifies that the Act received this name due to the leakage of 36 (thirty-six) pictures of the actress's private network, which is why there was widespread in the media, causing pressure on the legislature and promulgation of legislation. Although the law has brought progress to the Brazilian legal system, also brought several gaps in his text – were exposed nine-which rather than curb can stimulate the practice of gross negligence, which is why it is important to seek the comparative law and exemplify the discrepancy between the punishments. By ultimate, proposes possibilities for improvement along the Brazilian legislation on the fight against cyber crime at national and international level, as well as aware and directs users to protect their privacy on the network, by means of preventive maintenance of your computer and devices from their attitudes.

Keywords: Computer Crimes. Intimacy and Private Life. Safety. Law Advances. Gaps. Possibilities for improvement.

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABREVIATURAS

Art. por artigo
Arts. por artigos

SIGLAS

CD-ROM - compact disk (disco compacto), rom (ready only memory ou memoria apenas de leitura)
CEF – Caixa Econômica Federal
CF – Constituição Federal
CHP - *Califórnia Higway Patrol* (Polícia Rodoviária da Califórnia)
CP – Código Penal
CPB – Código Penal Brasileiro
DNA - *deoxyribonucleic acid* (ácido desoxirribonucleico)
FBI - Federal Bureau of Investigation (Departamento Federal de Investigação)
FEBRABAN – Federação Brasileira de Bancos
FECOMERCIO/SP – Federação do Comércio do Estado de São Paulo
GPS - Global Positioning System (sistema de posicionamento global)
HD - *hard disk* (disco rígido)
ICCC - *Internet Crime Complaint Center*
LC – Lei Complementar
ONG – Organizações Não-Governamentais
ONU – Organização das Nações Unidas
PL – Projeto de Lei
SMS - Short Message Service (Serviço de Mensagem Curta)
STF – Superior Tribunal Federal
STJ – Superior Tribunal de Justiça
WIPO- *World Intellectual Property Organization* ou Organização Mundial de Propriedade Intelectual

SUMÁRIO

INTRODUÇÃO

Os avanços advindos da era digital (informacionais, culturais, econômicos e sociais) foram importantes para o desenvolvimento da sociedade moderna. Todavia, o ingresso dessas informações não é um fato que trouxe somente fatores positivos, mas também tipos de crimes que a legislação brasileira não estava preparada para compreender, identificar e punir

Desta feita, o tema escolhido para o trabalho de conclusão de curso é importante porque traz a possibilidade de violação de significativos bens jurídicos constitucionais como: à intimidade, à vida privada, à honra e à imagem, através dos crimes virtuais, os quais são cometidos de forma covarde**,** sem chance de defesa**,** podendo causar danos irreversíveis às pessoas físicas e jurídicas.

Nesse contexto, emerge a seguinte problemática: As penas cominadas aos delitos informáticos da Lei Carolina Dieckmann foram eficazes na proteção dos direitos fundamentais à intimidade e à vida privada frente aos danos causados às vitimas?

Assim, o presente estudo tem por objetivo averiguar a eficácia da Lei Carolina Dieckmann (Lei 12.737/12), a qual entrou em vigor com um texto ambíguo e lacunoso que dificulta a atuação dos operadores do direito, sobretudo no que tange às penas, uma vez que são tão brandas que podem ser convertidas em prestação de serviço à comunidade, bem como prescrevem rapidamente, inviabilizando a punição. Vislumbra-se analisar a aplicação do direito comparado e a adequação do diploma legal às convenções e tratados internacionais para sanar as brechas da legislação pátria no combate aos crimes cibernéticos. Por outro viés, importa relatar que os danos causados às vítimas podem chegar ao suicídio, motivo pelo qual apresenta-se dicas e soluções preventivas à proteção da intimidade na rede.

Para fazer uma reflexão do tema, como um todo, bem como atingir o objetivo proposto foi necessário dividir o trabalho em 5 (cinco) capítulos. No primeiro capítulo, foram pontuados os direitos fundamentais à luz Constituição Federal de 1988 como à intimidade, à vida privada, à honra e à imagem dos seres humanos, os quais estão sendo violados pelas mentes perversas da era digital, motivo suficiente para buscar a proteção do Estado.

No segundo tópico, foi abordado o direito penal na sociedade da informação onde será ressaltado que a evolução indiscriminada da globalização desencadeou conflitos e uma nova zona criminológica, exigindo-se deste ramo do direito providências emergenciais. Por conta de tal avanço tecnológico, conceitos como soberania, território, tempo e espaço perdem o sentido, razão pela qual leva a sociedade a clamar pela tutela penal e a proteção de um novo bem jurídico “a segurança da informação”. Que por sua vez, trará um debate importante no que tange ao direito penal continuar sendo a *ultima ratio* - respeitando o princípio da lesividade ou se deve acompanhar as mudanças da sociedade de risco *sui genere*, sem mitigá-las, adotando a intervenção do sistema penal antes da lesão ao bem jurídico.

O terceiro capítulo tratou do caso da atriz Carolina Dieckmann, como sua intimidade foi violada, por quais crimes responderam os infratores, de que maneira esse evento contribuiu para a entrada em vigor do diploma legal sobre delitos informáticos.

Neste diapasão, serão explanados os crimes tipificados na lei 12.737/2012, elucidados mediante de um conjunto harmônico de ideias, opiniões e ensinamentos dos maiores doutrinadores de direito penal e digital - no que couber - à compreensão dos leitores quanto a: classificação doutrinária, bem jurídico tutelado, objeto material, ação nuclear, sujeitos ativo e passivo, tipicidades objetiva e subjetiva, tempo e local do delito, consumação e tentativa, modalidades equiparada e qualificada, modalidades comissiva e omissiva, benefícios legais, causas especiais de aumento de pena, pena, ação penal, suspensão condicional do processo, competência para julgamento e conflito aparente de normas.

Para tratar do tema primordial do trabalho, foi reservado o quarto capítulo, que esclarecerá os efeitos da Lei Carolina Dieckmann debatendo os aspectos positivos e negativos no que se refere à proteção da privacidade. Ora Elencados:

a) Aspectos positivos (avanços):

- A Repercussão do Episódio da Atriz foi Relevante para a Célere Aprovação da Lei; e;

- O Advento da Lei Trouxe Segurança Jurídica e Maior Rigor Penal.

b) Aspectos negativos (lacunas):

- Divergência dos Juristas e doutrinadores Sobre o Termo “Invasão” no que Tange à Medida Violenta e Mecanismos de Segurança;

- A Mera “Espiadinha” Configura o Crime Pelo Verbo “Obter”?;

- As Penas Brandas se Convertem em Prestação de Serviços à Comunidade;

- Os Ataques de Negação de Serviços Feitos a Particulares Não Foram Abrangidos pela Lei?;

- Despreparo da Polícia Investigativa para Apurar os Crimes Informáticos Podem Levá-los à Prescrição;

- Fragilidade para Retirada de Conteúdo da Internet e Ineficácia da Legislação Sobre a *Deep Web*;

- A Lei Dependerá de Jurisprudência para Funcionar;

- Conflito de Competência nas Esferas Civil e Penal;

- Consequências Para as Vítimas dos Delitos Informáticos;

Contudo, em que pese as peculiaridades da Lei 12.737/12, o quinto capítulo explanará possibilidades de melhoria para este diploma legal, com base na aplicação do direito alienígena sobre delitos informáticos, elencados em 17 (dezessete) países, trazendo uma comparação substancial da aplicação da lei penal no Brasil e na França - evidenciando a discrepância das punições. Destarte, será apresentado o manual para prevenção e controle de delitos relacionados com computadores elaborados pela ONU – seus problemas e soluções, bem como a proposta da Convenção de Budapeste para uniformizar a legislação penal mundial com o objetivo de vencer a luta contra a criminalidade no ambiente virtual e as adequações que a legislação brasileira deve efetuar para aderí-la.

Ademais, este capítulo contará com explanações sobre a conscientização e orientação aos usuários da internet e demais meios eletrônicos para prevenção de ataques cibernéticos, pois - uma vez ocorridos - trazem consequências graves para as vítimas. Por fim, a temática da responsabilização penal das pessoas jurídicas provedoras de acesso e conteúdo quanto ao *notice and takedown* (remoção automática do conteúdo sem autorização judicial) ou takedown (responsabilização civil por danos frente recusa à ordem judicial para derrubada do conteúdo).

Trata-se, portanto, de uma pesquisa bibliográfica, que abraçou a legislação pátria, alienígena, artigos periódicos e jurisprudências.

1. OS DIREITOS FUNDAMENTAIS TUTELADOS PELA CONSTITUIÇÃO E VIOLADOS PELA ERA DIGITAL

A Constituição Federal de 1988, que é a norma suprema do ordenamento jurídico pátrio, traz em seu manto os direitos fundamentais com a finalidade de proteger os seres humanos de: abusos, excessos e medidas autoritárias ou padronizadas aplicadas pela sociedade e pelo Estado, com vistas à construção de um Estado Democrático de Direito.

Conforme disposto no artigo 5º, inciso “X” da CF/88: “São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

Segundo Nucci (2010) os direitos fundamentais são os mais absolutos, intocáveis e invioláveis direitos do homem, voltados para o bem comum mediante a vivência harmônica, solidária, regrada e disciplinada de uma sociedade democrática e pluralista.

Alexandre de Moraes acrescenta a importância de se buscar a proteção dos direitos fundamentais junto ao poder judiciário, quando 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. A proteção judicial é absolutamente indispensável para tornar efetiva a aplicabilidade e o respeito aos direitos humanos fundamentais previstos na Constituição Federal e no ordenamento jurídico em geral. (MORAES, 2007, p. 99).

Por outro lado, o referido autor destaca que os direitos humanos fundamentais sofrem limitações na sua proteção quando usados para a prática de atos ilícitos, bem como para afastar ou diminuir a responsabilidade civil ou penal por atos criminosos, ocasião em que afrontam o verdadeiro Estado de Direito.

Ademais, Andrey Felipe Lacerda Gonçalves expõe a forma de positivação dos direitos fundamentais e a sua adequação frente à realidade:

> Os direitos fundamentais foram positivados, na sua grande maioria, em linguagem aberta e indeterminada, assumindo forma principiológica, isto é, estrutura de proteção otimizada na medida das condições fáticas e jurídicas existentes. Percebe-se que, o poder constituinte optou por deixar um espaço semântico-normativo livre para a hermenêutica de aplicação da norma, contextualizado o texto com a realidade fática do tempo em que a tutela será prestada. Isto porque seria praticamente impossível prever, de modo geral e

> abstrato, todas as possíveis violações aos direitos da pessoa humana. (GONÇALVES, 2013, p. 49-50).

Nesse diapasão, surge a tecnologia da era digital que fez-se imprescindível na vida das pessoas, evoluindo no sentido de torná-las escravas: atitudes comuns como o esquecimento do celular em algum lugar ou ficar sem conexão com a rede, acarreta sensações automáticas de ansiedade profunda e pesadelo constante. Além disso, os indivíduos passaram a se comunicar através de uma linguagem própria e serem encontrados em praticamente todos os lugares por meio de comunicadores instantâneos: mensagens de texto, telefonia celular, GPS, *check-ins* voluntários e até mesmo câmeras de segurança disseminadas.

Essa comodidade desenfreada fez com que surgissem mentes perversas capazes de invadir os dispositivos informáticos alheios, interromper serviços telemáticos ou de utilidade pública e até mesmo falsificar cartões de crédito e débito; condutas criminais que violam: a intimidade, a vida privada, a honra e a imagem das pessoas trazendo danos econômicos e sociais irreparáveis.

Acerca do delicado tema, Liliana Paesani informa:

> Sem a presença de uma tutela significativa em relação ao conjunto de informações colhidas a nosso respeito pelas inovações tecnológicas dos sistemas inteligentes, torna-se difícil preservar a privacidade e a dignidade sem reduzí-las a “mercadorias”. Como consequência, sente-se a necessidade de eliminar a ingerência de elementos externos na esfera privada das pessoas. (PAESANI, 2013, p. 31).

Patrícia Peck Pinheiro (2010) acrescenta que é preciso ter ética e saber tutelar os valores que precedem às leis, uma vez que na sociedade digital a ação de um pode atingir e gerar consequências e riscos sistêmicos a todos. Sendo assim, essa sociedade precisa reafirmar os valores que servirão de fundamento para o seu regime legal, bem como para a harmonização das regras que devem nortear as condutas dos indivíduos conectados em rede.

1.1. DIREITO À INTIMIDADE E SEUS LIMITES

Alexandre de Moraes (2007, p. 159) define: “o conceito constitucional de intimidade relaciona-se com as relações subjetivas e de trato íntimo da pessoa humana, suas relações familiares e de amizade”.

Canotilho (2013) explana que o direito à intimidade apresenta-se como direito à liberdade, a qual possui um conteúdo mais determinado ou determinável, atrelado a um conjunto de princípios constitucionais que traduz de forma concreta as suas manifestações.

Dentre os princípios constitucionais que guardam relação com o direito à intimidade, o autor destaca o Princípio da Dignidade da Pessoa Humana, que é o ponto de partida para a proteção do direito à intimidade, bem como o direito geral à vida privada. Feitas as devidas considerações é possível relacionar alguns princípios e regras constitucionais que estão interligados ao direito à intimidade, tais quais: a inviolabilidade da casa (art. 5º, XI), sigilo dos dados, da correspondência e das comunicações (art. 5º, XII), a inadimissibilidade no processo das provas obtidas por meios ilícitos (art. 5º, LVI) e o *habeas data* (art. 5º, LXXII), todos integram o "conteúdo" do direito à intimidade de forma não exaustiva.

Ressalte-se que o direito à intimidade concede um poder ao indivíduo para controlar a circulação de suas informações. Nesse sentido, Canotilho colaciona:

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

Não se pode olvidar das limitações referentes ao direito à intimidade, Canotilho (2013), explica que a depender do caso concreto, este direito pode sofrer limitações para garantir a eficácia de outros bens jurídicos, tais como: a saúde, a segurança pública, a punibilidade ou outro bem coletivo.

Questões como exame de DNA para a coleta de dados pessoais genéticos com vista a solução de uma investigação policial, ou satisfazer a pretensão da identidade genética de um suposto filho; o direito à informação no que tange à liberdade de imprensa e expressão levando-se em consideração o tipo de informação captada e publicada, o lugar da captação, o comportamento do titular do direito, o interesse público e a objetividade na divulgação da notícia.

Noutro viés, o autor demonstra as situações que são ilegítimas no trato dos limites à intimidade:

> Ilegítima será, no entanto, a afirmação, por um jornal ou blog, da homossexualidade de um homem público, […] jornalismo investigativo não pode sucumbir a “furos” ou ao “denuncismo” sem precatar-se da veracidade das informações e do interesse público da notícia, evitando divulgar dados de caráter íntimo e sem pertinência necessária e estrita com a matéria e com o público direito à informação, […] a curiosidade dos fãs, por exemplo, sobre uma malformação física, ou doenças graves, a vida conjugal ou extraconjugal de seus ídolos, se o comportamento destes demonstram a intenção de reserva em relação a tais fatos, […] biografias não autorizadas. (CANOTILHO, 2013, p. 283).

Vale salientar ainda, que o direito ao esquecimento integra à intimidade, desde que o “contratante” tenha mudado o seu comportamento frente aos olhos do público, optando por uma vida mais recatada e recolhida.

1.2. DIREITO À VIDA PRIVADA

De acordo com Paulo José da Costa Júnior (1995, p. 14) o direito à privacidade é “proclamado como resultado da sentida exigência de o indivíduo encontrar na solidão aquela paz e aquele equilíbrio, continuamente comprometido pelo ritmo da vida moderna”.

Para Gilmar Mendes (2013), todo homem tem a necessidade de ficar sozinho e realizar a chamada “reclusão periódica” à vida privada, para a sua própria saúde mental; pois sem privacidade, o livre desenvolvimento da personalidade fica prejudicado pela falta de condições propícias. Dessa forma, é possível afirmar que o controle de informações sobre si mesmo esta no âmago do direito à privacidade.

Esse posicionamento tem sido discutido há décadas, Alan West (1967, p. 31) informa que, de modo geral, “há consenso em que o direito à privacidade tem por característica básica a pretensão de estar separado de grupos, mantendo-se o indivíduo livre da observação de outras pessoas”.

Nessa linha de raciocínio, Gilmar Mendes exemplifica:

> Estar submetido ao constante crivo da observação alheia dificulta o enfrentamento de novos desafios. A exposição diuturna dos nossos erros, dificuldades e fracasso à crítica e à curiosidade permanentes de terceiros, e ao ridículo público mesmo inibiria toda tentativa de autossuperação. Sem a tranquilidade emocional que se pode auferir da privacidade, não há muito menos como o indivíduo se autoavaliar, medir perspectivas e traçar metas. (MENDES, 2013, p. 280 e 281).

Em estudo clássico, nos Estados Unidos, Willian Prosser, sustentou que haveria quatro meios básicos de afrontar a privacidade:

> 1) Intromissão na reclusão ou na solidão do indivíduo, 2) exposição pública de fatos privados, 3) exposição do indivíduo a uma falsa percepção do público (false ligth), que corre quando a pessoa é retratada de modo inexato ou censurável, 4) apropriação do nome e da imagem da pessoa, sobretudo para fins comerciais. (PROSSER, 1984, p. 107).

Canotilho (2013, p. 277) acrescenta que “o direito à privacidade desafia uma compreensão muito mais ampla, assentada na própria ideia de autonomia privada e da noção de livre desenvolvimento da personalidade, sem embargo, contida em certos desdobramentos materializantes”.

O autor explica que estes desdobramentos são produto da realidade social, econômica e política, os quais foram percebidos e revelados pelo pensamento jurídico contemporâneo. Essa materialização, por outro viés, não alcança os domínios indefinidos, tampouco contempla todas as potencialidades e manipulações ideológicas da “autonomia privada”, circunscrevendo-se antes à existência humana e suas projeções. Tudo porque o direito geral à vida privada une os sentidos de “autonomia”, “personalidade” e “dignidade humana”, sob a ótica da metodologia jurídica de pesquisa e argumentação que o concretiza, dando-lhe cores e fronteiras. Por fim, o mestre exemplifica alguns componentes definidores desse conteúdo: a liberdade sexual, a liberdade da vida familiar, a intimidade, além de outros aspectos de intercessão com outros bens ou atributos da personalidade.

1.2.1. Limites ao Direito à Privacidade

Segundo Gilmar Mendes (2013), quando há interesses públicos acolhidos por normas constitucionais, que sobrepujam o interesse de recolhimento do indivíduo “pretensão de ser deixado só”, estar-se-á diante de limites ao direito à privacidade. A divulgação de fatos relacionados com uma dada pessoa – que vive de uma imagem cultivada perante a sociedade – a depender de um conjunto de circunstâncias do caso concreto, poderá ser tida como admissível ou como abusiva.

Há que se perscrutar, o modo como a notícia foi obtida, bem como o desvendamento do fato relatado ao público – quando se tratar de pessoa famosa – pois o aspecto relacionado a intimidade de alguém pode ser propalado pelo titular do

direito contra a vontade do seu protagonista, ou seja, para o autor, a extensão e a intensidade da proteção à vida privada, dependem do modo como a notícia foi coletada e da finalidade a ser alcançada com a exposição da celebridade.

Aproveitando o ensejo, Alexandre de Moraes, comenta a possibilidade de indenização por danos morais e materiais quando a divulgação da notícia não demonstrar nenhuma finalidade pública e ferir a dignidade da pessoa humana:

> Encontra-se em clara e ostensiva contradição com o fundamento constitucional da dignidade da pessoa humana (CF, art. 1º, III), com o direito à honra, à intimidade e a vida privada (CF, art. 5º, X), converter em instrumento de diversão ou entretenimento assuntos de natureza tão íntima quanto a falecimentos, padecimentos ou quaisquer desgraças alheias que não demonstrem nenhuma finalidade pública e caráter jornalístico em sua divulgação. Assim, **não existe nenhuma dúvida de que a divulgação de fotos, imagens ou notícias apelativas, injuriosas, desnecessárias para a informação objetiva e de interesse público (CF, art. 5º, XIV), que acarretem injustificado dano à dignidade humana, autoriza a ocorrência de indenização materiais e morais**, além do respectivo direito à resposta. (MORAES, 2007, p.160, grifo nosso).

No que tange ao restrito âmbito familiar, Alexandre (2007) relata que os direitos à intimidade e a vida privada devem ser interpretados de forma mais ampla, pois atingem relações delicadas e sentimentais, as quais precisam ser protegidas de qualquer intromissão.

1.2.2. Restrição à Privacidade com o Consentimento do Indivíduo

Gilmar Mendes (2013, p. 284) dispõe que “os direitos fundamentais não são suscetíveis de renúncia plena, mas podem ser objeto de autolimitações, que não esbarrem no núcleo essencial da dignidade da pessoa”[1].

O autor exemplifica que uma “pessoa famosa” pode consentir que exponha as suas agruras: durante um sequestro ou dar entrevista por ocasião da morte de algum ente querido, nada impede que o faça[2].

---

[1] Na França, anulou-se um contrato, por imoral, em que uma pessoa concordava em expor para uma revista uma extraordinária anomalia sexual. (KAYSER, 1984, p.147).

[2] O Tribunal de Justiça do Rio de Janeiro também já se assentou que o consentimento expresso pode ser limitado pela pessoa que se exporá, devendo ser respeitada a sua decisão. Por isso, manteve condenação da revista, que, tendo sido solicitada por artista por ela entrevistado a que não mencionasse o fato de que tivera ambas as pernas amputadas, e tendo autorizado fotografias apenas da cintura para cima, viu estampada na capa do semanário tanto a fotografia que revelava a sua deficiência física como uma manchete que realçava essa circunstância. Não adiantou à empresa alegar que a reportagem fora elogiosa da coragem moral do retratado diante do seu drama (TJRJ, Ap. 5.246/91, RT 700/144).(MENDES, 2013, p. 284).

Gilmar Mendes (2013) comenta ainda, a dificuldade de identificar se houve o consentimento tácito da divulgação da matéria ou da imagem que envolve aspecto da intimidade de alguém. Em princípio, haveria um consentimento tácito da exposição, no caso de alguém que se encontrar num lugar público, pois estaria sujeito a ser visto e a aparecer em alguma foto ou filmagem do mesmo lugar, ou seja, a pessoa não poderia objetar a aparecer, sem proeminência, numa reportagem - uma vez que se encontra em lugar aberto ao público - e foi retratada como parte da cena com um todo.

Noutro viés, o autor expõe opiniões contrárias no que tange a possibilidade de se destacar alguém no âmbito da paisagem, por exemplo: se seria legítimo fotografar uma banhista sem a parte do biquíni numa praia:

> As soluções variam. Há precedentes na França condenando a publicação de foto de banhista fazendo *topless*, numa reportagem sobre as praias francesas. A mesma situação, entretanto, já ensejou que o Superior Tribunal de Justiça rejeitasse pedido de indenização por danos morais, no pressuposto de que a retratada teria, em casos assim, consentido tacitamente na exposição de sua imagem3. Pode-se por certo, todavia, que essas fotografias não poderiam ser utilizadas para fins comerciais. (MENDES, 2013, p.284).

Nesse sentido, Patrícia Peck Pinheiro contribui para formação do entendimento:

> É evidente que o direito à privacidade constitui um limite natural ao direito à informação. No entanto, não há lesão a direito se houver consentimento, mesmo que implícito, na hipótese em que a pessoa demonstra de algum modo interesse em divulgar aspectos da própria vida. (PINHEIRO, 2013, p. 87).

Ademais, Gilmar Mendes (2013) expõe que a legitimação da divulgação da notícia, não pode depender apenas da veracidade dos fatos, tampouco se destinar meramente a curiosidade ociosa do público; mas que, sobretudo, traga ao leitor orientação para uma melhor vivência. Há que se apurar ainda, o interesse público, no que tange ao desgaste material e emocional do retratato, num juízo de proporcionalidade estrita, para enunciar os atributos de validez da exposição. Sendo assim, notícias sobre hábitos alimentares exóticos ou

[3] No Resp 595.600 (DJ de 13-9-2004, Rel. Min. Cesar Asfor Rocha) lê-se: “A proteção à intimidade não pode ser exaltada a ponto de conferir imunidade contra toda e qualquer veiculação de imagem de uma pessoa, constituindo uma redoma protetora só superada pelo expresso consentimento, mas encontra limites de acordo com as circunstâncias e peculiaridades em que ocorrida a captação”. No voto do relator, ainda foi salientado que “a própria recorrente optou por revelar sua intimidade, ao expor o peito desnudo em local público de grande movimento, inexistindo qualquer conteúdo pernicioso na veiculação, que se limitou a registrar sobriamente o evento sem sequer citar o nome da autora”. Na mesma diretriz e do mesmo relator, o Resp 58.101, DJ de 9-3-1988. (MENDES, 2013).

sexuais de um artista não se incluem nesse rol de matérias de interesse público, ficando resguardada a proteção à intimidade.

Por fim, não exaurindo os exemplos sobre a matéria, Gilmar Mendes, (2013) informa que uma vez divulgadas as informações pelo indivíduo, que o fez por conta própria, e estas se tenham tornado públicas, não haverá como retê-las[4].

1.2.3. Intimidade e Vida Privada como Direitos da Personalidade

Segundo Canotilho (2003) os direitos fundamentais constitucionais são tutelados pelo direito da pessoa humana, mas nem todos, enquadram-se como direitos de personalidade, como é caso dos direitos à privacidade e intimidade. Dessa forma, é notória a importância que os direitos da personalidade têm para a preservação do princípio da dignidade da pessoa humana.

Andrey Felipe (2013, p.47) declara que a privacidade "é, hoje, sem dúvidas, inestimável à pessoa humana e fundamental ao complexo social. Nesse sentido e sob o prisma jurídico, trata-se de um direito fundamental cujo núcleo corresponde à própria intimidade do ser humano em sua vida privada".

Sarlet (2006) expõe que o conceito de dignidade da pessoa humana assume uma condição dúplice quando atua como fundamento estatal (art. 1º, III, da CF/88), sendo: direito defensivo (conduta inativa) e direito prestacional (conduta pró-ativa), uma vez que corresponde, concomitantemente, ao limite e a tarefa precípua dos poderes estatais da coletividade e de cada um dos indivíduos.

Nesse diapasão, Tatiana Malta (2007) leciona que o direito à privacidade caracteriza-se como típico direito de defesa quando protege a esfera individual do titular contra intromissões do Poder Público e dos demais concidadãos. Entretanto, para garantir que essas intromissões de terceiros - na intimidade e na

[4] É o que decidiu o Tribunal de Justiça do Rio de Janeiro, em acórdão da lavra do Des. Barbosa Moreira (notícia do acórdão na Apelação Cível n. 3.920/88 em Castanho de Carvalho, *Direito de informação*, cit., p. 47-48). O caso se refere a uma tentativa de Luiz Carlos Prestes de impedir um espetáculo teatral que reviveria o episódio do seu romance com Olga Benário Prestes e a deportação dela para a Alemanha, durante a Segunda Guerra Mundial. Os fatos já haviam chegado ao conhecimento do público e, como salientou o relator, teriam sido narrados pelo próprio Prestes ao autor do livro *Olga*, Fernando Morais. Daí concluir o aresto que, "se o agente se cinge a incluir na obra fato ou traço já objeto da ciência alheia ou acessível (em condições normais) a ela, não ofende o direito à privacidade, conquanto deixe de obter a autorização do titular". (MENDES, 2013, p. 286).

vida privada alheia - não violem o direito à intimidade, exige-se uma atuação positiva do Estado.

Torna-se relevante o posicionamento do Andrey Felipe (2013) ao explanar que os direitos de personalidade possuem origem no pensamento liberal-burguês do século XVIII e classificam-se como de primeira geração, pois se traduzem na expressão de liberdade e são conhecidos como direitos de defesa (direitos de cunho negativo), tendo em vista que exigem do Estado: não só uma esfera de autonomia individual, mas também uma não intervenção.

Contudo, Canotilho (2003) explica que os direitos de personalidade, apesar do cunho negativo, impõem ao Estado - o dever de proteção aos seus titulares perante terceiros – para que aqueles não tenham seus direitos violados.

1.3. DIREITO À HONRA E SEUS LIMITES

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

Canotilho (2013, p. 284) enriquece o tema: “conceitua-se direito à honra aquele que tem toda pessoa a ser respeitada perante si mesma e perante os outros”.

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

Canotilho (2013) acrescenta que toda pessoa possui um espaço de intimidade, que sofre alterações constantes - a partir do momento em que uma nova informação é inserida sobre o indivíduo. *Prima facie* pode-se confirmar que as atividades que modificam o conceito social de alguém, quando não consentidas, violam a sua intimidade.

Nesse diapasão, Alexandre de Moraes, expõe entendimentos jurisprudenciais:

> **Liberdade de informação e divulgação e inviolabilidade à honra e vida privada:** STJ – “Se, de um lado, a Constituição assegura a liberdade de informação, certo é que, de outro, há limitações, como se extrai do § 1º do art. 220, que determina seja observado o contido

> no inciso X do art. 5º, mostrando-se consentâneo o segredo de justiça disciplinando na lei processual com a inviolabilidade ali garantida" (STJ – 3ª T. – RMS n.º 3.292-2 PR – Rel. Min. Costa Leite – Ementário STJ, n.º 12/254). (MORAES, 2007, p. 197).
>
> **Liberdade de divulgação e indenização por dano moral:** STJ – "É indenizável o dano moral decorrente de noticiário veiculado pela imprensa, considerado ofensivo à honra do autor (art. 49, inciso I, da Lei n.º 5.250, de 9-2-67)". (STJ – 4ª T – Resp. n.º 2.187/RJ – Rel. Min. Barros Monteiro – Ementário STJ, n.º 4/160) **No mesmo sentido**: 3ª T. – Resp n.º 15.672-0/PR – Rel. Min. Dias Trindade – Ementário STJ, n.º 5/153). (MORAES, 2007, p. 197).

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

1.4. DIREITO À IMAGEM E SEUS LIMITES

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

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

O autor, por sua vez, classificou o direito à imagem sob duas vertentes: como objeto de um direito e como instrumento de informação comunicativa. O direito à imagem será considerado como objeto de um direito – conforme a experiência jurídica - quando for associado a componentes que se destacam na precisa definição dos poderes atribuídos a seus titulares. Sendo: *negativos*: no que tange ao conhecimento alheio, impedindo a produção, reprodução, oposição à sua realização, bem como *positivos* quando consentir a atribuição de todos os pontos negativos, sendo até certo ponto, um desdobramento da intimidade. Por outro viés, será

considerado como instrumento de informação comunicativa quando a imagem integrar o âmbito do direito à intimidade.

Canotilho explana algumas situações que dizem respeito aos limites do direito à imagem. A começar pela colocação de câmeras de vigilância nas empresas e governos com intuito de impedir ou reprimir a ocorrência de danos ou crimes. A partir dessa situação – muitas pessoas indagam se há legitimidade nesse emprego difundido.

> Em regra, responde-se positivamente, exigindo-se apenas que haja bem visível a informação de que o procedimento está sendo adotado. Há contudo, certos cuidados adicionais à regra que não podem ser desconsiderados. Para os dois casos, deve-se ter uma política de boas práticas no tratamento das imagens captadas. Claramente há de ser definido o tempo de permanência da gravação, seguindo-se as exigências de justa necessidade de prova. Em caso de não ocorrência de dano ou ilícito penal, a exclusão das imagens deve ser incontinente. Mesmo diante da necessidade de preservação das gravações, são necessárias as ações de cautela para impedir que terceiros captados pelas câmeras tenham sua imagem, identidade e intimidade adequadamente protegidas. (CANOTILHO, 2013, p. 284).

Por outro lado, o autor informa que a finalidade da vigilância se destina apenas à proteção do patrimônio de empresas e da segurança pública do Estado, ou seja, a ação de vigiar não pode estar voltada para incursões no espaço mais íntimo das pessoas de modo a identificar, por exemplo, as relações amorosas ou orientação sexual destas. Destarte, o foco da captação da imagem ou da informação, por meio da filmagem ou da fotografia, só guarda relevância no que for estritamente necessário à consecução da finalidade.

Nessa temática, o autor cita outra limitação ao direito à imagem. Esta alcança os motoristas de veículos automotores, na ocasião em que são vigiados por câmeras que controlam velocidades excessivas no trânsito:

> Se o objetivo da vigilância é identificar velocidades excessivas no trânsito, que podem pôr em risco a segurança de todos, a captação se deve restringir à placa de identificação veicular. A filmagem ou fotografia do interior do carro, em princípio, excede o objetivo perseguido, violando o direito à imagem e à intimidade dos condutores e de eventuais caronas. (CANOTILHO, 2013, p. 284).

Alexandre de Moraes expõe alguns entendimentos jurisprudenciais que corroboram a proteção do Estado no que tange ao direito à imagem das pessoas públicas:

> **Tutela à própria imagem: STF** – “Direito à proteção da própria imagem, diante da utilização de fotografia, em anúncio com fim lucrativo, sem a devida autorização da pessoa correspondente.

> Indenização pelo uso indevido da imagem. Tutela jurídica resultante do alcance do direito positivo" (STF – 2ª T. – Rextr. N.º 91.328/SP – Rel. Min. Djaci Falcão, Diário da Justiça, Seção I, 11 dez. 1981, p. 12.605). (MORAES, 2007, p. 222).
>
> **Direito à imagem e indenização: STF**: - "Direito à imagem. Fotografia. Publicidade comercial. A divulgação da imagem da pessoa, sem o seu consentimento, para fins de publicidade comercial, implica em locupletamento ilícito à causa de outrem, que impõe a reparação do dano" (STF – 1ª T. – Rextr. N.º 95.872/RJ – Rel. Min. Rafael Mayer, Diário da Justiça, Seção I, 1º out 1982, p. 9.830) No mesmo sentido: TJSP – Apelação Cível n.º 195.773-1 – São Paulo – Rel. Walter Moraes – 19-4-1994; TJSP – Apelação Cível nº 181.495-1 – São Paulo – Rel. Antonio Marson – 4-11-1992. (MORAES, 2007, p. 223).
>
> **Proteção à própria imagem e prescrição vintenária:** TJSP – "O direito sobre a própria imagem é direito pessoal protegido pelo art. 5º, XXVIII, a, da Constituição da República e prescreve em vinte anos, de conformidade com o art. 177 do Código Civil" (TJSP – 4ª Camara Civil – Ag. Nº 229.213-1/SP – Rel. Des. Cunha Cintra – JTJSP – Lex, 161/219). (MORAES, 2007, p. 222).

Alexandre de Moraes (2007) conclui que o direito à imagem deve ser interpretado de maneira mais elástica, quando estiver relacionado a - autoridades públicas, políticos, artistas ou assemelhados – devido a existência de maior exposição à mídia, bem como pela própria natureza das funções exercidas; uma vez que que os fatos que envolvem essas pessoas além de dizer respeito ao interesse público também devem ser expostos ao conhecimento de todos. No entanto, não obsta que elas busquem a tutela jurisdicional do Estado, no que extrapolar a linha tênue do respeito aos direitos fundamentais à vida privada e à honra.

2. O DIREITO PENAL NA SOCIEDADE DA INFORMAÇÃO

Auriney Brito (2013, p.26) declara 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”.

Ressalte-se que ao analisar a dinâmica da sociedade pós-moderna, o autor percebeu que essa evolução indiscriminada proporcionada pela globalização acabou por gerar riscos sociais - oriundos das novas formas de contato entre os cidadãos - trazidas pela “Era digital”. Dessa forma, resta claro que apesar de a internet ser uma importante ferramenta para o desenvolvimento econômico da sociedade, foi a responsável por estabelecer novos contatos sociais que desencadearam: além de novos atritos, uma nova zona criminológica.

Eduardo Reale Ferrari (2007) acrescenta que os novos riscos disponibilizados pela era da informática passaram a causar conflitos até então desconhecidos pelo Direito, razão pela qual exigiu-se que novas providências fossem tomadas, não mais para proteção de bens jurídicos clássicos e *palpáveis*, como a vida e o patrimônio dos cidadãos, mas para a proteção de bens jurídicos supraindividuais, os quais possuem como titulares à coletividade, sendo de forma determinável (coletivos) ou indeterminável (difusos).

Destarte, Auriney Brito (2013) afirma que com o surgimento da sociedade da informação, os riscos e a incerteza foram potencializados, uma vez que a população que utiliza a rede mundial de computadores cresce incontrolavelmente, ocasionando fatores que corroboram para a: globalização econômica, a produção e o consumo descontrolado, os riscos ambientais e a criminalidade organizada; de tal forma que exige atitudes de proteção por parte do Estado, que, por sua vez, já se encontra perplexo em receber mais demandas criminais, razão pela qual faz-se necessária a ampliação do horizonte de proteção do Direito Penal.

2.1. PRINCÍPIO DA SEGURANÇA DA INFORMAÇÃO E ELEMENTOS PARA A PROTEÇÃO JURÍDICA

Segundo Andrey Felipe Lacerda Gonçalves (2013, p. 46 e 58-60) “a privacidade é um dos bens da vida mais caros ao ser humano, uma vez que, sem ela, o homem expõe-se de modo a violar a sua própria personalidade”. Sendo assim, “nem tudo que o homem pensa precisa ser compartilhado”.

Ressalte-se que com os avanços da tecnologia e da difusão de informação, a sociedade pós-moderna tornou-se volátil, de modo que ninguém escapa à vigilância e à privacidade. O autor evidencia que na era digital, a proteção dos direitos fundamentais dos indivíduos, inerentes à vida privada, estão em situação delicada. Percebe-se que os meios de informatização exercem um poder sobre os indivíduos, uma vez que controlam a sua vida e os seus dados; por isso, como novel direito fundamental, faz-se necessária a proteção de dados[5], instrumento de defesa à vida privada e à intimidade, núcleos do direito à privacidade.

Stefano Rodotà agrega valor ao tema, quando afirma:

> 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).

Neste ínterim em que à privacidade é violada e os dados pessoais são coletados – devido à insegurança do meio – é estimulada a prática dos crimes digitais; que 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”. Há esta postura devido a insegurança do meio, uma vez que a sociedade não sente que a informação está sendo protegida, a vigilância não é feita de forma suficiente e os crimes não recebem a punição adequada frente ao dano causado.

---

[5] “No panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada”. DONEDA, Danilo. **A proteção de dados pessoais como direito fundamental**. Revista Espaço Jurídico 12/103. Joaçaba: Unoesc, 2011.

Desta feita, a autora acredita que o direito digital obriga toda corte que atua no processo judiciário: juízes, procuradores, advogados, delegados, investigadores, peritos e demais, a realizar uma atualização tecnológica. Tal postura é necessária para que se atinja uma sociedade digital segura; do contrário, o ordenamento jurídico restará prejudicado e colocará a sociedade em risco. Nessa hipótese, o conjunto norma-sanção é tão relevante no mundo digital, quanto no mundo real, ou seja, se o Estado não for eficaz no que tange a capacidade punitiva, os crimes aumentarão e os negócios virtuais serão desestimulados frente a sociedade digital.

Spencer Toth Sydow (2013, p.53) fortalece o entendimento da referida autora no momento em que declara “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”. O autor elucida que de fato a sociedade cresce pela criação de um ambiente eletrônico, computacional e virtual, mas por outro lado contribui para a insegurança do meio; vez que a regulamentação do ordenamento é incapaz de acompanhar a evolução da tecnologia. Desta feita, é importante colacionar a característica peculiar da sociedade informática:

> 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 a tecnologia da informação**. (SPENCER, 2013, p. 53, grifo nosso).

Nesse diapasão, Spencer (2013, p.69) declara que “se, por um lado a modernização traz vantagens aparentes para a maximização de valores, por outro, reflexivamente, há o fenômeno de um descontrole da harmonia social e a criação de novos riscos”. Sendo assim, o surgimento de uma relevância econômica para bens imateriais, desencadeia uma modificação significativa de paradigmas penais no que tange a proteção exclusivamente material.

Adentrando a temática, Alamiro Velludo Salvador Neto explana sobre o fenômeno da 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).

Por conta do avanço tecnológico, conceitos como soberania, território, tempo e espaço perdem o sentido, razão pela qual leva a sociedade a clamar pela tutela penal, que por sua vez encontra um novo bem jurídico para abraçar denominado “Segurança Informática”.

Spencer (2013, p. 70) relata que se faz necessário conceituar “segurança” para melhor construir o entendimento do risco *sui generis* da sociedade da informação, assim: “por segurança compreende-se a condição de algo ou alguém encontrar-se livre de perigo, perdas ou proteção”.

Segundo Auriney Brito, o direito à informação foi considerado como direito fundamental no Pacto Internacional de Direitos Civis e Políticos ocorrido em 1966 e ratificado pelo Brasil em 1992, ora preconizado no art. 19:

> Toda pessoa tem a liberdade de “procurar, receber e difundir informações e ideias de qualquer natureza independentemente de considerações de fronteiras, verbalmente ou por escrito, de forma impressa ou artística, ou por qualquer meio de sua escolha”. (BRITO, 2013, p. 43).

Diante dessa “liberdade”, surgiu a preocupação com a segurança da informação, por isso, o autor explana a abordagem desse assunto na Convenção de Budapeste, onde fora firmado um acordo internacional com vistas à proteção da comunicação e do tráfico de informações no *ciberespaço*. Destaca-se que a segurança da informação foi eleita pelo conselho europeu como um novo bem jurídico merecedor de tutela, por ser reconhecida sua relevância internacional.

Destarte, emerge o reconhecimento de um novo direito humano fundamental – princípio da segurança da informação - que precisa ser protegido pelo Direito de forma uniforme e universal, pois a autodeterminação informática fica prejudicada num ambiente inseguro, conforme preconiza o autor:

> Como na Sociedade da Informação a internet representa um importante meio de comunicação, os relacionamentos que exercitam outras liberdades, ou a livre-iniciativa, v.g, 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, grifo nosso).

Com base na análise empírica dos crimes mais corriqueiros que envolvam tecnologia, Spencer (2013) relata que é possível que se limite os

componentes que tornam o sistema informático inseguro. Nesse sentido, o Preâmbulo da Convenção de Budapeste sobre *Cibercrime* e o Comitê Gestor da Internet no Brasil, destacam os três pilares que tomarão vulto para a proteção jurídica:

> 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. (SPENCER, 2013, p. 70, grifo nosso).

Diante dos pressupostos da segurança da informação, também denominados elementos da proteção jurídica, quais sejam: **Confidencialidade**, **Integridade** e **Disponibilidade**, vale a pena adentrar no mérito de cada um, com vistas à sua compreensão e importância:

> **Confidencialidade** é a garantia de sigilo no que se referem às informações tratadas pelos aparatos informáticos e que pertencem a um número individualizável de usuários, não sendo, pois, pública e não podendo ser lida, utilizada ou de qualquer modo acessada por qualquer pessoa que não seja legítima ou legitimada. Isso se dá porque é de se compreender o material informático como verdadeira propriedade de um indivíduo. (SPENCER, 2013, p. 71, grifo nosso).

O autor exemplifica situações que corroboram para o entendimento inerente à confidencialidade:

> Os dados existentes dentro de um **aparato celular**, como a agenda eletrônica ou o arquivo de mensagens enviadas, pertencem exclusivamente ao legítimo detentor, ao produtor dos dados ou àqueles que receberam acesso autorizado por ele, a tal conteúdo. (Ibidem, p.71, grifo nosso).

Bem como:

> O **acesso a uma senha ou a um filme** existentes dentro de um computador só pode ocorrer pelo rol de usuários que compõe a lista de acesso autorizado pelo proprietário de tal ativo (no caso, bem intangível com valor), seja mediante pagamento, seja gratuitamente. (Ibidem, p.71, grifo nosso).

Do mesmo modo:

> A **intrusão informática**, a leitura de e-mails não autorizada, o acesso às informações particulares como senhas e dados bancários ou comerciais, o acesso ao correio eletrônico alheio para

> remetimento e difusão de *malwares* ou propaganda, a leitura ou uso de senhas pessoais, número de cartão de crédito, e até o assistir a filmes e o ouvir de músicas sem autorização dos produtores são alguns exemplos de condutas que violam diretamente a confidencialidade de dados. (Ibidem, p.72, grifo nosso).

Assim, Spencer (2013) conclui que a Confidencialidade é como se fosse um direito moral, pois está diretamente ligada ao interesse e a vontade do usuário-proprietário no que tange a prerrogativa de dispor de tal ativo e decidir o quão amplo será o conhecimento e quão livre será a inserção de tais dados. Trata-se da qualidade que o titular possui para restringir o acesso alheio, aos seus dados, até que haja permissão para tanto.

Spencer (2013, p. 73, grifo nosso) inseriu o conceito de Integridade com base no art. 4º, inciso VIII do Decreto n.º 4.553 de 30-12-2002, o qual dispõe: "A **Integridade** será compreendida como a incolumidade de dados ou informações na origem, no trânsito ou no destino".

Para o autor é prerrogativa do usuário manter seus dados na forma como foram criados, copiados ou armazenados, sendo proibida a sua alteração por terceiros sem autorização prévia, principalmente quando se tratar de propriedade que possua valor econômico. Desta feita, uma modificação em um arquivo pode fazer com que ele seja corrompido e não mais possa ser lido pelos aparatos ou que o dado arquivo cumpra outra função para o qual não estava programado, bem como torná-lo imprestável ou inadequado para o seu uso original, gerando prejuízos patrimoniais de grande ordem.

São exemplos de condutas que violam a integridade de um arquivo – que pode existir por si ou pode fazer parte de um sistema como o *cibervandalismo*:

> A inserção de *malware* para destruição de arquivos, a modificação de linhas de programação para inutilizar arquivos, a quebra de senhas, a inserção de arquivos (cracks) que permitem o uso de softwares piratas ludibriando os sistemas de verificação de autenticidade, dentre outras, pois que de alguma forma modificam arquivos e fazem com que seu uso seja modificado ou impedido. (SPENCER, 2013, p.74,).

No que tange ao terceiro elemento da proteção jurídica, Spencer (2013, p.75, grifo nosso) também aderiu ao conceito consubstanciado no art. 4º, inciso VI do Decreto n.º 4.553 de 30-12-2002, o qual preconiza que a **Disponibilidade** é "a facilidade de recuperação ou acessibilidade de dados e informações". Sendo assim:

> Não basta que os dados e seu conteúdo estejam resguardados do acesso não autorizado de terceiros nem que estejam íntegros, em perfeito estado de inteireza, se seu legítimo proprietário não consegue ter acesso a eles ou permitir que terceiros o tenham. É necessário que, para consolidar o conceito de segurança informática, tenha-se a ideia de acessibilidade ampla para o usuário autorizado. **Compõe a segurança da informação a possibilidade livre de o usuário utilizar-se de seus dados no momento em que desejar**. (SPENCER, 2013, p. 75, grifo nosso).

Spencer (2013) elucida ainda as condutas mais comuns que violam a Disponibilidade tais quais se destacam: a inserção de *malware* seguida de acesso e modificação da senha de *e-mail* ou rede social alheia, a inserção de *malwares* que se multiplicam tornando o uso da máquina lento, os ataques de provedores denominados *DoS* (*Denial of Service*), o erroneamente chamado "sequestro" de arquivos[6], o envio de arquivo que se instala na máquina alheia e reinicializa constantemente, entre tantas outras.

2.2. TUTELA PENAL NA SOCIEDADE DA INFORMAÇÃO

Auriney Brito (2013) explana que o Direito deve contemporizar, efetivamente, as mudanças da sociedade, principalmente no que tange a *Era da informação* ou *Era digital*, pois se o "Direito é o reflexo da sociedade", não se pode mitigar as efetivas mudanças, sob pena de ver essa afirmação se transformar em um mero argumento de retórica.

Nesse sentido, Tania Maria Cardoso Silva Amâncio concorda que não há como negar o desenvolvimento da tecnologia no mundo atual, especialmente o impacto que a informática apresentou na sociedade, inclusive no campo criminal:

> Os avanços, em todos os sentidos (informacionais, culturais, econômicos e sociais) advindos da informatização da sociedade, não podem ser esquecidos. Todavia, o ingresso da sociedade moderna na era da informação não é um fato que trouxe somente fatores positivos, estando envolto em um manto de exclusão dos menos favorecidos socioeconomicamente e, também, de ocorrência de novos tipos de crimes que a legislação brasileira não estava

[6] O art. 159 do Código Penal é explícito ao apontar que o termo "sequestro" somente é utilizado nesta ciência no sentido de privação de liberdade de uma pessoa, não sendo cabível qualquer extensão interpretativa – mesmo porque *in malam partem* -, muito especialmente ao se tratar de objetos intangíveis como dados informáticos. A privação da disponibilidade de arquivos com a consequente tentativa de obter vantagens patrimoniais configura-se crime de extorsão previsto no art. 158 do mesmo Códex, pois que a promessa de mal injusto (destruição de arquivo ou indisponibilidade) está configurada. (SPENCER, 2013, p. 76).

> preparada para compreender, identificar e punir. (AMÂNCIO, 2013, p. 24).

Zygmunt Bauman (2008) afirma que a sociedade ficou desprotegida com os avanços da tecnologia, pois esse contexto desencadeou os riscos, incertezas e a prática de crimes, fazendo surgir a *Sociedade da Incerteza* onde novos perigos são descobertos e anunciados quase que diariamente, não tendo como saber quantos mais, e de que tipo, conseguiram escapar à nossa atenção – preparando-se para atacar sem aviso.

Em razão disso, Silva Sánchez (2002) desenvolve a ideia de *expansão do Direito Penal* configurada na resposta apresentada pelo Estado para atender à referidas demandas no sentido de evitar ou atenuar os novos riscos, uma vez que se vale de forma desmesurada e, na maioria das vezes, contraproducente de sua principal máquina coercitiva. Seria a hipótese de deslocar o direito penal do ramo do ordenamento jurídico do caráter de *ultima ratio* do controle social, para desafiá-lo a acompanhar a evolução da sociedade.

Conforme assevera o referido autor (2002, p.61), o resultado é desalentador. “Por um lado, porque a visão do Direito Penal como único instrumento eficaz de pedagogia político-social, como mecanismo de socialização, de civilização, supõe uma expansão *ad absurdum* da outrora *ultima ratio”*.

Mas por outro lado, Auriney Brito declara:

> Porque tal expressão é em boa parte inútil, na medida em que transfere ao Direito Penal um fardo que ele não pode carregar, mesmo se mantido um modelo mais ou menos análogo ao clássico de garantias e regras de imputação. E, com maior razão, se tal modelo sofrer fraturas que o desnaturalizem por completo. (BRITO, 2013, p. 28).

Destarte, o autor assegura que a realidade inarredável na nova contextualização da sociedade configura-se na preocupação com a tutela de bens jurídicos supraindividuais, uma vez que gera um problema para o Direito Penal no sentido de ser este a panaceia primária de utilização do direito, principalmente pela existência de um modelo de imputação que é incompatível com a imaterialidade desses bens.

Em alguns casos, como ocorre com a segurança informática, Auriney Brito expõe:

> A supraindividualidade ou a transindividualidade deixa de estar relacionada com a população de uma comunidade ou região específica, e passa a preocupar usuários de internet de todo o

> mundo, o que nos permite, de forma inédita, nesse contexto, falar em uma transindividualidade global, em que a efetividade da proteção depende de um movimento protetivo uniforme em escala global. (BRITO, 2013, p. 29).

Dessa forma, o autor alerta para a possibilidade de ocorrência de danos absolutamente irreversíveis, frente ao acúmulo de condutas prejudiciais a bens jurídicos supraindividuais, podendo chegar – inclusive – ao extremo de comprometer a própria existência humana no planeta Terra, quando se tratar de ataques ao meio ambiente. Assim, exige-se do Estado a apresentação de medidas alternativas de precaução e prevenção de dados, uma vez que as demandas sociais deixaram de ser eminentemente reparatórias e passaram a ser também inibitórias, ou seja, caso essas demandas sejam efetivadas, não haverá mais o que se possa fazer.

Nesse sentido, Auriney Brito (2013) reitera que a missão do Direito Penal num Estado Democrático é proteger bens jurídicos, além de carregar consigo a poderosa função preventiva. Sendo assim, se não há prevenção, inexiste proteção. É exatamente essa a forma prática de agir do Direito Penal Clássico, pois não protege os bens jurídicos, enquanto estes não forem violados, ou seja – só punirá aquele que causou resultado danoso a outrem, depois que a lesão acontecer.

Esse posicionamento é criticado pelo autor, pois acredita que deve-se dar maior atenção ao uso cauteloso do efeito preventivo do Direito Penal para que se alcance o ideal de proteção aos bens jurídicos. Elucida-se que a tutela penal não deve ser vista como inconstitucional, por isso é importante pontuar o seu significado:

> Esse tipo de antecipação de tutela é diferente da antecipação de tutela que se vê na área cível, na qual há um provimento imediato que adianta, total ou parcialmente, os efeitos do julgamento final do processo, desde que verificados os pressupostos do fumus boni iuris e o periculum in mora. **A antecipação da tutela penal é a intervenção do sistema penal antes da lesão ao bem jurídico**. (BRITO, 2013, p. 30, grifo nosso).

Muitos doutrinadores argumentam que tal prática é absolutamente inviável por violar o princípio da lesividade, corolário da intervenção mínima, que determina que “só haverá crime se houver lesão ou ameaça concreta de lesão ao bem jurídico protegido”. Daí decorrem a tipicidade material e a ilicitude material como elementos do crime, e o princípio da insignificância como circunstância que exclui a tipicidade material.

Sobre a ofensividade, afirma Luiz Flávio Gomes:

> Por força do princípio da ofensividade **não se pode conceber a existência de qualquer crime sem ofensa ao bem jurídico (nulum crimen sine iniura)**. Desse princípio decorre a eleição de um modelo de Direito Penal com característica predominantemente objetiva, fundado em pelo menos dois pilares a proteção de bens jurídicos e a correspondente e necessária ofensividade. (GOMES, 2007, p.464, grifo nosso).

Misael Neto Bispo da França concorda com o posicionamento de Luiz Flávio Gomes, quando declara:

> Dentre as funções essenciais do Direito Penal, está a de exclusiva proteção de bens jurídicos fundamentais de terceiros; é o que se depreende do princípio da ofensividade, que exige que o poder de punir do Estado só se inicia em face de sérias lesões (ou ameaça de lesões sérias) aos direitos por ele tutelados. Também, a ideia de intervenção mínima, corolário da proporcionalidade necessidade, corrobora **o caráter cirúrgico do Direito Repressivo, tendo espaço, somente, quando da falência das outras esferas de controle social**. Noutros termos, tem-se noção de *extrema ratio* desse subsistema jurídico. (FRANÇA, 2013, p. 4, grifo nosso).

Auriney Brito (2013) leciona que não é mais possível afirmar, de forma absoluta, que não existe mais crime sem lesão ou ameaça concreta ao bem jurídico; pelo contrário, há que se perscrutar que em alguns casos, a atuação do Direito Penal com antecipação de tutela faz-se necessária, devido a característica do contexto social, sendo muito mais forte que qualquer paradigma antiquadro.

A prova é que, mesmo diante da resistência dos defensores da lesividade, essa manobra antecipatória vem sendo utilizada como técnica legislativa e está em plena vigência, com destaque para alguns artigos:

> O tipo penal previsto no art. 306 da Lei n. 9.503/97 (Código de Trânsito Brasileiro) de conduzir veículo automotor sob influência de álcool; o previsto no art. 28 da Lei de Drogas (Lei 11.343/2006), que nem sequer ameaça bem jurídico diverso do usuário da droga; o previsto no art. 12 da Lei n. 10.826/2003 (Estatuto do Desarmamento), assim como o próprio porte irregular de arma de fogo de uso permitido previsto no art. 14 do mesmo diploma legal; o previsto no art. 42 da Lei de Crimes Ambientais (Lei 9.605/98), que proíbe a fabricação de balões que possam causar incêndios nas florestas, dentre muitos outros destinados a proteger bens jurídicos supraindividuais, apresentam a mesma característica clara e evidente de antecipação de tutela penal. (BRITO, 2013, p.32).

Desta feita, Auriney Brito (2013) entende que a prevenção, como técnica legislativa, já se faz presente na realidade atual e que certamente abraçará alguns tipos penais criminalizadores de condutas atentatórias à segurança da informática e da internet.

Portanto, torna-se mais razoável pensar na possibilidade de relativização de alguns princípios constitucionais do Direito Penal Clássico - em especial o da lesividade - para garantir que o Direito Penal atual seja o instrumento legítimo para a proteção de bens jurídicos supraindividuais na sociedade da informação, respeitando sobretudo a subsidiariedade, a fragmentalidade e a legalidade.

3. A ENTRADA EM VIGOR DO DIPLOMA LEGAL SOBRE DELITOS INFORMÁTICOS E SUAS PECULIARIDADES

Segundo Auriney Brito (2013) a entrada em vigor do diploma legal sobre delitos informáticos representou um marco na história do ordenamento jurídico pátrio, tendo em vista o substancial avanço no que concerne à criminalidade informática. A Lei n.º 12.735 foi sancionada pela presidente Dilma Rousseff com a dura missão de estreitar as lacunas existentes sobre a matéria, bem como evitar a impunidade dos crimes cibernéticos.

3.1. O CASO CAROLINA DIECKMANN

Segundo reportagem por Guilherme Sardas (2013, p. 59), em maio de 2012, “36 fotos íntimas de Carolina Dieckmann, em que a atriz aparece em cenas de nudez e poses sensuais, vazaram na internet”. A propagação das imagens se deu em virtude da invasão de seu computador pessoal, comandada por dois *crackers*, um do pequeno município de Macatuba (SP), outro Córrego Danta (MG).

Alessandra Medina (2012) explana que a atriz estava sendo chantageada a pagar R$ 10.000,00 (dez mil reais) para não ter suas curvas divulgadas na rede. Os criminosos efetuaram 03 (três) ligações, bem como enviaram 05 (cinco) *e-mails* mostrando as fotos para o secretário da atriz, Alisson Oliveira, e seu empresário, Alex Lerner. Nesta oportunidade a atriz “foi orientada por autoridades de segurança a manter contato para tentar armar um flagrante”, mas não deu certo, segundo relatou seu advogado Antonio Carlos de Almeida Castro.

Desta feita, Guilherme Sardas informa como se deu a divulgação das fotos da atriz na rede, frente à recusa do pagamento pedido pelos *crackers*:

> Os criminosos pediram R$ 10.000,00 (dez mil reais) para não devassarem as curvas da atriz ao grande público, que ironicamente, figura na lista das musas ainda sonhadas pela revista playboy. **Sem terem o pedido atendido, em poucos minutos, soltaram na *web* a coleção de fotos, que, ajudada pela rápida proliferação do meio, ainda pode ser encontrada em diversos *sites***. (SARDAS, 2013, p. 59, **grifos nossos**).

Nesse ínterim, Marcelo Crespo explica sob qual tipificação serão enquadrados os delinquentes da ação penal promovida por Carolina Dieckmann,

tendo em vista a falta de legislação específica para invasão de dispositivo informático:

> A ação judicial promovida por Carolina deparou-se, porém, **com um obstáculo jurídico**, o mesmo que vem atenuando a punição em casos semelhantes que ocorreram há mais de uma década no Brasil. "**Se eu invadisse uma máquina e me valesse de informações confidenciais para ter um proveito financeiro, eu poderia responder por concorrência desleal, por extorsão, mas não pela invasão"**. [...], Por isso, os invasores responderão por crimes que a legislação brasileira já tipifica: **furto, extorsão e difamação.** (CRESPO, 2013, p. 59, grifo nosso).

Por fim, Marcelo Crespo (2013) declara que quem fizer o mesmo a partir de agora, vai ter tratamento diferente; uma vez que o caso da atriz foi determinante para a aprovação de uma lei específica sobre crimes cibernéticos.

3.2. A ORIGEM LEGISLATIVA E A RÁPIDA PROMULGAÇÃO DO DIPLOMA LEGAL SOBRE DELITOS INFORMÁTICOS

Segundo Liliana Paesani (2013) na segunda metade da década de 1990, com o advento da Internet e da globalização da economia, surge uma nova modalidade de crimes - denominados Crimes eletrônicos ou Crimes Virtuais – cometidos no espaço virtual da rede, através de: *e-mails*, *websites*, ou ocorridos em comunidades de relacionamentos na Internet, entre as quais a mais conhecida é o *Facebook*. Com isso, passou-se a exigir adaptações tecnológicas para garantir a segurança das transações comerciais, eletrônicas, transações bancárias *on-line* e do uso de senhas e demais mecanismos de segurança através da Internet.

A autora informa que o roubo de dados pessoais pela internet tornou-se comum, ocorrendo da seguinte maneira:

> **Por intermédio da instalação de programas espiões** (Trojans, Cavalos de Tróia, entre outros), **à revelia dos proprietários dos equipamentos informáticos, piratas virtuais infiltram-se nas máquinas para se apoderar de informações sigilosas dos seus proprietários**, tais como número de contas bancárias e de cartões de créditos, com as respectivas senhas, para realizar, indevidamente, transações financeiras fraudulentas. (PAESANI, 2013, p. 125, grifo nosso).

Luli Radfahrer (2013) relata que as transações eletrônicas *on-line* envolvendo identificação de senhas, certificação digital e demais mecanismos de segurança, têm-se revelado cada vez mais vulneráveis, uma vez que os recursos

tecnológicos para os crimes eletrônicos encontram-se muito mais sofisticados, uma verdadeira Pandemia Cibernética, pois:

> As pragas digitais são tantas e tão diversificadas que hoje configuram uma categoria de *software*: o ***malware***, do inglês *malicious software*. São ameaças como ***bots*** (que controlam computadores remotamente, criando redes de ataque ou distribuição), ***spyware*** (que monitoram as atividades de um sistema e enviam as informações coletadas), ***backdoors*** (que deixam a máquina desprotegida para a volta do invasor) e outros tantos, agindo isoladamente ou em conjunto e deixando a internet mais perigosa. Basta um ataque a uma rede como o ***Twitter*** para transformar os computadores de seus usuários em zumbis que disparam ***spans***. **Cibercrime é um braço em expansão do crime organizado e precisa ser combatido para garantir a qualidade de vida *on-line***. Desenvolver *malware* custa caro, precisa valer o investimento. **Sistemas de defesa podem tornar esse tipo de ação mais lenta e dispendiosa, bloquear serviços de redirecionamento de *links* e processar dados que aceitem depósitos de origem desconhecida**. Por mais complexo que seja o cibercrime, talento e dinheiro são uma combinação rara, e não é difícil identificá-la entre os principais suspeitos. (RADFAHRER, 2013, Jornal Folha de São Paulo. Caderno TEC, 25 fev. 2013, grifo nosso).

Segundo Fernando Galvão (2013) o Congresso Nacional vem discutindo o tema “legislação específica para internet” há mais de uma década. Em 24 de fevereiro de 1999, o deputado Luiz Piauhylino de Melo Monteiro do PSDB-PE apresentou o Projeto de Lei 84/99 sobre crimes cometidos na área de informática e suas penalidades. Dois anos depois, em meados de 2011 houve vários ataques de negação de serviço a *sites* do governo brasileiro. Devido a esse evento e demais casos, Patrícia Peck Pinheiro (2013) relatou que os deputados Paulo Teixeira (PT/SP), Luiza Erundina (PSB/SP), Manuel D’ávila (PCdoB/RS) e outros, apresentaram em 29 de novembro de 2011 o projeto de Lei n.º 2.793 dispondo sobre a tipificação criminal de delitos informáticos, alterando o Código penal. Mesmo diante de tamanhos problemas, os projetos continuaram em “*Stand By*”.

Spencer (2013) informou que somente depois de ter ocorrido o delito de extorsão pelo vazamento das fotos da atriz Carolina Dieckmann na rede, foi que o Congresso Nacional tomou providência, uma vez que o fato foi amplamente divulgado na mídia, ocasionando a pressão sobre o legislador para que surgisse algum tipo penal que tutelasse os dados informáticos.

Destarte, restaram aprovados os Projetos de Lei n. 35/2012 na Câmara dos Deputados, inicialmente originado pelo PL n. 2.793/2011, o qual foi apresentado como proposta alternativa ao PL n. 84/99. Oportunidade em que foram sancionados

e promulgados pela Presidência da República em 30 de novembro de 2012, através da Lei n. 12.737, apelidada de *Lei Carolina Dieckmann*.

Túlio Vianna (2013) elucida que a Lei 12.737, veio dispor sobre a tipificação criminal de delitos informáticos[7], bem como alterou o Código Penal brasileiro para acrescentar os artigos 154-A e 154-B, criando o tipo penal de "invasão de dispositivo informático". Pequenas modificações também foram realizadas nos artigos 266 e 298, ambos do CPB, para tipificar a "interrupção ou perturbação de serviço informático, telemático ou de informação de utilidade pública" e a falsificação de cartões de débito e crédito, respectivamente. Sendo assim, importante trazer à baila o referido diploma legal "*in verbis*":

> **LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.**
>
> Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.
>
> A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:
>
> Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.
> Art. 2º O Decreto-Lei n. 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
> **"Invasão de dispositivo informático**
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5ºAumenta-se a pena de um terço à metade se o crime for praticado contra:

[7] Delito informático pode ser tido como qualquer conduta constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com uso da informática em ambiente de rede ou fora dele, e que ofenda os elementos da segurança informática. (ROSSINI, 2004, p. 109-110).

I - Presidente da República, governadores e prefeitos;
II - Presidente do Supremo Tribunal Federal;
III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou;
IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."
"Ação penal
Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."
Art. 3º Os arts. 266 e 298 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:
"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública
Art. 266.....
§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública."
"Falsificação de documento particular
Art. 298.....
Falsificação de cartão
Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito."
Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.(http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm)

Com intuito de facilitar a compreensão da referida lei, bem como atender a expectativa do leitor; grandes doutrinadores como: César Roberto Bitencourt, Fernando Capez, Fernando Galvão, Guilherme de Souza Nucci, Luiz Regis Prado, participação de Marcelo Crespo, Rogério Greco e Túlio Vianna; formarão um conjunto harmônico de ideias, opiniões e ensinamentos dos referidos artigos do diploma legal – no que couber - quanto a: classificação doutrinária, bem jurídico tutelado, objeto material, ação nuclear, sujeitos ativo e passivo, tipicidades objetiva e subjetiva, tempo e local do delito, consumação e tentativa, modalidades equiparada e qualificada, modalidades comissiva e omissiva, benefícios legais, causas especiais de aumento de pena, pena, ação penal, suspensão condicional do processo, competência para julgamento e conflito aparente de normas.

O desenvolvimento desse conjunto será observado a partir dos tópicos 3.3, 3.4 e 3.5; abaixo declinados.

3.3. INVASÃO DE DISPOSITIVO INFORMÁTICO (ARTS. 154-A e 154-B do CP)

Segundo Nucci a *Classificação Doutrinária* do delito de Invasão de Dispositivo Informático:

> Trata-se de **crime comum** (pode ser cometido por qualquer pessoa); **formal** (delito que não exige resultado naturalístico, consistente na efetiva lesão à intimidade ou a vida privada da vítima, embora possa ocorrer); **de forma livre** (pode ser cometido por qualquer meio eleito pelo agente); **comissivo** (as condutas implicam ações); **instantâneo** (o resultado se dá de maneira determinada na linha do tempo), podendo assumir a forma de ***instantâneo de efeitos permanentes***, quando a invasão ou a instalação de vulnerabilidade perpetua-se no tempo, como rastro da conduta; **unissubjetivo** (pode ser cometido por uma só pessoa); **plurissubsistente** (cometido por vários atos). (NUCCI, 2013, p. 777, grifo nosso).

Quanto ao *Bem Jurídico Tutelado*, o autor explana:

> Insere-se no contexto dos crimes contra **a liberdade individual, bem jurídico mediato a ser tutelado**. Porém, de **forma imediata,** ingressou, com propriedade, no campo dos crimes contra a inviolabilidade dos segredos**, cuja proteção se volta à intimidade, à vida privada, à honra, à inviolabilidade de comunicação e correspondência, enfim, a livre manifestação do pensamento, sem qualquer intromissão de terceiros**. Sabe-se, por certo, constituir a comunicação telemática o atual meio mais difundido de transmissão de mensagem de toda ordem entre as pessoas físicas e jurídicas. O *e-mail* tornou-se uma forma padrão de enviar informes e mensagens a profissionais e particulares, seja para fins comerciais, seja para outras finalidades das mais diversas possíveis. As redes sociais criaram, também, mecanismos de comunicação, com dispositivos próprios de transmissão de mensagens. Torna-se cada vez mais rara a utilização de cartas e outras bases físicas, suportando escritos, para a comunicação de dados e informes. Diante disso, criou-se novel figura típica incriminadora, buscando punir quem viole não apenas a comunicação telemática, mas também os dispositivos informáticos, que mantém dados relevantes do seu proprietário. (NUCCI, 2013, p.774-775, grifo nosso).

Capez elucida sobre a *Ação Nuclear* dos referidos artigos:

> **O núcleo central da conduta típica consubstancia-se no verbo "invadir**", isto é, **ingressar virtualmente, sem autorização expressa ou tácita do titular do dispositivo**. A conduta de invadir traz ínsita a ausência de autorização do proprietário ou usuário do dispositivo, pois **não se pode dizer que houve invasão quando o acesso se dá mediante sua aquiescência**. Mesmo assim, o tipo penal do art. 154-A, *caput*, do CP, de modo supérfluo, repete ao final a exigência do elemento normativo do tipo "sem autorização expressa ou tácita do titular do dispositivo". (CAPEZ, 2013. p. 346, grifo nosso).

Bem como o *Objeto Material:*

> **O crime consiste em invadir dispositivo informático alheio** (o equipamento *hardware*) utilizado para rodar programas (*softwares*),

> ou ser conectado a outros equipamentos. **Exemplos: computador, *tablet*, *smartphone*, memória externa (*HD* externo), entre outros**. O dispositivo informático deve ser de titularidade de terceiros podendo ou não estar conectado à internet. A invasão deve se dar por meio de violação indevida de mecanismo de segurança estabelecido pelo usuário do dispositivo. Como exemplos de mecanismos de segurança, podemos citar: ***firewall,* antivírus, *antimalware*, *antispyware*, senha restrita para acesso pessoal do usuário** etc. O crime em tela exige também a finalidade especial do agente de buscar a obtenção, a adulteração ou a destruição de dados ou informações. Sem este fim especial, o delito não se aperfeiçoa. (Ibidem, p. 346, grifo nosso).

Túlio Vianna (2013, p. 94, grifo nosso) explica os *Sujeitos Ativo e Passivo*, onde: "O **sujeito ativo** é qualquer pessoa humana não autorizada a acessar os dados, exceto o proprietário do dispositivo informático no qual os dados estão armazenados" e "**sujeito passivo** é qualquer pessoa, física ou jurídica, proprietária dos dados informáticos, ainda que não necessariamente do sistema computacional".

Coube ao Cesar Roberto Bitencourt lecionar sobre a *Tipicidade Objetiva*:

> **Trata-se de um tipo penal complexo** que conta com um *elemento normativo especial da antijuridicidade* – **mediante violação indevida de mecanismo de segurança** – e com *dois elementos subjetivos especiais do injusto* – (i) com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita – cuja análise faremos em tópicos individuais, decompondo-se, assim, o seu exame, para a maior clareza de suas funções dogmáticas. Contém, no entanto, apenas uma conduta nuclear no *caput*, qual seja, "invadir", que tem o significado de entrar à força, ou de forma arbitrária ou hostil, sem o consentimento de quem de direito. A *invasão* tem a finalidade, em regra, de impedir ou embaraçar o curso normal de um trabalho. Nessa hipótese, contudo, o objetivo é outro, como veremos em tópico apartado (fim especial), bem como o próprio significado de *invadir* que, nesta figura típica, não significa o ingresso forçado ou arbitrário de *extraneus* em espaço não autorizado. Na verdade, *invadir*, neste caso, tem o significado de violar ou ingressar, clandestinamente, isto é, sem autorização ou permissão de que de direito, sem o consentimento do proprietário ou titular do *dispositivo informático*. [...]. Com efeito, a conduta é executada, segundo o próprio tipo penal, "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". (BITENCOURT, 2014, p. 680, grifo nosso).

Nucci expõe a *Tipicidade Subjetiva*:

> **É o dolo**. Há elemento subjetivo do tipo específico para as duas condutas previstas no tipo. **No tocante à invasão de dispositivo informático** é o fim de obter, adulterar ou destruir dados ou informações. Focaliza-se a obtenção (ter acesso a algo), a adulteração (modificação do estado original) ou a destruição

> (eliminação total ou parcial) de dados (elementos apropriados à utilização de algo) ou informações (conhecimento de algo em relação a pessoa, coisa ou situação). **Quanto à instalação de vulnerabilidade** é a obtenção de vantagem ilícita (qualquer lucro ou proveito contrário ao ordenamento jurídico). Pode ser, inclusive, a obtenção da invasão do dispositivo informático em momento posterior para obter dados e informações. **Não se pune a forma culposa**. (NUCCI, 2013, p.776, grifo nosso).

Túlio Vianna adentra ao mérito do *Tempo* e *Local do Delito:*

> O art. 4º do CPB adota, para a fixação do momento do crime, **a teoria da atividade**. Assim, a invasão de dispositivo informático será considerada realizada **no momento em que foi emitido o comando ou a sequência de comandos, destinados inequivocadamente a causar um acesso não autorizado aos dados do dispositivo informático**. O art. 6º do CPB adota, para a fixação do local do delito, a **teoria da ubiquidade**. Assim, a invasão a dispositivo informático será **considerada praticada tanto no local da execução (lugar do dispositivo informático do invasor) quanto no local da consumação (lugar do dispositivo informático invadido)**. Se forem distintos os países onde se deram a execução e a consumação do delito, **para que o agente possa ser punido é necessário que a conduta seja típica em ambos os países**. (VIANNA, 2013, p. 97-98, grifo nosso).

Capez leciona sobre a *Modalidade Equiparada*:

> Também será responsabilizado com a pena de detenção, de 3 (três) meses a 1 (um) ano, e multa, **quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a invasão de dispositivo informático alheio**. São os programas popularmente chamados “cavalos de troia”, que nada mais são do que *softwares* (programas de computador) utilizados para permitir a invasão do computador alheio. Há programa de computador que funciona como espião, e fica coletando os dados digitados no computador alheio, **o que possibilita a violação de informações sigilosas, como senhas de contas e cartões de crédito**. Além dos programas de computador (*software*) destinados à invasão indevida de outros dispositivos informáticos. São os famosos “chupa-cabras”, aparelhos utilizados para violação informações digitais de terceiros, e, com isso, obter lucro indevido. (CAPEZ, 2013, p. 348, grifo nosso).

Nucci retoma ao debate para elucidar sobre a *Modalidade Qualificada*:

> Trata-se de figura peculiar. Pela redação conferida pelo legislador, num primeiro momento, poder-se-ia sustentar a existência de um crime qualificado pelo resultado, pois se menciona: *se da invasão resultar*... Imagine-se que, diante da invasão ao dispositivo informático, ocorreria um segundo resultado qualificador. Entretanto, tal avaliação é somente aparente. Na essência, cuida-se de crime qualificado. **O foco da qualificação é a valoração feita no tocante aos dados e informações obtidos. Quando o agente alcança qualquer dado ou informe, configura-se o *caput***. Porém, quando obtiver, como dado ou informe, ou conteúdo de comunicação eletrônica privada (como o *e-mail* armazenado no disco rígido do computador), segredos comerciais ou industriais (informe sigilosos

> de interesse dos negócios comerciais ou da atividade produtiva da indústria) ou informações sigilosas, assim definidas em leis [...], **Qualifica-se o delito, elevando-se a faixa de cominação das penas**. A segunda parte do §3º espelha uma autêntica situação de **qualificação pelo resultado**, vale dizer, o agente obtém dados ou informes do computador da vítima e ainda mantém *controle remoto* do dispositivo invadido. O controle remoto significa instalar mecanismo apropriado para dominar o dispositivo informático à distância, sem autorização. Portanto, **além de violar dados e informes da vítima, provoca o agente a possibilidade de controlar o aparelho quando bem quiser**. **O duplo resultado qualifica o crime, embora ambos continuem voltados à tutela da intimidade e da vida privada**. (NUCCI, 2013, p.778-779, grifo nosso).

Nucci contribui ainda, com o entendimento sobre os *Benefícios Legais*:

> **Mesmo a forma qualificada é infração de menor potencial ofensivo, comportando transação**. À sua falta, outros institutos podem ser aplicados (penas restritivas de direitos, regime aberto etc.) Outro fator peculiar diz respeito à forma qualificada do delito consistir figura subsidiária, ou seja, **somente se pune caso inexista delito mais grave, como, por exemplo, a divulgação de segredo prevista no art. 153, §1º-A do Código Penal**. (Ibidem, p.779, grifo nosso).

Rogério Greco traz as *Causas Especiais de Aumento de Pena*:

> No que diz respeito ao § 2º do art. 154-A do Código Penal, **é importante frisar que o aumento de um sexto a um terço somente será aplicado às hipóteses constantes do *caput*, bem com de seu § 1º, tendo em vista a situação topográfica, devendo-se aplicar a regra hermenêutica que determina que os parágrafos somente se aplicam às hipóteses que lhe são anteriores**. Além disso, o aumento somente será possível no critério trifásico, previsto pelo art. 68 do Código Penal, **se ficar comprovado que o comportamento praticado pelo agente trouxe, efetivamente, prejuízo econômico à vítima**. Conforme determina o § 4º, na hipótese do §3º, ou seja, se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido, **a pena será aumentada de um a dois terços se houver divulgação, comercialização ou transmissão à terceiro, a qualquer título, dos dados ou informações obtidos.** Finalmente, **a pena ainda será aumentada de um terço até a metade** se quaisquer dos crimes (previstos no *caput*, §§ 1º e 3º do art. 154-A do Código Penal) **forem praticados contra as autoridades mencionadas no § 4º do art. 154-A** do diploma repressivo. (GRECO, 2014, p. 475, grifo nosso).

Greco complementa o tema com o *Concurso de Causas de Aumento de Pena*:

> Poderá ocorrer a hipótese em que, no caso concreto, **seja vislumbrada a possibilidade de aplicação de mais de uma majorante**. Assim, imagine-se a hipótese em que o agente, **em virtude da invasão de dispositivo informático alheio, tenha causado prejuízo econômico** (§ 2º do art. 154-A do CP), **bem como esse fato tenha sido cometido em face do Presidente do**

> **Supremo Tribunal Federal** (Inc. I do § 5º do art. 154-A do CP). Nesse caso, poderíamos aplicar, simultaneamente, as duas causas especiais de aumento de pena? Como resposta, prevalecerá a regra constante do parágrafo único do art. 68 do Código Penal, que diz no concurso de causas de aumento de pena ou de diminuição, previstas na parte especial, **pode o juiz limitar-se a um só aumento ou a uma só diminuição, prevalecendo, todavia, a causa que mais aumente ou diminua**. (GRECO, 2014, p. 477, grifo nosso).

Luiz Regis Prado explana *Pena e Ação Penal*:

> **A pena** prevista para o delito do artigo 154-A **é de detenção, de 3 (três) meses a 1 (um) ano, e multa**.
> Como observado, se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido, **a pena passa a ser de reclusão, de 6 (seis) meses a 2 (dois) anos, e multa**, se a conduta não constituir crime mais grave (§3º).
> O artigo 154-B determina que a **ação penal** nos delitos definidos pelo artigo 154-A será **pública condicionada**, **salvo** se o crime é cometido contra **Administração Pública Direta ou Indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos**, hipótese em que a **ação é pública incondicionada**. (PRADO, 2014, p. 869, grifo nosso).

Fernando Galvão elucida (2013, p. 480) a *Suspensão Condicional do Processo*: “Considerando que a pena mínima cominada ao crime em exame é inferior a um ano de privação da liberdade, será possível a suspensão condicional do processo, desde que atendidos os demais requisitos estabelecidos no art. 89 da Lei n. 9.099/95”.

O autor também explana a *Competência para Julgamento*:

> A competência para processar e julgar o crime é **do Juizado Especial da Justiça comum estadual**. No entanto, **a competência será do Juizado Especial da Justiça comum Federal** quando o crime for cometido contra a administração pública, direta ou indireta, de qualquer dos Poderes da União, quando cometidos a bordo de navios ou aeronaves brasileiras, quando o sujeito ativo ou a vítima for funcionário público federal no exercício de suas funções (inciso IV do art. 109 da CF – Súmula n. 147 do STJ), ou se houver concurso com um crime da competência da Justiça Federal (Súmula n. 122 do STJ). (GALVÃO, 2013, p. 480).

Fernando Galvão com o fim de agregar mais valor a temática apresenta três casos de *Conflito Aparente de Normas*:

> **Invasão de dispositivo Informático para a realização de outro crime**. O crime de *invasão de dispositivo informático* deve ser absolvido, em razão do princípio da consunção, quando realizado como meio necessário para a execução de outros crimes, por exemplo, em relação ao crime de extorsão (art. 158 do CP). Especial

> atenção merece a hipótese em que a invasão ocorre para o fim de instalar vulnerabilidade que visa à obtenção de uma vantagem indevida. Se a obtenção da vantagem indevida constituir crime, como é o caso da transferência bancária de valores que se utiliza de senha obtida por meio de vulnerabilidade indevidamente instalada no dispositivo informático, deve-se reconhecer apenas a ocorrência do crime patrimonial. O crime de *invasão de dispositivo informático*, que tutela a inviolabilidade de segredos, constitui apenas um meio necessário para posterior execução do crime contra o patrimônio. Nesse sentido, o crime de *invasão de dispositivo informático* somente será punido quando a conduta criminosa for interrompida antes de iniciar a execução do crime patrimonial. (GALVÃO, 2013, p. 480-481, grifo nosso).
>
> **Invasão de dispositivo informático e violação de correspondência eletrônica**. A interceptação de mensagem ao ambiente eletrônico constitui crime, previsto no art. 10 da Lei n. 9.296/96, que visa proteger a inviolabilidade da correspondência eletrônica. O aparente conflito entre as disposições incriminadoras da *invasão de dispositivo informático* e da *violação de correspondência eletrônica* deve ser resolvido com base no princípio da especialidade. O crime de *violação de correspondência eletrônica* deve ser considerado específico em relação ao crime de *invasão de dispositivo informático*, de modo que, se a *invasão do dispositivo informático* ocorrer para a interceptação de mensagem eletrônica, deve-se reconhecer apenas a ocorrência do crime específico de *violação de correspondência eletrônica*, o qual é previsto no art. 10 da Lei n. 9.296/96. (Ibidem, p. 481, grifo nosso)
>
> **Invasão de dispositivo informático e quebra de sigilo bancário**. Também em razão do princípio da especialidade, a previsão para o crime de *invasão de dispositivo informático* não possui aplicação quando a conduta for direcionada para a obtenção das informações bancárias que caracterizam o crime de *quebra de sigilo bancário*. Nos termos do art. 10 da LC n. 105/2001, a *quebra de sigilo bancário*, fora os casos autorizados, constitui crime e sujeita os responsáveis à pena de reclusão, de um a quatro anos, e multa. Nesse caso, a incriminação específica para o crime de *quebra de sigilo bancário* afasta a incidência da previsão incriminadora genérica para o crime de *invasão de dispositivo informático*. (Ibidem, p. 481, grifo nosso).

Feitas as devidas ponderações acerca do primeiro artigo da Lei 12.737/12 - Carolina Dieckmann - passaremos para o tópico seguinte, o qual se destina avaliar o segundo artigo.

3.4. INTERRUPÇÃO DE SERVIÇO TELEMÁTICO OU DE INFORMAÇÃO DE UTILIDADE PÚBLICA (ART. 266, § 1º e § 2º do CP)

Rogério Greco dá início a temática, razão pela qual explana a *Classificação Doutrinária*:

> **Crime comum**, tanto no que diz respeito ao sujeito ativo quanto ao sujeito passivo; **doloso**; **comissivo** (podendo, nos termos do art. 13,

> § 2º, do Código Penal, ser praticado via omissão imprópria, na hipótese de o agente gozar do status de garantidor); de **perigo**; de **forma livre**; **instantâneo**; **monossubjetivo**; **plurissubsistente**; **não transeunte**. (GRECO, 2014, p. 872, grifo nosso).

Tulio Vianna expõe *o Bem Jurídico Tutelado*:

> Trata-se de crime **contra a incolumidade pública**, o que pode ser facilmente constatado até mesmo por sua localização no "Título VIII" do CPB. Esse crime, portanto, **abarca tão somente condutas que atingem um número indeterminado de pessoas** e nunca a uma vítima ou grupo de vítimas determinado.
>
> A conduta de quem interrompe o serviço de Internet, entendida como uma espécie de serviço telemático, de **uma residência ou mesmo de um prédio inteiro jamais poderia ser tipificada no art. 266, § 1º, do CPB**, pois falta a ela a lesão ou perigo de lesão a um número de pessoas indeterminado.
>
> Por outro lado, os serviços devem ser públicos, **não se tipificando o crime caso seja praticado em grandes redes privadas (Intranets), ainda que afetando um número indeterminado de pessoas**.
> Para que o crime se consume **é indispensável que a interrupção ou perturbação do serviço de natureza pública cause um perigo de dano a um número indeterminado de vítimas**, o que ocorrerá quando o ataque for dirigido ao provedor de serviços, aos servidores de nomes de domínio (especialmente aos servidores raízes) ou à própria infraestrutura da rede. (VIANNA, 2013, p. 104, grifo nosso).

Cesar Roberto Bitencourt leciona o *Objeto Material*:

> O objeto material desta infração penal é o **serviço** […], ***telemático ou de informação pública***. […], ***Serviço telemático*** refere-e ao processamento de dados, produto da pós-modernidade e da era digital. ***Serviço de informação pública*** é aquele que tem como destinatário direto a coletividade como um todo, e não apenas determinado órgão oficial, não se prestando como tal, por exemplo, os chamados "serviços de inteligência", especialmente das autoridades repressoras. (BITENCOURT, 2014, p. 1125, grifo nosso).

Nucci elucida a *Análise do Núcleo do Tipo*:

> *Interromper* significa fazer cessar ou romper a continuidade. A conduta se volta a serviço telemático (transmissão de informes por meio de computador combinado com outros meios de telecomunicação; por exemplo: modem, banda larga, cabo, etc.) ou *serviço de informação de utilidade pública* (hipótese genérica, sem especificação apropriada, ferindo a taxatividade, visto poder se dar em qualquer linha de transmissão). Outra peculiaridade é a menção a serviço informático, no título do crime, sem a sua inserção no tipo penal, logo, inaplicável. Entretanto, o termo telemática já é suficiente para o cenário ora proposto. As figuras alternativas, tal como ocorre no caput são: impedir (impossibilitar a execução de algo) e dificultar (tornar algo mais custoso, colocando obstáculo). Voltam-se ao restabelecimento do serviço interrompido. Logo, responde pelo crime tanto quem interrompe o serviço como quem impede ou dificulta o seu restabelecimento. Se for o mesmo agente para todas as

> condutas, responde por um só crime, pois se trata de tipo misto alternativo. (NUCCI, 2013, p. 1075).

Capez (2013, p. 547) ensina os *Sujeitos Ativo e Passivo* do delito. “Sujeito Ativo: Qualquer pessoa pode praticá-lo” e “Sujeito Passivo: É a coletividade em geral”.

Nucci informa (2013, p. 1075) que o *Elemento Subjetivo do Tipo* “é o dolo de perigo (gerar risco intolerável a terceiros). Não há elemento subjetivo específico, nem se pune a forma culposa”.

No que tange a *Consumação e Tentativa*, Capez (2013, p. 547) relata que o delito “Consuma-se com a prática dos atos que interrompam, perturbem o serviço ou que impeçam ou dificultem seu restabelecimento. Cuida-se aqui mais uma vez de crime de perigo abstrato, isto é, presumido. A tentativa é admissível”.

Há que se perscrutar as *Modalidades Comissiva e Omissiva*, oportunidade em que Greco as elucida:

> Os núcleos interromper, perturbar, impedir e dificultar **pressupõem um comportamento comissivo levado a efeito pelo agente**. No entanto, poderá o delito ser praticado via **omissão imprópria quando o agente, garantidor, dolosamente, podendo, nada fizer para evitar a prática da infração penal em exame**, devendo ser, portanto, responsabilizado pelo delito de interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, nos termos do § 2º do art. 13 do Código Penal. (GRECO, 2013, p. 872-873, grifo nosso).

Greco informa também a *Causa Especial de Aumento de Pena*:

> […], § 2º Aplicam-se as **penas em dobro se o crime é cometido por ocasião de calamidade pública**. A majorante terá aplicação, portanto, quando o fato for praticado por ocasião de calamidade pública, isto é, conforme explica Mirabete, durante “uma situação excepcional, de infortúnio ou desgraça coletiva” a exemplo das epidemias, guerra, terremoto, inundações etc. (Ibidem, p. 873, grifo nosso).

Túlio Vianna explica os *Benefícios Legais, Ação Penal*, a *Suspensão Condicional do Processo* e a *Competência para Julgamento*:

> Tem-se um crime que é processado mediante **ação penal pública incondicionada** em que, considerando os patamares mínimo e máximo cominados ao delito em apreço (**detenção, de um a três anos, e multa**), **há a possibilidade de aplicação da suspensão condicional do processo** (art. 89 da Lei nº 9.99/95). Contudo, se a conduta do art. 266 do CPB for cometida por ocasião de **calamidade pública, a pena deverá ser duplicada**, e, portanto, **inviável será a aplicação do benefício da suspensão condicional do processo**. Isto porque a pena mínima que, *a priori*, era de um ano, será

> obrigatoriamente de dois anos. Por fim, ressalta-se que, como **a pena máxima em abstrato excede a dois anos**, a competência para julgamento do **crime é do juízo comum** e não do **JECrim**. (VIANNA, 2013, p. 106, grifo nosso).

Concluído o desafio proposto no segundo artigo, passaremos, neste momento, à análise do terceiro artigo da Lei Dieckmann.

3.5. FALSIFICAÇÃO DE DOCUMENTO PARTICULAR CONFIGURADO NO CARTÃO DE CRÉDITO OU DÉBITO (ART. 298, Parágrafo Único)

Segundo Greco a *Classificação Doutrinária* do delito em comento é:

> **Crime comum**, tanto no que diz respeito ao sujeito ativo quanto ao sujeito passivo; **doloso** (não havendo previsão para a modalidade de natureza culposa); **comissivo** (podendo, nos termos do art. 13, § 2º, do Código Penal, ser praticado via omissão imprópria, na hipótese de o agente gozar do *status* de garantidor); de **forma livre**; **instantâneo**; **monossubjetivo**; **plurissubsistente**; **não transeunte**. (GRECO, 2014, p. 955, grifo nosso).

Luiz Regis Prado (2014, p. 1269) leciona que o *Objeto Jurídico Tutelado* é “a fé pública, expressada na exigência de confiança nos instrumentos e papéis privados”.

Rogério Greco elucida (2014, p. 955) que o *Objeto Material* é “o documento particular falsificado, no todo ou em parte, ou o documento particular verdadeiro que foi alterado pelo agente”.

Capez (2013, p. 596) explana as *Ações Nucleares* do delito em estudo, “assim como o precedente, pune a falsidade material, ou seja, aquela que diz respeito à forma do documento. Assim, as ações nucleares típicas consubstanciam-se nos verbos falsificar ou alterar, no caso, documento particular”. O autor lembra ainda que “a falsidade grosseira poderá constituir crime impossível ou delito de estelionato”.

Nucci (2013, p. 1135) ensina sobre os *Sujeitos Ativo e Passivo*, sendo que: “Sujeito Ativo pode ser qualquer pessoa. O Sujeito Passivo é o Estado, em primeiro plano. Secundariamente, pode ser a pessoa prejudicada pela falsificação”.

Nucci explica ainda (2013, p. 1135) a *Análise do Núcleo do Tipo:* “Falsificar, […], quer dizer reproduzir, imitando, ou contrafazer. […], O objeto é documento particular. O tipo penal preocupa-se com a forma do documento, por isso cuida da falsidade material”.

Luiz Regis Prado relata sobre o *Tipo Subjetivo* o qual é representado:

> Pelo dolo, consubstanciado na vontade livremente dirigida no sentido da falsificação do documento particular. Não é preciso, pois, que o agente tenha sido impelido por um especial interesse de prejudicar terceiro ou de obter vantagem como decorrência do falso, malgrado a potencialidade para tanto seja essencial à existência do delito. (PRADO, 2014, p. 1270).

Capez informa que há de *Concurso de Crimes* na seguinte hipótese:

> Clonagem de cartão de crédito e estelionato: STJ: "Habeas corpus. Processual Penal. Crimes de falsificação de documento particular (clonagem de cartões de crédito) e estelionato. (…) O maquinário utilizado pelo paciente para reproduzir cartões de crédito de terceiros continuava apto a cometer novos crimes, ao reter informações de crédito e identificação particulares, persistindo assim a sua eficácia para atos futuros, não se aplicando, assim, o disposto no enunciado da Súmula 17, do Supremo Tribunal de Justiça. 4. Ordem denegada" (STJ, HC 43952/RJ, 5ª T., Relª Minª Laurita Vaz, j. 15.8.2006, DJ 11-9-2006, p. 317). (CAPEZ, 2013, p. 597).

Marcelo Crespo entra no debate para criticar a lei no que tange a equiparação do uso de cartões de débito e crédito, sem autorização, com a falsificação de documentos:

> Um ponto da lei equipara o uso de dados de cartões de débito e crédito sem autorização do titular à falsificação de documento (art. 298), com penas de 01 (um) a 5 (cinco) anos de prisão e multa.
> Para o autor, **a alteração proposta pela lei é inócua. "Se eu utilizo cartão falso para obter uma vantagem indevida, eu já respondo por estelionato, que já é tipificado no Código Penal. A justiça já entende isso de maneira muito tranquila".** (CRESPO, 2013, p. 60-61, grifos nossos).

Rogério Greco traz as *Modalidades Comissiva e Omissiva*:

> Os núcleos falsificar e alterar pressupõem um comportamento comissivo por parte do agente. No entanto, o delito poderá ser praticado via omissão imprópria na hipótese em que o agente, garantidor, dolosamente, nada fizer para evitar a prática da infração penal, devendo, portanto, ser responsabilizado nos termos do art. 13, § 2º, do Código Penal. (GRECO, 2014, p. 955-956).

O autor elucida ainda sobre a *Pena*, *Ação Penal* e *Suspensão Condicional do Processo:*

> A pena cominada ao delito de falsificação de documento particular **é de reclusão, de 1 (um) a 5 (cinco) anos, e multa**. A ação Penal é **de iniciativa pública incondicionada**. Será possível a confecção de proposta de suspensão condicional do processo, nos termos da Lei 9.099/95). (GRECO, 2014, p. 956, grifo nosso).

Túlio Vianna (2013, p. 107, grifo nosso) expõe que “A *Competência de Julgamento* do crime de falsificação de cartão é do **juizado comum**”.

Este debate, embora tenha sido elaborado com riqueza de detalhes, não esgota as peculiaridades do referido diploma legal.

4. OS EFEITOS DA LEI CAROLINA DIECKMANN

No que concerne à dimensão da mudança social, Liliana Minardi Paesani (2013, p. 128) declara: “inequívoco afirmar que a Lei dos Delitos Informáticos, ao alterar o Código Penal, almeja prevenir a ação delituosa, porém, não possui o alcance de promover mudança na estrutura social”.

Quanto ao alcance desta mudança, a autora diz que aferir essa possibilidade dependerá da futura efetividade que o instituto poderá demonstrar, particularmente do fundamento para ações do Ministério Público e decisões do Poder Judiciário, como fator de inibição dos delitos eletrônicos.

4.1. ASPECTOS POSITIVOS (AVANÇOS)

Tânia Maria Cardoso Silva Amâncio (2013) explana que são patentes as diversas mudanças no cotidiano da sociedade a partir do desenvolvimento da informática, sobretudo da internet, uma vez que esta permitiu as pessoas estarem presentes em todo o mundo a partir da tela de um computador.

Elucida-se que além da evolução trazida pela globalização, a informática também revolucionou todos os segmentos e atividades da sociedade moderna, principalmente pela exposição às muitas formas de crimes e criminosos, que buscam obter lucros, furtar dados e propagar atos de crueldade, sob o manto da impunidade.

Nesse contexto, a autora afirma que a fragilidade das leis foi fator preponderante para o surgimento *cybercrimes*, razão pela qual fez-se necessária a criação de lei específica:

> A fragilidade das leis brasileiras foi um dos fatores que mais contribuíram para que surgissem novos crimes, especialmente nos últimos vinte anos, no ambiente virtual. É certo que muitas condutas podiam ser abrangidas por disposições já existentes na Constituição Federal, no Código Civil, no Código Penal, no Estatuto da Criança e do Adolescente, mas a criação de leis específicas para este tipo de criminalidade se tornou cada vez mais impositiva. […], Nesse sentido, **merece destaque a Lei Carolina Dieckmann, que pode ainda se apresentar limitada, porém se revelou um grande salto na proteção às vítimas de crimes perpetrados na internet**. (AMÂNCIO, 2013, p. 28, grifo nosso).

Wanderlei José dos Reis (2013) ressalta que a alteração da legislação penal para a tipificação dos crimes cometidos via internet, através da Lei 12.727/12, veio ao encontro das necessidades sociais, uma vez que visa coibir práticas delituosas, que de alguma forma aufere vantagem indevida às vítimas. Sendo assim, a Lei Carolina Dieckmann representa um avanço legislativo pátrio, já que a tutela cibernética criou um novo bem jurídico – o dispositivo informático.

4.1.1. A Repercussão do Episódio da Atriz foi Relevante para a Célere Aprovação da Lei

Auriney Brito (2013, p. 67-68) declara que “a segurança informática, entendida como a *disponibilidade*, *confidencialidade* e *integridade* das informações dos usuários, há tempo já clamava por proteção jurídico-penal”.

Renato Opice Blum (2012, p.110) acrescenta que “o debate sobre uma legislação específica para a internet se arrastava em velocidade de conexão discada havia mais de uma década, mas ganhou ímpeto depois da invasão do computador da atriz global Carolina Dieckmann”.

Segundo reportagem com alguns especialistas do Direito, concedida a Guilherme Sardas, dentre eles: Hélio Bressan (Titular da 4ª Delegacia de Meios Eletrônicos de São Paulo), Thiago Tavares (Presidente da ONG Safernet Brasil), Marcelo Crespo (Advogado Especialista em Crimes Digitais), Marcos Manzoni (Diretor Presidente do Serpro) e Caio Cesar Carvalho (Advogado Especialista em Direito da Tecnologia da Informação) é unânime que a grande repercussão do episódio, por envolver uma atriz famosa, foi determinante para a rapidez da aprovação da lei.

Nesse ínterim, Hélio Bressan (2013, p. 59) se manifesta: “A pressão da opinião pública, nesse caso, de fato influenciou a célere reação do Congresso Nacional”.

Para Auriney Brito (2013) o caso da atriz Carolina Dieckmann deu velocidade à tramitação do processo legislativo e ensejo à mudança – embora não tenha sido o primeiro caso de extorsão e divulgação de conteúdo sigiloso na internet - mas devido a grande repercussão midiática acelerou a criação da lei no âmbito penal. Salienta-se que a nova lei de crime informático não está em desequilíbrio

holísitico, pois vem satisfazer grande parte das necessidades de criminalização de condutas intoleráveis na Sociedade da Informação.

4.1.2. O Advento da Lei Trouxe Segurança Jurídica e Maior Rigor Penal

Segundo Renato Opice Blum, especialista em crimes de internet, mesmo com falhas, o avanço pelo advento da lei é inegável, pois:

> O Brasil tem a quinta maior população de usuários de internet do mundo, com 70 milhões de pessoas, que passam em média 25 horas por mês online. **Com uma movimentação dessas já era hora de termos segurança jurídica para nossos usuários**. (BLUM, 2012, p. 110, grifo nosso).

Liliana Minardi Paesani (2013) explana que a promulgação da Lei dos Delitos Informáticos é mais uma etapa do amoldamento do Direito brasileiro à sociedade da informação, uma vez que a atualização normativa e o recurso ao aparelho judiciário não são os únicos mecanismos de acomodação de conflitos nas sociedades complexas; no entanto, essa inovação legislativa é vista como um movimento de positivação jurídica que vem somar-se, no sentido de combater o crime cibernético no Brasil.

Para Marcos Mazoni (2013, p.60) “a lei é positiva no sentido de estabelecer maior rigor penal – as penas variam de um a três anos de detenção mais multa. Esperamos que isso possa causar uma sensação de que o risco de punição é maior, apesar de não ser uma relação direta."

Wanderlei José dos Reis leciona que por não haver no nosso ordenamento jurídico a tipificação de crimes cometidos via internet, o magistrado era obrigado a se utilizar da analogia para aplicar a legislação que versava sobre condutas semelhantes já tipificadas, conforme exemplo:

> **A violação de e-mail era enquadrada como crime de violação de correspondência, previsto na Lei nº 6.538/78**, que, em seu art. 40, estatui que é crime devassar indevidamente o conteúdo de correspondência fechada dirigida a outrem, estabelecendo a pena de detenção, de até seis meses, ou o pagamento não excedente a vinte dias-multa. (REIS, 2013, p. 33, grifo nosso).

Nesse diapasão, Renato Opice Blum (2012) reitera que antes do advento da Lei Carolina Dieckmann a polícia e os juízes tinham que fazer

malabarismos para tentar enquadrar os criminosos, vez que toda a legislação já existente era pré-internet, e acrescenta:

> Pode parecer estranho, **mas até a publicação da Lei 12.737, invadir dispositivos informáticos no Brasil não era crime**. […], Casos como o de Carolina eram decididos com adaptações de artigos que já constavam no Código Penal brasileiro. (BLUM, 2013, p. 62, grifo nosso).

Desta feita, Blum (2013) espera que com a nova legislação, a justiça seja mais ágil, por estar munida de instrumentos próprios, capazes de criminalizar a invasão de dispositivos informáticos.

4.2. ASPECTOS NEGATIVOS (LACUNAS)

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

Ressalte-se que muitos doutrinadores e operadores do direito digital questionaram a brandura das penas cominadas aos delitos informáticos ora consubstanciados na lei Carolina Dieckmann, frente aos danos causados às vítimas. Misael Neto Bispo da França (2013) atesta que penas sem o mínimo de força dissuasória não previne a ocorrência e a recorrência de comportamentos criminosos, pelo contrário – diz Renato Opice Blum (2013) – ao invés de coibir pode estimular a prática delituosa. Quanto aos danos causados às vítimas, apresentam-se de formas variadas: isolamento, ansiedade, depressão, superação e suicídio.

Estas e outras lacunas serão melhor discutidas e pontuadas abrangentemente nos tópicos a seguir.

4.2.1. Divergência dos Juristas e doutrinadores Sobre o Termo “Invasão” no que Tange à Medida Violenta e Mecanismos de Segurança

Flávia Penido, Advogada e Professora de Direito Digital, relata a discussão de alguns juristas acerca do artigo 154-A do diploma legal, o qual preconiza:

> 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. (PENIDO, 2013, p. 3, grifo nosso).

Para a autora o texto é claro, mas já há polêmicas instauradas:

> Alguns juristas entendem que **o verbo “invasão” requer medida violenta para que o crime se configure; outros ainda questionam a necessidade de “mecanismo de segurança**”. Segundo alguns especialistas, em não havendo senha, tela de bloqueio ou anti-vírus, não há ocorrência do crime previsto no art. 154-A. (Ibidem, p.3, grifo nosso).

Para Auriney Brito (2013, p. 69) é importante “que se observe cada elementar do crime para que se tenha total noção dos limites da imputação penal”. No caso o verbo núcleo do tipo invadir seria “entrar sem autorização do proprietário”. Já a elementar mediante violação indevida de mecanismo de segurança significa que “só haverá o crime do art. 154-A se o autor da conduta usar sua habilidade para superar a proteção do sistema informático, por mais simples que ela seja”.

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

Por outro viés, Auriney Brito expõe duas análises no que tange à prática do *phishing*[8]:

> Em primeira análise, […], conclui-se que **o criminoso poderá ser punido pelo art. 154-A do CP, mesmo que a própria vítima tenha liberado o acesso**, ela não agiu de forma consciente, foi induzida em erro, considerando-se portanto, que houve violação indevida da segurança do computador. (BRITO, 2013, p. 70).

A segunda análise consubstancia-se:

[8] Aglutinação dos termos americanos *password* (senha) e *fishing* (pescaria), que nada mais é que a utilização de técnicas de engenharia social com o objetivo de *pescar* as senhas das vítimas, principalmente as senhas de internet bank. […], O criminoso faz com que a própria vítima entregue as informações que ele precisa, ou que ela mesma desabilite sua segurança para que ele possa acessar livremente os dados. (BRITO, 2013, p.70-87).

> Porém, se com a habilidade o criminoso conseguir que a vítima entregue o conteúdo informático, **sem que haja invasão**, não há que se falar em crime por ausência do verbo núcleo do tipo. (Ibidem, p. 70, grifo nosso).

Wanderlei José dos Reis informa que a redação do *caput* do dispositivo foi duramente criticada no seio doutrinário, tendo em vista que o verbo nuclear do art. 154-A, qual seja "invadir", exprime, consoante a definição do *Dicionário Aurélio*:

> O ato de "entrar à força, apoderar-se violentamente" **e a julgar pela redação do novel artigo, somente se configuraria o crime se o agente acessasse o sistema de informática à força**. (REIS, 2013, p. 34, grifo nosso).

Wanderlei José (2013, p. 34) explica que só há duas formas de se ter acesso a banco de dados de forma indevida: "quando o agente acessa fisicamente o dispositivo ou quando o usuário, de forma inadvertida, permite que sejam instalados no seu computador os chamados *malwares*, que aparecem na forma de arquivos enviados por *e-mail*, *links* na internet ou em dispositivos móveis como *pendrives*".

Dessa forma o autor conclui que o legislador pecou na qualidade técnica do artigo 154-A, onde solução legal seria substituir o verbo "*invadir*" por "*acessar*", uma vez que o agente não opera com violência, mas tão somente com o emprego de ardil para a obtenção de dados, ou seja, na prática o *modus operandi* não se coaduna com a maior parte dos delitos cibernéticos, nos quais o agente se utiliza da estratagema para enganar e alcançar o seu desiderato criminoso.

Auriney Brito (2013) complementa que o legislador deixou claro que é imprescindível que haja uma lesão ou ameaça concreta ao bem jurídico tutelado – para que se atenda ao princípio da lesividade – pois só a ação do agente não é suficiente para configurar o crime. No entanto, vive-se hoje um contexto de relativização desse princípio penal, razão pela qual há que se falar em antecipação de tutela penal, para que se evite que algo danoso aconteça às vítimas dos crimes digitais.

4.2.2. A Mera "Espiadinha" Configura o Crime Pelo Verbo "Obter"?

Segundo Renato Opice Blum (2012), especialista em crimes de internet, a lei já nasce com brecha, no que tange a parte final do art. 154-A, pois não

prevê punição para alguém que invade o computador e não rouba nada - o faz apenas por curiosidade - ou tenta invadi-lo mas não consegue.

Destarte, Flávia Penido expõe a parte final do referido artigo e aponta a dúvida dos especialistas no que se refere a mera “espiadinha”:

> 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. (PENIDO, 2013, p.3).

Ressalte-se que o verbo “obter” causa dúvida nos especialistas quanto a configuração do crime de obtenção de dados, uma vez que é possível entrar e sair do sistema alheio para dar uma mera “espiadinha”, razão pela qual há quem diga que sim e quem diga que não há crime.

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

> É o que fazem os hackers, que se distinguem dos crackers por não intentarem causar qualquer dano ao proprietário das informações violadas. **Aqueles indivíduos, em face da expertise que demonstram, são, inclusive, contratados por grandes empresas que se valem do seu trabalho para corrigir as falhas dos seus sistemas**. (FRANÇA, 2013, p. 4, grifo nosso).

O autor acredita que a conduta dos *hackers*, à luz da inteligência do legislador penal, encontra-se aceita pela sociedade contemporânea, devido à sua colaboração para o aperfeiçoamento das atividades daqueles que seriam suas vítimas, por isso elucida sua postura de acordo com o princípio da adequação social:

> **Não há razão, em face do princípio da adequação social**, **para punir a conduta de quem, tão somente, invade sistema informático alheio e obtém dados, de forma desautorizada**. Seria a consagração do paradoxo neste estágio de evolução social, em que **se aceita e, mesmo, estimula, com remunerações substanciais, a atuação dos hackers**. Igualmente paradoxal seria punir quem vende insumos para tal consecução. (FRANÇA, 2013, p. 5, grifo nosso).

Por outro viés, Flávia Penido expõe os possíveis transtornos que os profissionais especializados em segurança da informação podem sofrer:

> Somando a isso, na vida corporativa, **esse artigo pode causar transtornos entre os profissionais especializados em procurar vulnerabilidades em sistemas alheios visando solucionar ou evitar falhas de segurança**, a depender de como se dá o trabalho do profissional e de como esteja redigido o contrato de prestação de

> serviços, prevendo a exclusão de eventual incidência criminosa nessas atividades. (PENIDO, 2013, p. 3, grifo nosso).

Por fim, a autora conclui que somente a Jurisprudência irá solucionar essa dúvida, com o passar do tempo, tendo em vista a formação de opinião pela interpretação da lei.

4.2.3. As Penas Brandas se Convertem em Prestação de Serviços à Comunidade

Segundo Misael Neto Bispo da França (2013) a falta de dignidade penal, atestada pela insignificância do *quantum* da reprimenda cominada à tal conduta, *ex vi* da previsão do recente art. 154-A, aponta para a sua pouca relevância, uma vez que se configura em pena de 3 (três) meses a 1 (um) ano e multa.

Ademais, Misael Neto (2013) elucida a ciranda despenalizante do diploma legal, pois a pena máxima cominada em 1 (um) ano, arrasta o crime para o rito sumaríssimo dos Juizados Especiais, onde se estimulará a conciliação, a composição civil dos danos e a transação penal.

Somando-se a isso, o autor explana:

> A pena mínima, abaixo de 1 ano favorece a suspensão condicional do processo, se não houve condenação ou se não existe processo por outro crime. [...] Daí por que dizer que **a reprimenda, associada ao comportamento delitivo, tem de ser idônea, isto é deve fazer jus à gravidade da sua efetivação em face da liberdade do indivíduo, sob pena de, desnaturando as suas próprias funções**, **dá azo a inevitável autofagia**. Noutras palavras, penas insignificantes não atendem aos princípios clássicos de Direito Penal, sobretudo o da lesividade. (FRANÇA, 2013, p. 5).

Thiago Tavares, presidente da ONG Safernet Brasil, complementa o entendimento no que tange à brandura das penas:

> Ainda que a medida seja exaltada pelo esforço de tipificação, o que dificulta a manobra de advogados de defesa que alegam ausência de leis específicas para a internet, as penas estabelecidas para a invasão de computadores, celulares, tablets e contas de e-mails têm sido vistas como brandas. O tempo de reclusão é de três meses a um ano, com previsão de fatores de majoração de pena. "**No Brasil, se o réu for primário, penas inferiores a quatro anos podem ser convertidas, por exemplo, à prestação de serviços à comunidade. Ou seja, ninguém vai para a cadeia por esse crime**". (TAVARES, 2013, p. 59, grifo nosso).

Conforme estimativas de Opice Blum (2013), devido a natureza branda das penas impostas ao réu primário – oportunidade em que é possível a conversão em pagamento de cestas básicas – cria-se um problema, bem como uma situação inusitada: a nova lei pode estimular o delito ao invés de coibi-lo, pois:

> **Tem muito computador por aí com informação que vale muito mais do que uma cesta básica** [...], **Aos criminosos, cometer o delito, ser pego e ter de pagar pelo crime de invasão pode compensar**. Isso se o sujeito for pego, identificado e julgado a tempo. Como as penas para o crime são pequenas, elas prescrevem rapidamente, inviabilizando a punição. (BLUM, 2013, p. 64, grifo nosso).

Dessa forma, Misael Bispo da França (2013) atesta que é função da pena prevenir a ocorrência (e a recorrência) de comportamentos criminosos, no entanto, se a pena não atribuir o mínimo de força dissuasória esta meta torna-se difícil de ser alcançada.

4.2.4. Os Ataques de Negação de Serviços Feitos a Particulares Não Foram Abrangidos pela Lei?

Segundo Patrícia Peck Pinheiro (2013) em meados de 2011 ocorreram vários ataques de negação de serviço a *sites* do governo brasileiro, tornando-os instáveis até sair do ar, razão pela qual, o poder público percebeu que era necessário ter mais atenção com as questões de segurança nacional, pois os ataques eram possíveis devido às vulnerabilidades, bem como pela estratégia precária de um plano de contingência e continuidade.

Alexandre Atheniense explana que esse não foi o primeiro ataque a *sites* governamentais, inclusive os responsáveis técnicos divulgaram os danos causados de forma escassa, razão pela qual o autor buscou maiores informações:

> Os ataques visaram, em regra, efetivar uma mudança visual no site, com troca de imagens e registro da marca do hacker que promoveu o evento danoso (pichação virtual – “website defacement”, a qual se caracteriza pela quebra da proteção da segurança); invasão da rede interna das entidades, via acesso não autorizado, e consequentemente tentativa de furto de informações sigilosas; e disparo de inúmeros acessos simultâneos, originados de vários computadores denominados “zumbis”, situados em localidades diversas, com o fim de sobrecarregar o sistema até derrubá-lo. Esses procedimentos ficaram conhecidos como “ataques de negação de serviços do tipo DDoS – *Distributed Denial of Service* ou DoS – *Denial of Service*”. (ATHENIENSE, 2011, p. 14).

O autor informa que embora muitos *experts* tenham considerado os ataques recém-ocorridos como de limitado potencial danoso, os dados da Febraban relataram exatamente o contrário: os prejuízos originados pelas fraudes eletrônicas e as humilhações causadas pelos recentes atentados e pichações virtuais aos *sites* governamentais corresponderam a estratosféricos R$ 900.000.000,00 (novecentos milhões de reais). Assim, restou claro que, ao contrário do que ocorre no setor bancário, os *sites* governamentais ainda prescindem de investimentos na área da segurança, sobretudo no que tange aos ataques de "negação de serviços" para reduzir a vulnerabilidade.

Auriney Brito (2013) afirma que não foram só os *sites* do governo que sofreram ataques de "negação de serviços", em 2012 várias empresas como a TAM, a GOL, os Bancos do BRASIL, BRADESCO também foram alvo dos ataques "DDoS", causando prejuízos incomensuráveis para as empresas, vez que estas perderam o seu sistema por um tempo. Vale salientar, que muitas empresas não assumem os ataques tampouco os prejuízos milionários, para não transparecer vulnerabilidade e insegurança aos clientes.

Destarte, emerge a urgência na aprovação dos Projetos de Lei n. 84/99 e 2.793/11, os quais foram sancionados e promulgados pela Presidência da República em 30/11/2012 - mediante a Lei 12.737/2012 - com vistas ao combate dos crimes digitais.

Entretanto, a lei em discussão nasce com numerosas lacunas, entre elas a limitação à utilidade pública no crime de interrupção ou perturbação de serviço telemático ou de informação, razão pela qual o professor Rony Vainzof (2013) indaga: E os demais casos de interrupção, igualmente lesivos, mas não considerados de utilização pública não serão abrangidos pela lei?

Segundo a pesquisa elaborada por Flávia Penido (2013), a maioria dos especialistas dizem que os ataques de negação de serviço – conhecidos como *DoS ou DDoS*[9] – feitos a particulares, não estariam abrangidos pelo dispositivo legal ora

[9] Trata-se de uma prática criminosa, também denominada de "negação de serviço", que se caracteriza pelo envio simultâneo de requisições de serviços para determinado recurso de um servidor, tornando-o indisponível, como ocorreu recentemente no *site* da Presidência da República. Esclareça-se que o "*cybercriminoso*" contamina centenas ou até mesmo milhares de computadores (*botnets*), a fim de torná-los disponíveis para o ataque, mediante acesso simultâneo ao *site* de que, assim, não pode dispor o usuário. (JORGE, 2011, p. 7).

em vigor, uma vez que o artigo 266, §1º, fala apenas em serviços de utilidade pública, in *verbis*:

> Incorre na mesma pena quem interrompe **serviço telemático ou de informação de utilidade pública**, ou impede ou dificulta-lhe o restabelecimento. (PENIDO, 2013, p. 3, grifo nosso).

O Professor Rony Vainzof (2013) destaca que resta enquadrar o *hacker* na legislação penal pelo crime de dano, configurado no artigo 163 do CP: “destruir, inutilizar ou deteriorar coisa alheia”, já que não é possível enquadrá-lo pelo art. 266, § 1º da Lei Carolina Dieckmann, inclusive questiona se o termo “coisa” pode ser aplicado a um *site*. Nesse sentido, “a maioria das decisões do STJ concluem que sim, que “coisa” pode ser *bits* ou *bytes*, ou seja crime punido com detenção de 1 a 6 meses”.

Desta feita, houve uma discrepância ainda maior em relação a punibilidade do agente que comete o crime de interrupção ou perturbação nas organizações privadas, pois só lhe caberá o crime de dano, com pena de 1(um) a 6 (seis) meses – conforme descrito acima, ao passo que na Lei Carolina Dieckmann a pena seria de 1 (um) a 3 (três) anos. Assim, pode-se verificar mais uma lacuna que compromete a eficácia e a credibilidade da Lei 12.737/12, uma vez que o dano causado “no ambiente digital” atinge prejuízos incomensuráveis para as vítimas.

4.2.5. Despreparo da Polícia Investigativa para Apurar os Crimes Informáticos Podem Levá-los à Prescrição

Para João Loes (2013), a Lei 12.737 requererá uma apuração veloz para funcionar, porque os crimes possuem penas pequenas, e por esta razão prescrevem rapidamente, inviabilizando a punição dos criminosos.

Desta feita, o autor expõe que um dos maiores entraves para o sucesso da Lei Carolina Dieckmann é a falta de estrutura para apurar os delitos informáticos. Elucida-se que o Brasil ainda carece de um corpo representativo de profissionais treinados para lidar com esses delitos, embora conte com alguns centros de excelência em perícia digital. Assim, caso haja demora na investigação - a depender da pena do crime - não haverá mais o que fazer devido à prescrição, por isso exemplifica:

> Hoje, por exemplo, quem busca a polícia para registrar um boletim desse tipo de ocorrência, **pode esperar até três meses para ter seu equipamento periciado**. (LOES, 2013, p.64, grifo nosso).

Importante fazer um adendo com Patricia Peck Pinheiro (2013, p. 231) para conceituar computação forense "Consiste no uso de métodos científicos na preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais", bem como para explanar a importância que esta ciência terá para a sociedade, no que tange a apuração dos crimes digitais:

> Segundo pesquisas atuais, **crescem os crimes virtuais, e estes, em breve, irão ultrapassar os crimes físicos**. Sendo assim, podemos vislumbrar a importância que a computação forense terá para a **sociedade, pois é por meio dessa ciência que será possível descortinar os fatos e punir os infratores**. (PINHEIRO, 2013, p. 230-231, grifo nosso).

Nesse diapasão, Leandro Bissoli (2013, p.64) alerta que diante da atual conjuntura é mister se ter uma equipe competente e rápida, pois "os rastros do crime digital são frágeis" e "sem uma perícia competente e rápida, pouco se salva".

Caio César Carvalho relata que alguns estudiosos entendem que é muito difícil capacitar agentes de polícia para o combate específico de crimes na internet, já que estes podem envolver múltiplas ações, como por exemplo:

> Se eu tenho tráfico de drogas, por exemplo, vou mandar para uma delegacia eletrônica? Uma opção para isso seria capacitar a polícia para prestar assessoria às demais delegacias. (CARVALHO, 2013, p. 61).

Luiz Flávio Gomes participa do debate sobre a Lei Carolina Dieckmann no V Congresso - Crimes Eletrônicos - Formas de Proteção (Fecomércio/SP), realizado nos dias 12 e 13 de agosto de 2013, oportunidade em que crítica a incompetência da polícia para atuar com crimes na internet:

> Na lei está escrito assim: "a lei pune os crimes informáticos[10] e a polícia vai se preparar para apurar esses crimes". Então a polícia não tem competência para atuar agora com a internet? Ainda vai se preparar? **Seja do ponto de vista técnico, seja do ponto de vista material; a polícia não tem estrutura para apurar tudo isso**. (GOMES, 2013, V Congresso – Crimes Eletrônicos – Formas de Proteção).

[10] A expressão crimes informáticos não é adotada de maneira uniforme pela doutrina, que apresenta outras nomenclaturas para o mesmo estudo, quais sejam, exemplificativamente, "crimes da era da informação", "crimes mediante computadores", "crimes cibernéticos", "cibercrimes", "crimes de computador", "crimes eletrônicos", "crimes tecnológicos", "crimes digitais", "crimes *high-tech*", "tecnocrimes", "netcrimes", "crimes virtuais", "crimes da tecnologia da informação" e até mesmo "e-crimes". (SYDOW, 2013, p. 56).

Nesse evento, o jurista propõe competência para os escritórios de advocacia fazerem investigações sobre os crimes eletrônicos:

> Os próprios escritórios de advocacia tinham que ter essa competência para fazer investigação, **pela lei eles tinham que estar autorizados a fazer determinados procedimentos investigatórios**, como é nos Estados Unidos (E.U.A). **Nos Estados Unidos, os escritórios produzem provas e levam ao juiz; e o juiz julga em cima da prova que foi colhida e a outra parte produz a prova dela**. (Ibidem, grifo nosso).

Marcelo Crespo apresenta outro aspecto que pode dificultar a justa punição de usuários, que em poucos minutos - destroem reputações ou revelam sigilos de uma empresa - pela demora da perícia:

> Outro aspecto pode dificultar a justa punição de usuários que, **em poucos minutos, destroem reputações ou revelam dados sigilosos de uma empresa**. “Como a pena é pequena, o prazo para investigar o crime é menor. **Então, se você coloca uma investigação curta com exigências complexas, como perícias demoradas, muitas penas vão prescrever**”. (CRESPO, 2013, p. 59, grifo nosso).

Destarte, João Loes (2013) conclui que se a perícia não for competente para apurar os crimes digitais, a lei Carolina Dieckmann perderá a função, por mais bem-intencionada que seja.

4.2.6. Fragilidade para Retirada de Conteúdo da Internet e Ineficácia da Legislação Sobre a *Deep Web*

Segundo Marcos Manzoni o fato de as fotos da atriz Carolina Dieckmann ainda serem acessíveis a qualquer usuário disposto a fazer uma breve pesquisa na rede, revela o nível de complexidade jurídica que envolve o ambiente virtual, pois:

> Nesse caso, os *crackers* utilizaram servidores hospedados fora do Brasil - como a maioria deles o faz. Sem um mecanismo jurídico específico para confrontar tal estratégia, as autoridades brasileiras têm de contar com acordos internacionais ainda frágeis e a colaboração de empresas mundiais de telefonia e *softwares* para tirar conteúdos e identificar criminosos. (MANZONI, 2013, p. 60).

Marcela Buscato (2012) informa que Carolina Dieckmann chegou a brigar para tentar impedir que as fotos se espalhassem pela rede mundial, mas foi uma tentativa frustrada. O advogado da atriz, o criminalista Antônio Carlos de

Almeida Castro – Kakay – conseguiu, por meio de pedido, retirar as fotos nos dois primeiros *sites* que fizeram a divulgação, ambos situados no exterior. Bastou “Kakay” mandar reportagens divulgadas no Brasil sobre a aquisição das fotos por meio ilegal.

Neste ínterim, vale a pena colacionar os dados da Safernet em parceria com a *childhood* Brasil, trazidos por Manzoni (2013, p. 60): “97,6% do conteúdo denunciado no país estão hospedados em servidores estrangeiros, especialmente nos Estados Unidos”.

Por outro lado, Marcela Buscato mostra o insucesso do advogado frente ao pedido feito ao *Google* para não divulgar as fotos da atriz nos resultados de suas buscas:

> Em nota, o Google disse **não ter responsabilidade sobre os conteúdos publicados na internet e que “não interfere em seus resultados de busca**”. Para fazer isso, exige uma medida judicial. (BUSCATO, 2012, p. 85, grifo nosso).

Marcos Manzoni (2013) explica ainda que a dificuldade de identificação das mentes perversas não opera só com pessoas físicas, mas também com Pessoas Jurídicas de Direito Público como foi o caso de ataques que atingiram entre outros o *site* da Presidência da República e o da Receita Federal, razão que elucida:

> Ano passado, o Serviço Federal de Processamento de Dados (Serpro), responsável pelos processos de arrecadação e de despesas da União e do conteúdo de inúmeros *sites* públicos, teve de lidar com o "surto" de ataques que atingiram, entre outros, o site da Presidência da República e o da Receita Federal. […], **A resposta jurídica para este tipo de caso também é dificultosa. A maioria se dá em ambientes de difícil identificação**. É preciso estabelecer regras internacionais e de governança porque hoje a internet está muito mais ligada aos EUA do que a qualquer outro país do mundo. (MANZONI, 2013, p. 60, grifo nosso).

Patricia Peck Pinheiro (2013) revela que um incidente eletrônico gera maior dano, por quê:

> Ocorre em geral **de forma covarde**, **sem chance de defesa**, **além de gerar consequências que se perpetuam, pois a Internet é global e é difícil de limpar totalmente uma informação dela**. Por mais que haja retratação, uma publicação roda o mundo em poucos minutos. (PINHEIRO, 2013, p. 319, grifo nosso).

Por outro viés, Thiago Tavares (2013) relembra que para retirar conteúdo da internet no Brasil é preciso ordem judicial. Esse problema se agrava por considerar uma das regras mais polêmicas do Marco Civil da Internet: o chamado *notice and take down*, que permite a remoção automática – portanto, sem qualquer intervenção judicial – de conteúdos que ferem os direitos autorais no país.

Dessa forma, o referido autor acredita que há uma contradição nos critérios adotados:

> "Para remover qualquer conteúdo na web, a gente precisa de uma ordem judicial, mas essa mesma regra não se aplica ao direito autoral. Ou seja, **nós estamos dando maior valor à propriedade material do que à dignidade e à integridade das pessoas**". (TAVARES, 2013, p. 61, grifo nosso).

Outro ponto polêmico será apresentado por Manuel Martin Pino Estrada, trata-se da ineficácia da legislação sobre a *Deep Web* ou Internet Profunda.

Segundo Manuel (2013, p. 40): "Muitas invasões de dispositivos informáticos e quebras de dados pessoais são decorrentes do uso da *Deep Web*[11] ou internet profunda pelos *crackers*." Esta internet paralela – não deixa rastros – ou seja, qualquer *cracker* iniciante pode entrar e vasculhar dados sigilosos, sem deixar que seu IP (Protocolo de Internet) seja identificado. É impossível, via de regra, conseguir rastrear estes criminosos – pela *Deep Web* – nem mesmo um *cracker* que utiliza a Internet Profunda pode localizar outro, salvo no caso de cometimento de erros de discrição, possibilidade remotíssima.

Há que se perscrutar que hoje não há nehuma lei capaz de combater um *cracker* que usa *Deep Web* para invadir computadores no mundo inteiro. Inclusive nem a própria *Federal Bureau Investigation* (FBI) consegue ter sucesso nesta missão, só em casos muito raros, como o *Silk Road*[12]*. Sendo assim,* não há nada que as autoridades possam fazer, neste momento, para brecar estes *crackers*.

Por fim, o autor expõe que atualmente existem milhares de vítimas dos crimes eletrônicos, número que pode aumentar significativamente, devido a utilização da *deep web* pelos *crackers*. Razão pela qual o autor alerta o profissional do Direito Penal, pois vai se deparar com um caso que por hora não tem solução – o ataque de crackers por meio da internet invisível - uma vez que não há como localizá-los; bem como avisa as autoridades públicas para darem foco a informática sustentável dos seus *sites*, visto que na maioria das vezes os mantêm vulneráveis.

---

[11] A expressão *deep web* foi criada por Michael K. Bergman, fundador do programa *Bright software* especializado em coletar, classificar e procurar conteúdo nessa esfera da *web*. O termo, traduzido para o português, remete ao significado de profundeza, tendo sido fixada em oposição à *surface web*, vocábulo que visa dar a ideia de superficialidade. Chamada como *web* ou internet "invisível", a *deep web* consiste em *sites* que, dispersos na internet, são programados para propositadamente não serem encontrados. Assim, mesmo existentes, esses *sites* não são acessados pelo grande público, ficando escondido nas "profundidades" da rede. (WRIGHT, 2009).

[12] Era o maior mercado *on-line* de drogas (de haxixe do Marrocos a cocaína da Holanda e cogumelos dos Estados Unidos), remédios controlados, equipamentos para hacking e espionagem, joias falsas, pacotes de conteúdo pornográfico. […], Em 1º de outubro de 2013, a FBI conseguiu prender o fundador do *Silk Road* e fechar o *site*, graças a erros básicos de discrição. (ESTRADA, 2013, p. 39).

4.2.7. A Lei Dependerá de Jurisprudência e Leis Complementares para Funcionar

Segundo João Loes (2013) para tornar a lei efetiva terá que passar por algumas dificuldades, a começar pelo próprio texto- que segundo especialistas - está excessivamente ambíguo, pois quando o legislador menciona, por exemplo, as expressões: “dispositivos informáticos”, “mecanismos de segurança” e “obtenção de dados”, os limites pouco claros do que cada conceito representa pode dar margem a interpretações oportunistas.

Destarte, os advogados Renato Opice Blum e Leandro Bissoli pontuam que esses conceitos ambíguos no texto legal podem atrapalhar a implantação da nova legislação, por isso questionam o significado das expressões e o seu alcance.

> **O que significa “mecanismo de segurança**”? Usuários que não usam um sistema de segurança, como uma senha, não estão protegidos pela lei? Em casos nos quais o usuário tem uma senha, mas o aparelho foi violado quando o dispositivo estava temporariamente desbloqueado, a vítima continua sem a proteção da lei? (BLUM, 2013, p.64, grifo nosso).

Nesse contexto, Leandro Bissoli indaga:

> **O que significa dispositivo informático**? Não se sabe se o conceito valerá apenas para dispositivos de *hardware*, como computadores, *nootebooks*, celulares e *tablets*, ou se ele também se aplicará a serviços de *internet*, como *e-mails*, discos virtuais, contas em redes sociais, entre outros. (BISSOLI, 2013, p. 64, grifo nosso).

Os autores ainda interrogaram sobre o significado da expressão “obter dados”:

> **Quando a lei fala em “obter dados”,** não se sabe se ela diz respeito apenas ao criminoso que copia ou retira os dados de um dispositivo invadido ou também ao criminoso que só faz a consulta desses dados, sem copiá-los. (BLUM; BISSOLI, 2013, p.64, grifo nosso).

Sendo assim, João Loes (2013) elucida que embora seja louvável o esforço para se fazer uma lei mais genérica, há que se atentar para a amplitude e aplicabilidade desta, pois quanto mais ampla a legislação, mais aplicável ela é, dessa forma, se existir lacunas nas partes fundamentais gerar-se-á problemas.

Diante disso, Leandro Bissoli (2013, p. 64) acrescenta: “As especificações terão de ser definidas pelos juízes nas primeiras decisões”.

Luiz Flávio Gomes critica no V Congresso – Crimes Eletrônicos – Formas de Proteção – a eficácia da Lei Carolina Dieckmann:

> **A eficácia que todo mundo espera da norma penal não vai acontecer,** eu contei 104 (cento e quatro) verbos, cada verbo é uma interpretação, **tudo hoje demanda uma interpretação e cada juiz interpreta da sua maneira e cada autor interpreta do seu jeito**. (GOMES, 2013, V Congresso – Crimes Eletrônicos – Formas de Proteção, grifo nosso).

Portanto, João Loes (2013) conclui que a Lei Carolina Dieckmann dependerá de jurisprudências, bem como precisará de investimento e leis complementares para funcionar plenamente.

4.2.8. Conflito de Competência nas Esferas Civil e Penal

Higor Vinicius Nogueira Jorge (2011, p. 446) elucida: “muitos imaginam que violência signifique unicamente agressão física contra outras pessoas, ou seja, a ação de infligir uma dor corporal contra a vítima, como no caso em que ela recebe um tapa, um soco ou um empurrão”.

O autor explana que existem outras modalidades de violência, não tão consideradas pelas pessoas, que podem ser praticadas com o uso de instrumentos eletrônicos (cibernéticos), como por exemplo a agressão moral - na atualidade - conhecida por *Cyberbullying*[13]. Perscruta-se que este tipo de ofensa é semelhante as modalidades comuns, mas quando praticadas em ambiente virtual causam efeitos muito piores e algumas vezes se perduram por toda a vida da vítima.

Jorge Vinícius (2011, p. 446) destaca algumas modalidades comuns de *Cyberbullying*: “envio de *e-mails* ofensivos para a vítima ou conhecidos dela, envio de mensagens SMS, via celulares, postagem de vídeos, publicação de ofensas em *sites, blogs*, redes sociais, fóruns de discussão, hotéis virtuais (*haboo*), mensageiros instantâneos, etc”. Vale salientar que o *Cyberbullying* é muito frequente em ambiente escolar (entre jovens), bem como praticado no seio familiar, entre vizinhos, amigos ou em outros ambientes. Guarda motivos variados para sua existência tais quais:

[13] Consiste na prática de agressões físicas ou psicológicas de forma habitual traumática e prejudicial às vítimas,[…], porém praticadas de forma eletrônica (ou cibernética), ou seja, por intermédio de computadores ou outros recursos tecnológicos. Esse tipo de ofensa pode ser praticada das mais variadas formas e tem uma característica que é a rápida disseminação pela rede, ou seja, em pouco tempo é disponibilizada em uma infinidade de *sites* e *blogs*. Dificilmente a vítima consegue extirpar a informação de todos os locais aonde se encontra. (JORGE, 2011, p.446).

diferenças entre características físicas (usa óculos, é obeso, possui alguma deformidade) e características gerais (intelectual, religião, etnia ou preferência sexual).

O autor preconiza ainda que alguns casos de *Cyberbullying* se enquadram em previsões penais, uma vez que rompem os limites da licitude. Nesta oportunidade surgem os crimes cibernéticos, dentre os quais se destacam: calúnia, difamação, injúria, ameaça, constrangimento ilegal, falsa identidade, perturbação da tranquilidade, etc.

Desta feita, o delegado Jorge Vinícius agrega valor ao comentar e exemplificar cada um dos crimes cibernéticos acima relacionados. A começar pela "Calunia" – afirmar que a vítima praticou algum fato criminoso – é um dos crimes cibernéticos mais praticados, principalmente em *sites* de relacionamento:

> Um exemplo comum é o caso de mensagens deixadas no perfil de um usuário do Orkut ou outro *site* de relacionamento que imputa a ele a prática de determinado crime, como por exemplo, que certa pessoa praticou um furto ou um estupro. A pena para este tipo de delito é de detenção de seis meses a dois anos e multa. (JORGE, 2011, p. 445).

A "Difamação" se configura ao propagar fatos ofensivos contra a reputação da vítima:

> O estudante que divulgou no *Twitter* que determinado empresário foi visto saindo do motel acompanhado da vizinha praticou o crime de difamação. Mesmo que o estudante prove que realmente o empresário foi visto no local, o crime subsistirá, pois independe do fato ser verdadeiro ou falso, o que importa é que prejudique a reputação da vítima. O delito tem uma pena de detenção de três meses a um ano e multa. (JORGE, 2011, p. 445).

A "Injúria" ofende a dignidade ou o decoro de outras pessoas:

> Geralmente se relaciona com xingamentos, exemplo, escrever no *Facebook* da vítima ou publicar na *Wikipédia* que ela seria prostituta, vagabunda e dependente de drogas. Também comete este crime aquele que filma a vítima sendo agredida ou humilhada e divulga no *YouTube*. A pena é de detenção e varia entre um a seis meses ou multa. Se a injúria for praticada com violência ou vias de fato a pena varia de três meses a um ano de detenção e multa. Caso as ofensas sejam relacionadas com a raça, cor, etnia, religião, origem ou condição de pessoa idosa ou portadora de deficiência o crime se agrava e a pena passa a ser de reclusão de um a três anos e multa. (Ibidem, p. 445).

A "Ameaça" significa ameaçar a vítima de mal injusto e grave:

> É corriqueiro a vítima procurar a Delegacia de Polícia para informar que recebeu *e-mails*, mensagens de *MSN* ou telefonemas com

> ameaças de morte. A pena é de detenção de um a seis meses ou multa. (Ibidem, p. 445).

Já o “Constrangimento ilegal” pode ocorrer se for feita uma ameaça para que a vítima faça algo que não deseja fazer e que a lei não determine:

> Por exemplo, se um garoto manda uma mensagem instantânea para a vítima dizendo que vai agredir um familiar dela caso não aceite ligar a câmera de computador (*web cam*). Também comete este crime aquele que obriga a vítima a não fazer o que a lei permita, como no caso da garota que manda um *e-mail* para uma conhecida e ameaça matar seu cachorro caso continue a namorar o seu ex-namorado. A pena para este delito é a detenção de três meses a um ano ou multa. (Idem, p. 445).

A “Falsa identidade” é a ação de atribuir-se ou atribuir a outra pessoa falsa identidade para obter vantagem em proveito próprio ou de outro indivíduo ou para proporcionar algum dano:

> Tem sido frequente a utilização de *fakes* em *sites* de relacionamentos, como no caso de uma mulher casada que criou um *fake* para poder se passar por pessoa solteira e conhecer outros homens. Também recentemente uma pessoa utilizou a foto de um desafeto para criar um perfil falso no *Orkut*, se passou por ele e começou a proferir ofensas contra diversas pessoas, visando colocar a vítima em uma situação embaraçosa. A pena prevista para este tipo de ilícito é de três meses a um ano ou multa se o fato não for considerado elemento de crime mais grave. (Idem, p. 445).

“Molestar ou perturbar a tranquilidade” neste caso não há um crime e sim uma contravenção penal que permite punir aquele que passa a molestar ou perturbar a tranquilidade de outra pessoa por acinte ou motivo reprovável:

> Como por exemplo, nos casos em que o autor passa a enviar mensagens desagradáveis e capazes de incomodar a vítima. Esse tipo de comportamento é observado pelos denominados *trolls*, que são pessoas que utilizam a internet para criar discussões, além de irritar e desestabilizar outras pessoas. Recentemente ocorreu um caso de um indivíduo que passava o dia inteiro realizando ligações telefônicas e enviando centenas de mensagens SMS com frases românticas para a vítima. O caso foi esclarecido e o autor foi enquadrado nesta contravenção penal. (JORGE, 2011, p. 445).

A prática do *cyberstalking* que consiste no ato de perseguir a vítima e ultrapassar os limites da sua privacidade também se enquadra neste crime:

> Como nas situações em que o autor passa a incomodar a vítima com telefonemas a todo momento ou que manda e-mails repetidamente para ela. A pena para essa figura delitiva é de prisão simples, de quinze dias a dois meses ou multa. (Ibidem, p. 445)

Higor Vinicius (2011, p. 445) relata que prática deste tipo de crime pela internet não é sinônimo de impunidade, muito pelo contrário, a Polícia Civil e a Polícia Federal possuem instrumentos adequados e profissionais capacitados para que, por intermédio da investigação criminal, a autoria e a materialidade sejam comprovadas.

O referido autor informa que a prática destas ofensas desencadeiam diversos reflexos civis, sendo um dos mais importantes a obrigação de reparar os danos morais ou materiais proporcionados pelos autores das ofensas.

Por este motivo, Higor Vinicius (2011) elenca alguns dispositivos legais que tutelam a vítima dos males causados pelos autores de crimes cibernéticos:

A Constituição Federal, no artigo 5°, X assegura o direito à indenização pelo dano material ou moral ao determinar que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

No mesmo sentido o Código Civil estabelece no artigo 927 que "aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo".

Esta norma define o ato ilícito no artigo 186 como sendo "aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito".

O artigo 953 prevê que "a indenização por injúria, difamação ou calúnia consistirá na reparação do dano que delas resulte ao ofendido". Em seguida, o parágrafo único deste artigo declara que "se o ofendido não puder provar prejuízo material, caberá ao juiz fixar, equitativamente, o valor da indenização, na conformidade das circunstâncias do caso".

Embora muitos crimes estejam tipificados no Código Penal (Calúnia - art. 138, Injúria - art. 140 e Difamação - art. 139), quando tratados no campo digital, são julgados na área cível, razão pela qual Higor Vinícius colaciona algumas condenações:

> O juiz de direito da 4ª Vara Cível de Taguatinga e mantida pela 2ª Turma Cível do Tribunal de Justiça do Distrito Federal, que **condenou uma pessoa a indenizar duas vítimas em razão de ter postado no Orkut mensagens com palavras e expressões de baixo calão** (Processo: 200701014929). (JORGE, 2011, p. 444, grifo nosso).

> No Rio de Janeiro **um grupo de pais de alunos e ex-alunos foi condenado a pagar uma indenização de R$ 18.000,00 por danos morais em razão da criação de uma comunidade na mesma rede social com a finalidade de ofender a vítima** (14ª Câmara Cível do Tribunal de Justiça do Rio). (Ibidem, p. 444, grifo nosso).
>
> No Estado de Minas Gerais no ano de 2007, **um indivíduo que foi comparado ao ET de Varginha em um *site* de relacionamento recebeu indenização de R$ 3.500,00 de um colega de Faculdade** (9ª Câmara Cível do Tribunal de Justiça de Minas Gerais). (Ibidem, p. 444, grifo nosso).

Rômulo de Andrade Moreira traz dois casos de punições de delitos informáticos, no que tange a prejuízos econômicos:

> Em meados do ano passado, em Fortaleza, foi **descoberto um esquema de fraude pela Internet que teria causado um prejuízo de cerca de R$ 30 milhões a empresas de todo o País**. O agente, que agia há oito anos, utilizava um programa de computador (**por meio do qual tinha acesso a todos os dados das empresas, inclusive o estoque**) para criar uma identidade fictícia, falsificar cartões de crédito e fazer compras de produtos pela Internet. **Em outra oportunidade**, a Polícia Federal prendeu na Cidade de Sorocaba, interior paulista, **um rapaz que utilizava a Internet para aliciar mão-de-obra, inclusive para o exterior**. (MOREIRA, 2013, P. 103, grifos nossos).

Em meio a prática de diversos delitos cometidos por meios eletrônicos, surge em 30 de novembro de 2013, a Lei Carolina Dieckmann com vistas a proteger os direitos fundamentais à intimidade e à vida privada das pessoas, mediante a justa punição de delitos informáticos. Entretanto, tal advento não foi bem recepcionado por diversos operadores do direito, levando inclusive ao debate acerca do conflito de competência nas esferas civil x penal.

Nesse sentido, o jurista Luiz Flávio Gomes (2013) relata que a Lei Carolina Dieckmann não vai surtir efeitos práticos visto que possui deficiências técnicas, deficiências materiais da polícia e principalmente porque o direito penal – não funciona para crimes eletrônicos – essas matérias têm que ser tratadas no campo civil.

O autor expõe algumas situações que corroboram para a aplicação de indenização, bem como apuração de responsabilidades no campo cível:

> Como dito, **o direito penal não funciona para essas coisas, vai para o campo civil**, apura responsabilidades, taca uma indenização decente, uma indenização firme, contundente. **Acaba com o sujeito que lhe fez uma agressão, que te xingou, que te injuriou, que entrou no teu computador e que depois divulgou segredos seus – acaba com esse cara economicamente** não é só para a Carolina

> Dieckmann ou Cicarelli. (GOMES, 2013, V Congresso – Crimes Eletrônicos – Formas de Proteção).

Desta feita, Luiz Flávio Gomes (2013) acredita que a justa punição para situações oriundas do meio eletrônico, configura-se na apuração das responsabilidades do sujeito, bem como na aplicação de indenização conduntente, capaz de aniquilá-lo economicamente.

4.2.9. Consequências Para as Vítimas dos Delitos Informáticos

Alessandra Medina leciona:

> Em qualquer curso, cartilha ou panfleto sobre segurança na internet, **diz-se com todas as letras que tudo, rigorosamente tudo o que está no seu computador é passível de ser visto por todo mundo**. Mesmo sabendo disso, **pouquíssima gente resiste à tentação de compartilhar intimidades e guardar imagens e infomações privadas em *laptops*, *tablets* e celulares, na ilusão de que está num ambiente seguro. Não está**. Nas mãos de quem sabe usar (e nem precisa saber muito), **o mundo digital é acessível e a internet, um território aberto e incontrolável**. (MEDINA, 2012, p. 94, grifo nosso).

Neste contexto a autora faz um alerta para os cuidados que as pessoas devem tomar no que se refere ao conteúdo colocado na rede, pois uma vez inserido, dificilmente será apagado; e, na maioria das vezes, trazem consequências graves.

Marcela Buscato (2012) explana através de depoimentos que há três pontos de vista a serem observados no que tange às consequências para as vítimas dos delitos informáticos, os quais são: Moral, Psicológico e Neurológico.

Antes de adentrar ao mérito dos pontos acima relatados, a autora enfatiza a reação popular diante da divulgação das fotos da atriz Carolina Dieckmann:

> A reação popular às fotos de Carolina **variou da admiração pelo corpo da atriz às críticas escancaradas ou veladas a seu comportamento: quem, afinal, mandou tirar fotos pelada**? Não é o caso de atirar pedras, porém. **Todo mundo tem o direito de se fotografar da maneira que quiser**. (BUSCATO, 2012, p. 85, grifo nosso).

Desta feita, é possível traçar o ponto de vista moral, que segundo Marcela (2012, p. 85): “o sujeito que furta as fotos é um criminoso idêntico ao que arromba uma janela e retira fotos de família de uma gaveta na cômoda do quarto. Um ladrão nem mais e nem menos”. Quanto à nudez, ela já faz parte de um amplo

contexto de mudança de hábito, uma vez que as pessoas estão se fotografando e se deixando fotografar em momentos íntimos - isso ocorre no mundo inteiro - inclusive tornou-se uma prática cultural. Contudo, embora traga prazer, também acarreta risco às pessoas, tendo em vista a incerteza da proteção das informações frente ao olhar alheio.

A autora traz explicações psicológicas para justificar o gosto por fotos íntimas, sob duas ordens: Em primeiro lugar, devido à popularização das câmeras digitais as pessoas se encantaram e cada vez mais querem ser retratadas, gerando prazer pelo reconhecimento em fotos, ou seja, inserem-se no grupo. Em segundo lugar, a constante exposição a imagens e vídeos com apelo sexual, fez com que despertasse nas pessoas a vontade de reproduzir aquelas situações glamourosas, mesmo sem ter o desejo (ao menos inconsciente) de dividi-las com outras pessoas.

Por fim, Marcela expõe o ponto de vista neurológico, utilizando-se das palavras do neurocientista americano Ogi Ogas (2012, p. 86) “O cérebro feminino é programado para excitar-se com a excitação masculina”, ou seja, “é estimulante para as mulheres retratarem-se em poses sensuais e roupas diminutas”.

Estas explicações serviram para embasar o momento em que estes pequenos flagrantes íntimos deixam de ser um prazer para se transformar num pesadelo para as vítimas, pois a exposição pública pode gerar consequências graves.

Nesse diapasão, Marcela Buscato (2012, p. 86) elucida: “Os sentimentos variam de remorso à dificuldade de expressar emoções. Algumas vítimas isolam-se. Outras apresentam quadros de ansiedade. Poucas entram em depressão e há relatos de suicídio”.

A autora destaca alguns exemplos de vítimas de delitos informáticos, os quais trouxeram-lhes consequências graves:

> Nos Estados Unidos**, duas jovens, Jesse Logan, de 18 anos, e Hope Witsell, de 13 anos, se mataram depois que fotos que elas tiraram nuas foram parar nas mãos de colegas**. As duas histórias são semelhantes: as imagens foram enviadas aos namorados, que as repassaram. Claro que casos extremos são minoria. (BUSCATO, 2012, p. 86, grifo nosso).
> [...],
> A estudante Naina Yamasaki, filha da cineasta brasileira Tizuka Yamasadi, também foi responsabilizada por conhecidos quando**, em 2008, um filme em que ela aparecia numa relação sexual vazou. Até hoje, ela não sabe ao certo como o vídeo, que gravara aos 16 anos, saiu de seu computador. O material caiu na rede e se espalhou de *sites* pornôs às telas de computador de seus**

> **colegas, numa faculdade de São Paulo**. Naina teve a sensação de que todo mundo tinha visto. O que mais escutou foi: "**Você é burra". "Fez por merecer**", diz Naina, que **mora atualmente em Nova York**. (Ibidem, p. 86, grifo nosso).
> […],
> Carolina Dieckmann, fortalecida pela decisão de reagir à chantagem, **parece firme, ainda que fragilizada. Ela tem evitado sair de casa, mas cumpre compromissos de trabalho.** (Ibidem, p. 86, grifo nosso).

O jurista Luiz Flávio Gomes corrobora as autoras, oportunidade em que explana que o mundo informático traz - não só consequências graves, mas também o direito ao não esquecimento - do que entra na rede- sobre as pessoas:

> Hoje o mundo informático, e sobretudo na internet, **é um mundo que traz consequências graves para muita gente e pior – não tem direito ao esquecimento – é uma área que entrou teu nome, entrou uma acusação – ainda que totalmente falsa – entrou na rede, você não apaga mais**. (GOMES, 2013, V Congresso – Crimes Eletrônicos – Formas de Proteção, grifo nosso).

Alessandra Medina (2012, p. 94) relata: "O vazamento de fotos e a tentativa de extorsão à atriz Carolina Dieckmann confirmam o que todo mundo sabe mas não leva a sério: privacidade é artigo raro no mundo digital".

Por isso, é necessário que as pessoas compreendam a vulnerabilidade da rede, provada pela multiplicação de episódios de violação de imagem envolvendo artistas e anônimos, razão pela qual reitera-se o cuidado para o que postar no dispositivo informático, pois as consequências das vítimas de delitos informáticos variam de superação como fez a atriz Carolina Dieckmann ao suicídio como no caso das americanas Jesse e Hope.

5. DIREITO COMPARARADO SOBRE DELITOS INFORMÁTICOS E AS POSSIBILIDADES DE MELHORIA JUNTO À LEI CAROLINA DIECKMANN

Como sabido os delitos informáticos são globais e ultrapassam as fronteiras nacionais, razão pela qual se torna indispensável o estudo da eficácia das legislações e tratados estrangeiros bem a adoção de medidas satisfatórias, no que tange a justa punição aos criminosos cibernéticos.

5.1. A CONVENÇÃO DE BUDAPESTE

Segundo Auriney Brito (2013, P. 47) “O Comitê Europeu para os Problemas Criminais (CDPC), mediante a Deliberação CDPC/103/211196, datada de novembro de 1996, decidiu formar um comitê de especialistas para discutir sobre os crimes praticados através da rede mundial de computadores”.

Elucida-se que em 23 de novembro de 2001, na cidade de Budapeste, ocorreu a elaboração da Convenção sobre o Cibercrime – logo após o atentado terrorista do dia 11 de setembro nos Estados Unidos da América. O autor relata que este referido documento sugeriu a uniformização da legislação penal pelo mundo e os mecanismos e instrumentos de colaboração visando vencer a luta contra a criminalidade no ambiente virtual.

Tatiana Malta Vieira (2009) leciona que a Convenção de Budapeste consiste no mais significativo instrumento jurídico internacional a respeito dos "cibercrimes" os quais abarcam toda conduta humana típica, antijurídica e culpável em que o processamento eletrônico de dados serve como meio para a prática do delito ou é alvo deste.

Auriney Brito (2013) informa que até o primeiro semestre de 2010, 43 (quarenta e três) países assinaram a Convenção de Budapeste, mas apenas 22 (vinte e dois) países ratificaram a Convenção. Dentre os países signatários Tatiana Malta Vieira (2009) destaca: Conselho da Europa + Canadá + Japão + África do Sul + EUA, bem como relata alguns países não signatários: Andorra, Azerbaijão, Liechtesnstein, Mônaco, Rússia, Turquia e República de San Marino.

Dessa forma, Tatiana (2009) explana que o sucesso do tratado se deve não somente a sua abrangência geográfica, tendo em vista que engloba vários

países de fora do continente europeu, mas também pelo fato de efetivamente harmonizar a legislação tanto dos países signatários como de países não signatários, configurando-se como uma referência legislativa mundial a respeito da criminalidade informática, sua tipificação e persecução.

5.1.1. Breves Considerações

Segundo Auriney Brito (2013) a Convenção recomenda a manutenção criteriosa das informações que circulam nos sistemas informatizados, procedimentos processuais penais, bem como sua liberação para autoridades; atendendo aos três objetivos específicos a saber:

> […] a) harmonizar a tipicidade penal no ambiente do ciberespaço pelos Estados signatários; b) definir os elementos do sistema de informática promovendo a unidade na interpretação da legislação penal interna e possibilitar a credibilidade da prova eletrônica no ambiente virtual; c) implementar um sistema rápido e eficaz de cooperação internacional no combate à criminalidade informática. (BRITO, 2013, p. 56).

O autor explana que a adesão de novos Estados dá-se por convite e aprovação por maioria do Conselho, deixando ela própria a aplicação da Convenção a critério de cada Estado. Neste contexto, complementa, Tatiana Malta Vieira:

> Para adesão à Convenção **por países não membros do tratado**, o Comitê de Ministros do Conselho da Europa pode, após consultar os Estados participantes, convidá-los a aderir à Convenção (conforme art. 37° do tratado). (VIEIRA, 2009, p. 201, grifo nosso).

Tatiana salienta ainda, o procedimento que o Brasil deve adotar em caso de adesão:

> Procedimento a ser adotado pelo Brasil em caso de adesão: (i) assinatura pelo Presidente; (ii) aprovação pelo Congresso por meio de Decreto Legislativo; (iii) adesão pelo Presidente; (iv) promulgação mediante publicação do Decreto Presidencial respectivo. (Ibidem, p. 201).

Elucida-se que que a Convenção de Budapeste trata da cooperação internacional, da assistência mútua, da denúncia espontânea, da extradição e sugere procedimentos na ausência de acordos internacionais, além da definição da confidencialidade e limitações de uso.

5.1.2. A Convenção de Budapeste e a Legislação Penal Brasileira

Segundo Auriney Brito (2013) se considerarmos que um dos objetivos da Convenção é a uniformização da legislação penal para delitos informáticos cometidos no ciberespaço, há que se avaliar se o Brasil está atendendo de forma satisfatória aos requisitos no sentido da prevenção e repressão de crimes informáticos ou se ainda há correções a serem feitas na legislação brasileira.

Destarte, o autor expõe o que está definido na Convenção de Budapeste frente a legislação penal brasileira.

Umas das condutas de criminalização sugerida pela Convenção é o "*acesso ilegal*". Este delito abarca o acesso a qualquer parte de um sistema de computador – sem a devida permissão – desde que seja de forma intencional; motivo pelo qual não se prevê a tipicidade na modalidade culposa para essa espécie de delito.

O autor leciona que o dolo requerido na Convenção consubstanciaria a quebra de medidas de segurança, sem a autorização daquele que detém o poder de permitir o acesso, para obter dados de computador, ou outra desonra.

No que tange a legislação brasileira, Brito informa:

> Ao que se depreende, no Brasil a prática de acesso ilegal, com as elementares requeridas, já encontra um tipo penal abstrato recentemente criado para essa subsunção, sendo, portanto, típico nos termos do art. 154-A do Código Penal, ressalvada também a existência de um tipo específico para os pleitos eleitorais previsto no art. 72, I, da Lei n. 9.504/97.14. (BRITO, 2013, p. 59).

O art. 3º da Convenção sobre Cibercrime trata da *interceptação ilegal*, razão pela qual é recomendado aos Estados signatários adotar medidas legislativas para considerar tal conduta como crime.

> Assim como a anterior a conduta já se encontra criminalizada no Brasil por força do art. 10 da Lei n. 9.296/96, que estabeleceu o crime de interceptação não autorizada como sendo a conduta de "realizar interceptação de comunicação telefônicas, de informática ou telemática, ou quebrar segredo de justiça, sem autorização judicial ou com objetivos não autorizados por lei". (BRITO, 2013, p. 60).

[14] Art. 72, I. Constituem crimes, puníveis com reclusão, de cinco a dez anos:
I – obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos. (BRITO, 2013).

No art. 4º, a Convenção aparentemente repete a exigência determinando a criminalização de *interferência de dados*; no entanto, o documento elucida que o crime se refere à danificação, deleção, deteriorização, alteração ou supressão de *dados de computador* sem permissão, desde que seja com intenção e não a captação de informações privadas e íntimas, uma vez que já foi abarcada no artigo anterior.

> Como em todas as hipóteses, a Convenção não aceita a modalidade culposa do delito, o que, nessa espécie também não é aceito no Brasil, havendo necessidade de que haja a presença do *animus nocendi*. A conduta escrita, em tese, se encontra criminalizada pela redação do art. 163 do Código Penal, que prevê "Destruir, inutilizar ou deteriorar coisa alheia".
> Em razão e possíveis generalidades que tornariam o tipo penal inconstitucional, já tramitam no Congresso Nacional projetos de lei que visam alterar a redação do art. 163 do CP, ou criar uma nova modalidade de crime, que abrangeria os dados eletrônicos ou de computador, que não entrariam no conceito aberto de coisa alheia. (Ibidem, p. 60).

No art. 5º a Convenção sugere a criminalização da *interferência de sistema*, que encomenda punição para o ato que, de forma intencional, cause sério atraso, sem permissão, de funcionamento de sistema de computador, por meio de transmissão, inserção, danificação, deleção, deterioração, alteração ou supressão de dados do computador.

> O fato descrito, de acordo com as elementares apresentadas, em tese, já possuía um tipo penal genérico no Brasil. Trata-se do art. 256 e 266 do Código Penal, que considera crime contra a segurança do serviço de utilização pública a conduta que "atentar contra a segurança ou o funcionamento de serviço de água, luz, força ou calor, ou qualquer outro de utilidade pública"; ou do 266, em que "Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento" acarreta pena de detenção, de um a três anos, e multa.
> Porém, com a alteração promovida pela Lei n. 12.737/12 no Código Penal, foi acrescentado ao art. 266 o § 1º com redação mais específica: "Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento". (BRITO, 2013, p. 60-61).

No art. 6º da Convenção atribui-se relevância penal ao *mau uso de equipamentos*, sugerindo aos países signatários adotarem medidas legislativas para criminalizar a conduta de produção, venda, compra para uso, importação, distribuição ou disponibilização de dispositivos, que incluem programas de computador, projetados ou adaptados primariamente, com o propósito de cometer os delitos de *acesso ilegal*, *interceptação ilegal*, *interferência de dados e a interferência de sistema*, ou então a disponibilização de senha de computador,

código de acesso, ou dados similares, por meio dos quais o todo ou qualquer parte de um sistema de computador possa ser acessado com a intenção de praticar essas condutas.

O autor explana ainda que o mesmo artigo ainda menciona que a posse de qualquer dos materiais descritos utilizados com a intenção de cometer os delitos de acesso ilegal, interceptação ilegal, interferência de dados e interferência de sistema também deve ser considerado crime. Perscruta-se que essa hipótese prevê uma excludente de ilicitude quando o objeto do agente não seja o cometimento dos ilícitos.

> Com a alteração promovida pela Lei n. 12.737/12, o § 1º do art. 154-A trata exatamente da venda, distribuição ou difusão de dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput, que é o acesso ilegal.
> Atualmente a prática do *phishing*, que tem como principal meio de execução a remessa de milhares de mensagens eletrônicas (spam), com o objetivo de captar informações sigilosas que facilitem o acesso a determinadas vantagens, foi tipificada nesse artigo, importante inovação que, se não vier acompanhada de vantagem patrimonial indevida, não constitui fato típico no Brasil. (BRITO, 2013, p. 61).

No art. 7º da Convenção, encontra-se a tipificação do delito de *falsificação computacional*, que objetiva estabelecer como ofensa penalmente relevante a inserção, a alteração, a deleção ou a supressão de dados de computador, transformando-os em falsos com a intenção de serem considerados ou terem sido realizados para propósitos legais como se autênticos fossem.

> Atualmente a falsificação de qualquer documento, seja ele público ou particular, encontra tipificação na legislação penal brasileira, o que não acontece com o dado eletrônico ou de computador. Se o dado for um documento público ou particular, não há necessidade de alteração legislativa.
> O documento internacional não prevê nessa hipótese a existência de dano, bastaria a conduta de falsificar dado eletrônico no intuito de se passar por autêntico para a realização de propósitos legais que o exijam.
> Os projetos de lei que tramitam hoje no Congresso Nacional pretendem criar essa modalidade de delito ou alteração dos arts. 171, 297 e 298, todos do Código Penal.
> Já a fraude relacionada a computador, diferentemente da falsificação de dados eletrônicos, prevê as práticas de inserção, alteração, deleção, supressão de dados de computador ou qualquer interferência no funcionamento de um sistema de computador com intenção fraudulenta, de compra, para si ou para outrem, visando benefício econômico.
> **A discussão sobre essa conduta é grande na doutrina e na jurisprudência, pois se amolda nos crimes previstos nos arts. 155, § 5º (furto mediante fraude), e 171 (estelionato), *caput*, do Código Penal**. (BRITO, 2013, p. 62, grifo nosso).

Auriney Brito (2013) informa que já existe um ponto específico no Congresso Nacional Brasileiro, sobre essa problemática, a qual visa a criação de uma modalidade peculiar de crime previsto no art. 171 do Código Penal denominado estelionato eletrônico, o que, apesar da boa intenção, pode trazer consequências inesperadas e desastrosas. [15]

Desta feita, tal atividade legislativa só prejudicaria todo trabalho já realizado pela polícia, Ministério Público e Judiciário. Apesar da indefinição quanto ao tipo penal referente a essa prática, já se sabe que ele é típico com certa tendência ao tipo penal do art. 155, § 5º, conforme se concluiu no julgamento do conflito de competência n. 67.347:

> O furto mediante fraude não pode ser confundido com o estelionato. No furto, a fraude é utilizada para burlar a vigilância da vítima, para lhe tirar a atenção. No estelionato, a fraude objetiva obter o consentimento da vítima, iludi-la para que entregue voluntariamente o bem. Na hipótese, o agente valeu-se da fraude eletrônica via internet para subtrair valores da conta corrente de titularidade de correntista da CEF, assim há furto mediante fraude, essa usada para burlar o sistema de vigilância e proteção do banco aos valores mantidos sob sua guarda. Outrossim, é consabido que o furto consuma-se no momento em que o bem é subtraído da vítima, ao sair da esfera de sua disponibilidade, e o desapossamento, embora efetivado por meio digital, teve lugar na conta corrente da agência situada em Campo Mourão-PR, o que leva à fixação da competência na vara federal daquela cidade (STJ. Terceira Seção. Relatora Ministra Laurita Vaz). (BRITO, 2013, p. 63).

Analisando essa situação, o autor entende que a consequência principal absolutamente dispensável refere-se ao fato de que já existem muitas condenações às penas do estelionato simples e muitas outras por furto mediante fraude para pessoas que obtiveram vantagem indevida após uma fraude eletrônica. Destarte, o advento de uma lei que cria um novo tipo penal específico para esses casos é a declaração oficial de antes da referida lei esse fato era atípico. E em nome dos princípios da reserva legal e da anterioridade penal seria extinta a punibilidade de todos os criminosos já condenados, gerando algo que se pode denominar de *atipicidade retroativa*.

A Convenção não olvidou a questão das ofensas relacionadas à violação de direitos autorais ou imateriais - mesmo já possuindo outros instrumentos

[15] Refere-se ao Projeto de lei n. 76/2000, de relatoria do Senador Eduardo Azeredo, que pretende alterar o Código Penal para incluir o Estelionato eletrônico como espécie do gênero Estelionato. (BRITO, 2013, p. 62).

vinculantes – tais quais: o Ato de Paris, de 24 de julho de 1971, da Convenção *de Berna*, para a proteção dos trabalhos literários e artísticos; o acordo sobre os Aspectos dos Direitos de Propriedade Intelectual Relacionados como o Comércio; e o Tratado de Direitos Autorais WIPO, com a exceção de quaisquer direitos morais conferidos por tais Convenções, em que tais atos sejam cometidos intencionalmente e por meio de computador - em uma escala comercial - assim como inúmeros outros documentos que recomendam a criminalização dessas condutas violadoras de direitos de autor e correlatos.

> A legislação brasileira possui regramento específico sobre o tema, como a Lei n. 9.609, de 1998 (Lei do *Software*), a Lei n. 9.610, de 1998 (Lei do Direito Autoral) e da Lei n. 10.695 de 2003.
> No entanto, muito embora o Brasil já tenha se adiantado a respeito do assunto, acredita-se que a Convenção quer estabelecer crimes próprios, pois nessa hipótese pretende outro julgamento para condutas praticadas através da rede mundial de computadores.
> O Ministério da Justiça sugeriu que esse dispositivo deva ser reservado integralmente com a emissão de uma declaração unilateral, pois entende que a Convenção de Budapeste é incompatível com a legislação interna. (BRITO, 2013, p. 63-64).

A Convenção também alvitrou a punição para *tentativa, ajuda ou encorajamento* para o cometimento das condutas de acesso ilegal, interceptação ilegal, interferência de dados, interferência de sistema, mau uso de equipamentos, falsificação relacionada a computador, fraude relacionada a computador, danos relacionados à pornografia infantil, ofensas à transgressão de direitos autorais e direitos correlatos, e responsabilidade corporativa.

> Tais condutas já se encontram perfeitamente tipificadas em nosso ordenamento jurídico nos arts. 14, II, 29, e 286, todos do Código Penal.
> O art. 14, II, do Código Penal se coaduna com a sugestão de *tentativa* da Convenção de Budapeste, no qual descreve que "tentado, quando, iniciada a execução, não se consuma por circunstâncias alheias à vontade do agente", que no nosso entender encontra texto satisfatório para o *enquadramento* das condutas sugeridas pela Convenção.
> No que diz respeito ao termo ajuda utilizado pela Convenção, percebe-se que o art. 29 do Código Penal, com seu texto que determina: "quem, de qualquer modo, concorre para o crime, incide nas pena a este cominadas, na medida de sua culpabilidade", já vem a contemplar a intenção do documento internacional.
> Por último, o termo encorajamento, também previsto na Convenção encontra contemplação do art. 286 do Código Penal, deixando de fora o crime, com o texto: "incitar publicamente a prática de crime", contudo, a modalidade de delito de apologia pode se consumar se a incitação for de maneira genética. (BRITO, 2013, p. 64-65).

A Convenção esclarece que a incitação deve ser aos crimes de acesso ilegal, interpretação ilegal, interferência de dados, interferência de sistema, mau uso de equipamentos, falsificação relacionada a computador, fraude relacionada a computador, danos relacionados à pornografia infantil, ofensas relacionadas à transgressão de direitos autorais e direitos correlatos, diferente da legislação brasileira, que abarca qualquer modalidade de delito previamente estabelecido.

Uma questão bastante interessante trazida pela Convenção é justamente a possibilidade de responsabilização penal do provedor de acesso, a qual:

> [...], Não contemplada pela Constituição Federal de 1988 e tampouco pela legislação infraconstitucional, com a devida *vênia* aos que entendem de maneira diversa em face da leitura do art. 241 do Estatuto da Criança e do Adolescente, matéria que será discutida em momento oportuno. (BRITO, 2013, p. 65).

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

O autor informa ainda que o documento confere aos Estados discricionariedade para tomar outras medidas necessárias para assegurar que a pessoa jurídica também seja responsabilizada como, por exemplo, nos casos em que houver falha de supervisão ou controle por uma pessoa física, ou seja, aqui se pretende punir a omissão penalmente relevante, com previsão legal absolutamente satisfatória na legislação penal brasileira.

> Recentemente aprovado, o Projeto de Lei de autoria do senador Eduardo Azeredo, substitutivo dos Projetos de Lei do senado n. 76/2000, 137/2000 e do Projeto da Câmara n. 89/2003, visa alterar o Decreto-lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-lei n. 1001, de 21 de outubro de 1969 (Código Penal Militar), a Lei n. 7.716, de 5 de janeiro de 1989, e Lei n. 8.069, de 13 de julho de 1990, e a Lei n. 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

> O projeto sugeriu a criminalização de diversas condutas, dentre as quais podemos citar o *acesso desautorizado* à rede de computadores, dispositivo de comunicação ou sistema informatizado, conduta que, de acordo com a classificação apresentada no capítulo anterior, representada a categoria dos delitos informáticos próprios, e poderia ser visto, até pouco tempo atrás, como um exemplo claro da hemiplegia legislativa no que concerne a condutas praticadas exclusivamente no âmbito informático.
> De um lado, portanto, têm-se os delitos impróprios já resguardados pela legislação penal existente, e de outro, representando uma pequena porcentagem de condutas – mas, como já se observou, com alto grau de relevância – têm-se os delitos próprios, que, pela ausência de legislação, relevância paralisada a atuação do Estado. (BRITO, 2013, p. 66-67).

É importante colacionar os principais desafios e dificuldades no combate ao cibercrime no Brasil destacados por Tatiana Malta Vieira em 2009, bem como o processo de superação da lacuna legislativa exposto por Patrícia Peck Pinheiro:

> (a) A morosidade das reformas legislativas necessárias quando comparada ao rápido avanço da tecnologia;
> (b) A falta de aparelhamento da Polícia Judiciária e de técnicos habilitados, notadamente número suficiente de peritos de informática para efetuar diligências em todo o território nacional;
> (c) A identificação de usuários de cibercafés, *lanhouses* e redes *wireless,* tendo em vista a ausência de regulamentação e fiscalização dessa atividade pelo Poder Público;
> (d) A profissionalização de organizações criminosas especializadas em crimes cibernéticos, principalmente pornografia infantil, fraudes bancárias e financeiras, lavagem de dinheiro, espionagem industrial, produção e disseminação de códigos maliciosos;
> (e) O baixo investimento em segurança da informação, especialmente nas organizações públicas, o que aumenta as vulnerabilidades das infra-estruturas críticas tais como água, energia, telecomunicações, transporte e saúde;
> (f) O crescente uso de estenografia e de outras técnicas para esconder imagens de pornografia infantil e de outros conteúdos ilícitos;
> (g) A disseminação do uso de recursos criptográficos nas organizações criminosas aliada à falta de controle da importação, exportação e distribuição dessa tecnologia de uso dual;
> (h) O caráter transnacional dos delitos, o que exige cooperação jurídica internacional calcada em procedimentos ágeis e eficazes à prevenção e repressão desses ilícitos. (VIEIRA, 2009, p. 204-205).

Patrícia Peck Pinheiro (2013, p. 94-95) informa que alguns estados brasileiros já possuem legislação específica no que tange ao item “c” da lista acima relacionada, a qual determina a identificação de usuários de c*ybercafé* e *lanhouse,* conforme tabela abaixo:

Tabela 1- Estados onde há lei para *cybercafé* e *lanhouse*

UF	LEGISLAÇÃO	UF	LEGISLAÇÃO
ACRE	Não há	PARÁ	Não há
ALAGOAS	Lei n. 6.891/2007	PARAÍBA	Lei n. 8.134/2006
AMAPÁ	Lei n. 1.047/2006	PARANÁ	Não há
AMAZONAS	Leis ns. 3.173/2007 e 3.351/2008	PERNAMBUCO	Projeto de Lei n. 143/2007
BAHIA	Projeto de Lei n. 17.362/2007	PIAUÍ	Lei n. 5.747/2008
CEARÁ	Não há	RIO DE JANEIRO	Lei n. 5.132/2007
DISTRITO FEDERAL	Lei Distrital n. 3.437/2004	RIO GRANDE DO NORTE	Não há
ESPÍRITO SANTO	Lei n. 8.777/2007	RIO GRANDE DO SUL	Lei n. 2.698/2007
GOIÁS	Não há	RONDÔNIA	Não há
MARANHÃO	Não há	SANTA CATARINA	Não há
MATO GROSSO	Lei n. 8.502/2006	SÃO PAULO	Lei n. 12.228/2006
MATO GROSSO DO SUL	Lei n. 3.103/2005	SERGIPE	Não há
MINAS GERAIS	Projeto de Lei n. 1.720/2007	TOCANTINS	Não há

Desta feita, Tatiana Malta Vieira propõe cotejar a legislação nacional com a Convenção de Budapeste de forma a subsidiar eventuais propostas de reformas penais na legislação pátria, considerando-se os principais fatores críticos à prevenção e ao combate ao cibercrime no Brasil.

Auriney Brito conclui que boa parte das condutas apresentadas como merecedoras de pena, pela Convenção de Budapeste, já se encontram na legislação penal brasileira. No entanto, muitos projetos de lei, ainda vêm sofrendo alterações substanciais em seu conteúdo - devido à importância da intervenção de profissionais especializados em delitos informáticos - para que não se aprove uma lei que gere problemas de ordem prática ou que apresente dispositivos que desrespeitem preceitos fundamentais do Estado Democrático de Direito.

5.2. APLICAÇÃO DA LEGISLAÇÃO COMPARADA SOBRE DELITOS INFORMÁTICOS EM OUTROS PAÍSES

Auriney Brito (2013) expõe a legislação comparada sobre delitos informáticos em vários países, tais quais: Alemanha, Áustria, Suíça, Portugal, França, Bélgica, Itália, Espanha, Inglaterra, Chile, México, Peru, Venezuela, Bolívia, Costa Rica, Equador, Estados Unidos da América, Canadá e Holanda.

Segundo Auriney (2013, p. 76) pode-se afirmar que a Alemanha, a partir da década de 1970, “foi o primeiro país a manifestar interesse na alteração legislativa de combate à criminalidade informática”. Na época o movimento teve início para controle da atividade econômica, devido à preocupação com as fraudes financeiras realizadas através de computadores.

O doutrinador alemão Klaus Tiedemann (1985, p, 124) narra em sua obra *Poder económico y delito* “Um fato ocorrido na Alemanha Federal em 1973, onde um funcionário público, manipulando os computadores do órgão, desviou entre 5.000 (cinco mil) e 10.000 (dez mil) marcos alemães de diversas contas bancárias”.

Segundo Auriney Brito (2013), em 1978 houve o início das modificações, especialmente nas áreas de fraudes eletrônicas, tendo em vista o reconhecimento da possibilidade de cometer crimes mediante o uso de computadores.

Para fazer frente à delinquência relacionada com a informática e com os efeitos, a partir de 1º de agosto de 1986, adotou-se a Segunda Lei contra a Criminalidade Econômica, de 15 de maio de 1986, a qual contemplava os seguintes delitos:

> Delitos de pirataria informática, danos de coisas, alteração de dados, sabotagem de computadores. Todos admitiam tentativa, e os três casos de identificação pela autoria policial de causa especial de interesse público. (LÓPEZ DIAS, 1999, p. 236-310).

Na Áustria, a reforma do Código Penal local é de 22 de dezembro de 1987 e contemplou figuras relativas à destruição de dados pessoais, não pessoais e programas que causem prejuízos econômicos, resultando, desse modo, na Lei n. 565, de proteção de dados pessoais, de 18 de outubro de 1978 (*Bundesgesetz über den Schutz personembezogener Daten*):

Art. 126. Destruição de dados

> 1. Quem prejudicar a outro através da alteração, cancelamento, inutilização, ou ocultação de dados protegidos automaticamente, sigilo ou divulgados, sobre os quais careça no todo ou em parte de disponibilidade, será punido com pena privativa de liberdade de até seis meses ou com pena de multa de até 360 dias-multa. (BRITO, 2013, p. 77).

Na Suíça, Auriney Brito (2013, p. 77) informa que o art. 144 do Código Penal prevê como condutas típicas: “As de modificar, apagar, ou abusar de informação registrada ou transmitida de modo eletrônico ou meio similar. Tais condutas ilícitas serão punidas com pena de prisão ou multa”. Logo, trata-se de crimes de ação penal privada, salvo se o dano produzido seja considerável, ocasião em que a persecução penal será de ofício. Desta feita, todas essas condutas encontram-se reunidas no capítulo de crimes contra o patrimônio.

Portugal foi um dos primeiros países a ter uma lei específica disciplinando a matéria, a Lei n. 109, de 18 de agosto de 1991 – Lei de Criminalidade de Informática.

O autor relata que a referida lei traz em seu bojo os conceitos de rede informática, sistema informático, programa informático e interceptação.

Feita a conceituação, Brito (2013, p. 78, grifo nosso) explana que a lei criminaliza a conduta de dano relativo a dados ou programas informáticos com pena que varia de acordo com o valor do dano causado. “Se for de valor elevado, a pena será de **5 anos ou multa de 600 dias-multa**. Se for de valor consideravelmente elevado, a pena será de **1 a 10 anos**).

Dentre os diversos crimes informáticos contidos na lei, o autor destaca as penalidades da *sabotagem informática*, *acesso ilegítimo* e *interceptação ilegítima:*

> No artigo sexto criminaliza a ***sabotagem informática*** com pena de **até 5 anos ou multa de 600 dias-multa**. Se o dano for **consideravelmente elevado, a pena será de 1 a 10 anos**. No artigo sétimo aparece o crime de ***acesso ilegítimo*** com **pena de prisão de até um ano ou pena de multa de até 120 dias-multa**. Por último, no artigo oitavo, torna crime a conduta de ***interceptação ilegítima***, fixando a **pena de prisão de até três anos ou pena de multa**. (BRITO, 2013, p. 78, grifo nosso).

O autor relata que deva ser aplicado, de forma subsidiária, o Código Penal português para a referida legislação.

A França, em 5 de janeiro de 1988, editou a Lei n. 88/19 (Lei *God-frain*), tratando de fraude informática, onde restaram criados tipos penais como: “os de acesso fraudulento a um sistema informático, sabotagem informática, destruição

de dados, falsificação de documentos informatizados e uso de documentos informatizados falsos".

Auriney (2013) informa que em razão das modificações correspondentes aos anos de 2000, 2002 e 2004, o Código Penal francês passou a prever delitos informáticos da seguinte forma:

> **Acessar ou manter-se fraudulentamente**, no todo ou em parte, em um sistema de tratamento automatizado de dados, é punível **com 2 anos de prisão e 30.000 euros de multa** Se resultar **supressão ou modificação de dados informáticos** contidos no sistema, ou **qualquer alteração deste**, a pena **será de 3 anos de prisão e 45.000 euros de multa**. **Introduzir fraudulentamente dados** em um sistema de tratamento automatizado ou **suprimir ou modificar fraudulentamente os dados** que contém, é punível com **5 anos de prisão e 75.000 euros de multa** (BRITO, 2013, p. 79, grifo nosso).

Na Bélgica, em fevereiro de 2001, o parlamento incorporou ao Código Penal condutas como o *hacking*, a sabotagem e a fraude informática.

A Itália criou a Lei n. 547, de 23 de dezembro de 1993, que trouxe significativas modificações e integrações das normas do Código Penal e do Código de Processo Penal, inserindo princípios aos crimes de informática. Em suma, o autor (2013, p. 79) informa que "A legislação italiana preferiu dar uma adaptada dos artigos, conferindo verdadeira solução metodológica na interpretação da lei penal, ampliando conceitos, por exemplo, integrando de modo harmônico os princípios, não conferindo aos crimes de informática tratamentos diferenciados".

Destaca-se com um dos mais interessantes, o art. 615 do Código Penal italiano, que equiparou à tradicional invasão de domicílio a invasão do sistema informático, criando três novas figuras:

> a) Acesso não autorizado a um sistema de computadores ou telecomunicações; b) posse e disponibilidade de códigos de acesso a sistemas de computadores ou telecomunicações; c) difusão de programas que possam causar danos ou interromper sistemas de computação. (BRITO, 2013, p. 79).

Na Espanha, segundo Brito (2013, p. 80) houve atenção às recomendações existentes de organismos internacionais, alterando por completo a versão do Código Penal (Lei Orgânica n. 10, de 23 de novembro de 1995), no qual inseriu "repressão aos delitos de alta tecnologia, modificações tanto na Parte Geral quanto na Parte Especial e inovação de tratar de indenizações a título de reparação civil".

Brito (2013, p. 80, grifo nosso) informa que na Inglaterra, em 1991, foi criada a *Computer Misure Act* (Lei de Abusos Informáticos), “em que a maior preocupação do legislador foi com a integridade dos dados informáticos, **punindo, com até 5 anos de prisão**, quem impedisse, alterasse ou dificultasse o acesso a dados informáticos confiáveis”.

Ressalte-se ainda que a Inglaterra tipificou acesso não autorizado e modificação não autorizada de material por meio *do Computer Crime Act from Great Britain*.

O Chile foi o primeiro país da América Latina a modernizar seu arcabouço punitivo no que concerne à criminalidade informática. Em 29 de maior de 1993, foi editada a Lei n. 19.223, que tipificou como crimes algumas condutas novas como:

> Destruição ou inutilização maliciosa de *hardware* e *software*, assim como alteração de seu funcionamento; acesso ilegítimo a informação de um sistema com a finalidade de dela apodera-se, usá-la ou conhecê-la indevidamente; difusão maliciosa de dados sigilosos etc. (BRITO, 2013, p. 80)

No México, o Código Penal sofreu uma alteração em 1999, quando o seu art. 211 foi expandido para enquadrar diversas condutas relacionadas ao uso de computadores.

No Peru, em 2000, foi acrescentado ao Código Penal, um capítulo específico sobre crimes informáticos, criando os arts. 207-A; 207-B e 207-C.

A Venezuela tratou de criar uma lei especial:

> Com definição inicial, objetivo, conceitos e tipos em espécies dos delitos cibernéticos, dando proteção integral dos sistemas que utilizam tecnologias de informação, prevendo, além de uma sanção penal, aspectos preventivos. **As definições de termos técnicos impedem dúvidas de interpretação**. (BRITO, 2013, p. 80)

O autor afirma que a Venezuela tratou cuidadosamente do regramento específico dos delitos em ambiente virtual, pois se atentou para os problemas da extraterritorialidade, adotou a responsabilidade penal das pessoas jurídicas (provedores de acesso) e incluiu dispositivos atinentes à indenização civil.

Na Bolívia, através da Lei n. 1.768, de 10 de março de 1997, houve uma reforma no Código Penal que incorporou as seguintes figuras:

A primeira incorporação se refere à *Manipulação Informática* que preconiza:

> Aquele que, com a intenção de obter um benefício indevido para si ou terceiro, manipule um processamento ou transferência de dados informáticos que conduza a um resultado incorreto ou evite um processamento cujo resultado seria correto, ocasionando, dessa maneira, uma transferência patrimonial em prejuízo de terceiro, **será sancionado com reclusão de um a cinco anos e multa de 60 a 200 dias**. (BRITO, 2013, p. 81, grifo nosso)

A segunda incorporação diz respeito *a Alteração, acesso e uso de dados informáticos*:

> Aquele que, sem autorização, se apodere, acesse, utilize, modifique, suprima ou inutilize, dados armazenados em um computador ou em qualquer suporte informático, ocasionando prejuízo do titular da informação, **será sancionado com prestação de trabalho por até um ano ou multa de até duzentos dias**. (Ibidem, p. 81, grifo nosso).

Na Costa Rica, a Lei n. 8.148 agregou os arts. 196, 217 e 229 ao Código Penal do país, criminalizando as seguintes condutas:

Art. 196 – Violação de comunicações eletrônicas:

> Será punido com pena de **prisão de seis meses a dois anos** a pessoa que, para descobrir os segredos ou violar a intimidade de outro sem o consentimento, se apodere, acesse, modifique, altere, suprima, intercepte, interfira, utilize, difunda ou desvie de seu destino, mensagens, dados e imagens contidas em equipamentos: eletrônicos, informáticos, magnéticos e telemáticos. **A pena será de um a três anos de prisão** se as ações descritas forem praticadas por pessoas encarregadas de operar o equipamento. (BRITO, 2013, p. 81, grifo nosso).

Art. 217- Fraude informática:

> Será imposta **a pena de prisão de um a dez anos** à pessoa que, com a intenção de procurar ou obter um benefício patrimonial para si ou para terceiro, influencie no processamento ou resultado dos dados de um sistema de computador, mediante programação, emprego de dados falsos ou incompletos, uso indevido de dados ou qualquer outra ação que incida no processo dos dados do sistema. (Ibidem, p. 81, grifo nosso).

Art. 229- Alteração de dados e sabotagem informática:

> Será imposta **a pena de prisão de um a quatro anos** a pessoa que, por qualquer meio, acesse, apague, suprima, modifique ou inutilize sem autorização os dados registrados em um computador. (Ibidem, p. 81-82, grifo nosso).

O autor (2013, p. 82, grifo nosso) explana ainda: “Se como resultado das condutas indicadas se entorpece ou se inutiliza o funcionamento de um programa de computador, uma base de dados ou um sistema informático, **a pena será de três a seis anos de prisão**”. Bem como, “Se o programa de computador, a

base de dados ou sistema informático contém dados de caráter público, será imposta **pena de prisão de até oito anos**".

No Equador, a Lei de Comércio, Firmas Eletrônicas e Mensagens de Dados, vigente desde 2002, incorporou ao Código Penal crimes como "violação de comunicações privadas, violação gravada de comunicações, captação de comunicações e dano informático".

Nos Estados Unidos da América, Auriney Brito (2013, p. 82) ensina que é importante levar em consideração o "*The National Information Infrastructure Proteccion Act*, que alterou o *The Computer Fraud and Abuse Act,* em 1996, no sentido de eliminar dúvidas legislativas relacionadas a *vírus*, *cavalos de tróia* e outros programas considerados nocivos aos dispositivos informáticos".

Acrescentaram-se também dois tipos penais relacionados à criação e transmissão de vírus de computador, ao dano informático e ao acesso desautorizado.

O autor ressalta ainda:

> Praticamente todos os Estados norte-americanos têm suas legislações locais e cada uma delas possui **um elenco de dispositivos dedicados a coibir práticas criminosas relacionadas a computadores, uma mais, outras menos rigorosas, mas nenhuma delas com falhas que possam facilitar a impunidade**. Em caso de conflito entre leis estaduais e a federal, esta última é a que prevalece. (BRITO, 2013, p. 82, grifo nosso)

No Canadá seu Código Penal destaca o acesso não autorizado, danos informáticos e obstrução de tráfego de sistemas.

Por fim, o autor destaca o último país citado em sua obra (2013, p. 82), a Holanda, que teve o "*Dutch Computer Crime Act*, que define termos e tipifica condutas indesejáveis relacionadas ao mau uso da internet".

Auriney Brito (2013) percebe que a preocupação com crimes eletrônicos tornou-se fator universal, razão pela qual surge a proposta da Convenção de Budapeste, com intuito de uniformizar a legislação mundial para combater o aumento da delinquência informática, recomendando a criminalização de algumas condutas, bem como incentivando a cooperação internacional entre os países.

Destarte, por se tratar de um tópico que versa sobre o direito comparado entre vários países, nada mais justo que fazer um confronto entre a Lei Francesa e a Lei Brasileira no que tange à pena privativa de liberdade e à multa.

Assim, se tomarmos por base o crime: **introduzir fraudulentamente dados em um sistema de tratamento automatizado** na lei francesa com **instalar vulnerabilidades para obter vantagem ilícita** na lei brasileira (art. 154-A, segunda parte), haverá uma discrepância significativa no que se refere à punibilidade do agente, pois: na lei francesa a pena é de 5 (cinco) anos e multa de 75.000 euros e na lei brasileira, a pena varia de 3 (três) meses a 1 (um) ano e multa de R$?

Para se ter uma ideia do valor da multa aplicada aos crimes informáticos franceses, há que se perscrutar a cotação do euro (€). Desta feita: 1,00 € vale R$ 3,10 (Disponível em: <http://www.wap.economia.uol.com.br/cotacoes>. Acesso em: 26 abr 2014). Ou seja, se o agente cometer o crime na França pagará cerca de R$ 232.500,00 (duzentos e trinta e dois mil e quinhentos reais) além da pena de 5 (cinco) anos de prisão, ao passo que no Brasil a pena varia de 3 (três) meses a 1 (um) ano e multa a cargo do juiz. Sem contar na possibilidade de conversão da pena privativa de liberdade em pena restritiva de direito, uma vez que o delito se encaixa no *quantum* delimitado no art. 44, §2º do Código Penal (igual ou inferior a 1 (um) ano)), assim, o agente brasileiro pode acabar prestando serviços à comunidade (art. 43, IV do Código Penal).

5.3. MANUAL PARA PREVENÇÃO E CONTROLE DE DELITOS RELACIONADOS COM COMPUTADORES ELABORADO PELA ONU

Segundo Spencer Toth Sydow (2013) a imaterialidade dos delitos informáticos propriamente ditos frente aos modelos preventivos apresentados mostram-se parcialmente capazes de produzir efeitos na realidade atual.

Desta feita, o autor relata que a mera análise da problemática dos delitos informáticos, leva-nos a um incômodo e inquietante vazio, seja numa perspectiva legalista, seja numa perspectiva criminológica, e ainda mais especificamente na ótica vitimológica.

Diante de tais óticas, Spencer conclui que torna-se possível aos pensadores propor novos e mais complexos modelos de manutenção do fenômeno delinquente a níveis toleráveis.

5.3.1. Principais Problemas na Temática

Inicialmente Spencer (2013) relata a importância de demonstrar a maneira com a qual a doutrina vem se manifestando quanto a este problema, para que em seguida, apresente-se uma proposta, razão pela qual, explana, Susan W. Brenner:

> Apresenta inicialmente **quatro frentes de atuação para o combate ao delito informático**, que denominou nova estratégia de controle de crimes: **a partir dos apontamentos feitos pelas convenções sobre ciberdelitos de Conselho da Europa e da Organização das Nações Unidas; a partir de técnicas legais de coação pós-fato; a partir de técnicas civis de reação; e a partir de um aumento de fiscalização e controle nas mãos das autoridades**. (BRENNER, 2007, p. 17-22, grifo nosso).

O autor expõe que a ONU elaborou um texto denominado “Manual para Prevenção e Controle de Delitos Relacionados com Computadores, em sentido amplo, em que aponta quais seriam os principais problemas na temática, os quais são:

> a) a falta de um consenso global sobre quais tipos de conduta deveriam ser considerados delitos relacionados com computadores;
> b) a ausência de um consenso acerca da definição legal de condutas criminosas;
> c) ausência de conhecimento técnico por parte da polícia, Ministério Público e das cortes ao tratar do tema;
> d) a falta de adequação dos poderes para investigar e acessar sistemas informáticos, incluindo a inaplicabilidade dos poderes de sequestro (medidas constritivas) para bens intangíveis como os dados computadorizados;
> e) a falta de harmonia entre procedimentos legais de diferentes nações concernentes à investigação de delitos relacionados com computadores;
> f) a caráter transacional de muitos delitos de computador; e;
> g) a falta de tratados de extradição e de assistência mútua e mecanismos de coação sincronizados que permitam a cooperação internacional, ou a incapacidade que os tratados existentes têm para lidar com as necessidades especiais de investigação de delitos de computador. (SPENCER, 2013, p. 252).

Spencer (2013) verifica que é de suma importância a identificação de problemas na nova casuística da criminalidade, bem como que a elaboração da proposta de prevenção e controle de delitos informáticos seja capaz de contribuir, de alguma forma, para uma melhor compreensão e mantença de tal tendência a níveis mínimos.

5.3.2. Propostas para Sanar os Problemas Sugeridos pelo Oitavo Congresso das Nações Unidas Para Prevenção de Crimes e Tratamento de Criminosos

Spencer (2013) explana que o Oitavo Congresso das Nações Unidas Para Prevenção de Crimes e Tratamento de Criminosos, como resposta a tais problemáticas, sugeriu como propostas especificamente:

> a) Modernização das leis e procedimentos criminais, incluindo-se medidas para:
> 1. assegurar que os tipos existentes e as leis relativas a poderes de investigação e admissibilidade de evidências em procedimentos judiciais apliquem-se adequadamente e, se necessário, fazer mudanças;
> 2. na falta de leis que se apliquem adequadamente, criar tipos penais e procedimentos investigativos para coleta de evidências que necessariamente sejam capazes de lidar com as novas e sofisticadas formas de atividade criminosa;
> 3. providenciar o confisco ou a restituição de bens adquiridos ilegalmente pelo cometimento de delitos relativos a computador;
> b) Melhoria de segurança de computadores e medidas de prevenção, levando-se em conta problemas relacionados à proteção da privacidade, o respeito aos direitos humanos e direitos fundamentais e qualquer mecanismo regulatório pertinente a uso de computadores;
> c) Adoção de medidas para sensibilizar o público, o judiciário e as agências reguladoras sobre o problema e a importância da prevenção acerca de delitos relacionados a computadores;
> d) Adoção de medidas para treinamento adequado de juízes, oficiais e agências reguladoras responsáveis pela prevenção, investigação, persecução e adjudicação de delitos econômicos e relacionados a computadores;
> e) Elaboração, em colaboração com organizações interessadas, de regras sobre ética no uso de computadores e ensinamento de tais regras como parte do currículo e treinamento em informática;
> f) Adoção de políticas para as vítimas de delitos relacionados com computadores para que sejam conscientes com a Declaração das Nações Unidas de Princípios Básicos de Justiça para Vítimas de Crime e Abuso de Poder, incluindo a restituição de bens ilegalmente obtidos e medidas de encorajamento das vítimas a comunicar tais crimes às autoridades competentes. (SPENCER, 2013, p. 253-254).

Spencer (2013, p. 254) expõe que nesse sentido, os próprios Estados Unidos da América do Norte desenvolveram legislações e órgãos de plantão e apoio a delitos informáticos, como por exemplo, o CHP (*Califórnia Higway Patrol*) e o ICCC (ou IC3 – *Internet Crime Complaint Center*), que têm como objetivo “fornecer auxílio e presteza na investigação da criminalidade, apoiando nas investigações por meio da rede mundial de computadores”.

Quanto ao segundo ponto, o autor elucida que alguns doutrinadores questionam qual seria o melhor método positivista para combater a criminalidade

informática, abrindo-se vista para duas possíveis ações de política criminal legalista[16]: a criação de "*do laws*" e a criação de "*do not laws"*, onde:

> As ***do laws*** seriam as normas que determinam uma obrigação de fazer (ou um ônus) que, desatendida, geraria consequências. As ***do not laws*** seriam, reversamente, normas que determinam deveres de abstenção ou obrigações (rectius, recomendações) de não fazer. (SPENCER, 2013, p. 255, grifo nosso).

Assim, o autor (2013) leciona que as normas que determinam que os cidadãos sigam certa conduta, por exemplo - a determinação para o uso do cinto de segurança – são aquelas que criam sanções para o desrespeito a tal obrigação, ou seja, se não usar o cinto de segurança, gera sanção pecuniária. Por outro viés, as normas que apontam para um não agir, pedem uma abstenção que deve ser respeitada, exemplo, as leis penais que tipificam condutas que, uma vez desrespeitadas, avoca a atuação do poder-dever de punir do Estado.

Acredita-se precipitada a sugestão de "*do laws*", pois os usuários teriam um ônus deveras imenso, uma vez que estariam obrigados a se defender de ataques complexos, ou seja:

> **Estar-se-ia transferindo ao usuário a obrigação de** compreender os meios técnicos de alta complexidade (programas), utilizá-los de modo adequado para impedir ações delinquentes, além de ser obrigado a modificá-los e atualizá-los constantemente para somente assim serem capazes de afastar as ameaças de modo eficiente. **Acrescente-se ainda, o fato de que tais programas ainda deveriam ser gratuitos para garantir o acesso defensivo a todos os usuários**, o que certamente não se atina à tendência pátria. (Ibidem, p. 255-256, grifo nosso).

Além disso, o autor defende que o caráter técnico do conhecimento informático geraria uma obrigação desproporcional ao usuário, ao passo que também surgiria para o Estado uma obrigação de punir de duvidosa aplicabilidade.

Quanto à necessidade de autoridades é imprescindível:

> Que mais delegacias de polícia estejam preparadas para atender às denúncias do cidadão atacado pelo ofensor informático; autoridades policial e judicial devem ser capazes de compreender os novos rumos tomados pela criminalidade, os novos meios utilizados e os novos bens jurídicos. Devem ser treinados para entender as

[16] Alguns doutrinadores já propuseram, também, sanções eletrônicas promovidas pelo poder de punir, para reagir ao crime informático, a partir de disseminação de códigos maliciosos, destruição e ações para tornar indisponível o aparato, sistema ou site de um delinquente desta esfera. Contudo, deixaremos de apontar tal solução como jurídica, tendo-se em vista que os mecanismos de controle de tais atos, mão de obra capacitada e a provável ineficácia de tais ações, além de possíveis abusos, seriam problemas consequentes a serem enfrentados. Nesse sentido, REINDENBERG, J. (2004).

> características específicas geradas pelo novo ferramental e, então, especializarem atendimento em tais delitos. (Ibidem, p. 256).

Por fim, Spencer (2013) orienta que os usuários devem se prevenir, uma vez que os agentes procuram as vítimas que favorecem as condutas criminosas.

5.4. CONSCIENTIZAÇÃO E ORIENTAÇÃO AOS USUÁRIOS DA INTERNET E DEMAIS MEIOS ELETRÔNICOS

Segundo Marcela Buscato (2012), muitos criminosos cometem delitos informáticos a partir de dados fornecidos pelas próprias vítimas em redes sociais e de descuidos na segurança do computador e dos dados.

Rodrigo Vale, chefe do grupo de operações da Delegacia de Repressão aos Crimes de Informática, relata que:

> **A maior ferramenta do hacker é a engenharia social**. […]. As pessoas mostram a casa, fazem fotos, mostram os filhos, os nomes, endereços, tudo. Alguém pode reunir esses dados e cometer fraudes em compras on-line ou tentar falsos sequestros por telefone. (VALLE, 2012, apud BUSCATO, 2012, p. 84, grifo nosso).

Foi assim, que o *hacker* americano Christopher Chaney, de 35 (trinta e cinco) anos, conseguiu entrar em todas as contas de *e-mails* de 50 (cinquenta) celebridades e acessar todos os documentos e imagens que estavam armazenados, da seguinte maneira:

> Ele clicava no botão "**senha esquecida**" **e testava a combinação com base em informações colhidas na internet sobre a vida das celebridades: data de nascimento, apelidos, nome do animal de estimação**. Famosos como **Scarlett Johanson tinham senhas previsíveis a ponto de ser advinhadas por Chaney**. Milhões de pessoas ao redor do mundo puderam saciar sua curiosidade sobre o corpo da atriz vendo as imagens que ela mesma tinha feito para seu marido à época, o ator Ryan Reynolds. Depois do escândalo, Chaney foi descoberto por uma investigação do FBI, a Polícia Federal americana. Ele está preso […]. (BUSCATO, 2012, p. 84, grifo nosso).

Segundo Alessandra Medina (2012), além de divulgar as fotos de Scarlet Johanson, Chaney divulgou fotos da Vanessa Hudgens, Mila Kunis, Christina Aguilera. Também já foram expostas Rihanna, Blake Lively e Miley Cirus.

Auriney Brito (2013) explana que atualmente, a prática mais comum na internet que exige a colaboração da vítima é o *fishing*. Normalmente esses ataques

são realizados através do envio de *e-mails* com assuntos atuais, notificações de órgãos públicos, cobranças dos serviços de proteção ao crédito, fotos de modelos famosas etc, com o objetivo de “pescar” as senhas das vítimas. Os bancos já criaram campanhas educativas de proteção ao uso da internet pois muitas pessoas estavam recebendo *e-mails* solicitando suas informações bancárias, recadastramento de dados, inclusive mediante páginas falsas que imitavam a página verdadeira, tudo para induzir o cliente a erro, com vistas a obter seus dados bancários e principalmente as senhas do *internet bank*.

O autor explica que há também a possibilidade de o bandido cibernético usar o *e-mail* ou a rede social de uma pessoa do ciclo de amizades do usuário para facilitar a instalação do vírus. Ocorre, por exemplo:

> […], No e-mail enviado por um amigo que diz “veja nossas fotos do final de semana”. **Obviamente que, se você não estava com esse amigo no final de semana, a informação vai soar estranha. Porém, são nas coincidências que se conseguem os melhores resultados nas ações criminosas**. (BRITO, 2013, p. 87-88, grifo nosso).
> […],
> Com a popularização das **redes sociais**, estão comuns as ocorrências de **futo de *perfis***, que seria como a identidade do usuário dentro daquele *site*. **Obtidos os dados de acesso, a pessoa entra na página pessoal e imediatamente troca a senha para que a vítima não tenha mais acesso**. A partir daí passa a utilizar aquele espaço para **publicar informações ofensivas à honra, causando danos irreparáveis aos ofendidos**. (Ibidem, p. 88, grifo nosso).

Auriney Brito leciona que além das formas diretas de propagação do vírus, existe a forma indireta que ocorre quando o agente deixa suas *iscas* espalhadas em computadores públicos:

> Como no relato de um caso em que **a vítima encontrou um *pen drive* em uma *Lan House* e, ao abrir, viu que continha algumas fotos e vídeos sensuais**. Resolveu levar para sua residência e mostrar para outros amigos compartilhando o que eles consideravam divertido, **mas, que, na verdade, nada mais era que a isca deixada por alguém para disseminar o vírus que lá continha**. (BRITO, 2013, p. 88, grifo nosso).

Ademais, Brito (2013) explana outra prática – mais comum do que parece ser – o chamado *fake love*, ou falso amor, em que mulheres usam a *internet* para encontrar parceiros dispostos a ter um relacionamento amoroso e acabam vítimas de um golpe:

> Na rede muitos criminosos criam perfis em *sites* de relacionamentos apresentando-se como médicos, psicólogos, advogados, **e buscam**

> **seduzir mulheres carentes que procuram um amor, até que estas estejam dispostas a exibir seus corpos através da *webcam***. A partir daí, com as imagens gravadas, os criminosos revelam suas verdadeiras identidades e **passam a exigir vantagens econômicas das apaixonadas, sob pena de veiculação das imagens por toda a internet**. Os homens também são constantemente vitimados nessas situações. (BRITO, 2013, p. 88, grifo nosso).

Destarte, Auriney Brito (2013) elucida que quanto mais os usuários evitarem os famosos “CLIQUE AQUI”, mais eles terão preservado o seu sistema pessoal contra instalações de programas maliciosos, pois são inúmeras as técnicas para invasão de um sistema informático. O autor alerta ainda, que jamais devem ficar armazenados em computadores de uso coletivo: dados pessoais, imagens, vídeos e documentos sigilosos. Quanto aos relacionamentos, é necessário que as pessoas reforcem os cuidados básicos de confiabilidade *via web* sob todas as formas de contato, principalmente no tocante às investidas no mundo cibernético, sob pena de viver o drama sofrido por muitas pessoas.

Auriney Brito (2013, p. 89) conclui que “a maioria dos crimes praticados pela internet só alcança a consumação em razão da ajuda dada pela vítima”.

Nesse diapasão, Spencer (2013, p. 287) leciona “que a vítima pode ser vista: como uma potencial incentivadora da delinquência por falta de deveres de cuidado, falta de conscientização e até mesmo por falta de compreensão”.

O autor propõe que os usuários passem a ter um verdadeiro dever de agir no momento em que se conectam à rede, uma vez que com o enraizamento dessa cultura na sociedade, os delitos informáticos aumentam significativamente - sendo a vítima determinante para o sucesso ou não do vitimizador - ou seja, cada uma deve assumir o grau de responsabilidade para a preservação e segurança de seus bens particulares e disponíveis.

Por outro lado, Spencer ressalta que há usuários informáticos, que devem ser observados de forma diferente, tendo em vista que certos delitos são explorados por falhas ímpares:

> Isso se dá pelo fato de que a esfera de navegação é desconhecida em seu potencial mutável e por conta de a janela representada pela tela (do celular, do monitor, do notebook ou qualquer outra) exibir apenas a representação audiovisual inteligível para o usuário leigo, que em verdade não compreende a complexidade do processamento de dados. (SPENCER, 2013, p. 258).

Existe ainda o caso do usuário, cuja cautela ao seu bem jurídico não lhe interessa, seja por renunciar, seja por ele mesmo colocá-lo em risco.

Desta feita, o autor questiona: até que ponto pode-se atribuir à falta de precaução de uma vítima a uma consequência, ou até que ponto uma omissão informática pode ser irresponsável? Razão pela qual Spencer (2013, p. 267) explana: “A criação de princípio vitimológico de autorresponsabilidade da vítima é uma forma de reduzir-se a desproporcionalidade da aplicação da lei penal, criando obrigações e mantendo a ideal subsidiariedade da ciência penal”.

Noutro viés, Marcela Buscato (2012, p. 84-88, grifo nosso) aponta 06 (seis) dicas e suas respectivas soluções, para que os usuários possam proteger sua intimidade na rede, senão vejamos:

Tabela 2 - Dicas e soluções para a proteção da intimidade dos usuários na rede

Dica	Solução
1ª) Previna-se contra invasão de *hackers*	**Mantenha o sistema do computador atualizado**. As correções enviadas pelas empresas de *software* evitam o ataque de *hackers*. Por esse motivo, use sempre programas originais. Os piratas não recebem as atualizações. **Evite arquivos de procedência duvidosa**: se não conhece o remetente ou desconfia do arquivo, não acesse. **Tenha um antivírus** para destruir *softwares* daninhos.
2ª) Cuide dos arquivos armazenados no computador	Se você quer impedir que *hackers* acessem algum conteúdo íntimo, deve **armazená-lo numa mídia externa**, como *HD´s*, *pendrives* ou *CD-ROMs*. Lembre que alguns programas podem recuperar informações deletadas. Uma maneira de evitar a exposição é **usar criptografia**, para embaralhar informações e apresentá-las de outro jeito, ilegível para quem acessá-las.
3ª) Crie senhas difíceis	A senha dos *e-mails* **deve ser complicada até mesmo para o dono** (se for preciso, anote suas senhas num arquivo de texto e o proteja com criptografia). **Tenha cuidado com as “perguntas secretas**” – usadas pelos provedores para a recuperação de senhas. As respostas, nome do

Dica	Solução
	bicho de estimação, escola em que estudou podem estar em seu perfil numa rede social. **Use senha no celular**.
4ª) Aceite os limites (invisíveis) da privacidade virtual	Se você não quer que alguém veja alguma foto, vídeo ou informação pessoal, **não publique em nenhuma rede social**. Mesmo que seus dados só estejam disponíveis a quem você autoriza, eles podem ser repassados por essa pessoa para outras. Não se engane: **você não tem controle sobre sua exposição quando sua intimidade está *online***.
5ª) Para Pensar	A invasão de privacidade **não ocorre apenas com gente famosa e descuidada**.
6ª) Para Agir	É necessário **proteger as imagens produzidas na intimidade**.

Ressalte-se que embora existam usuários que provocam o cometimento de delitos cibernéticos de forma consciente, há outros que acreditam estar seguros e por descuido acabam sendo vítimas da ação de criminosos. Por fim, há os leigos que precisam de orientação para conseguir preservar seus dados com segurança. Nesse contexto, Patricia Peck Pinheiro (2013, p. 320) elucida “Temos que pegar a quadrilha que envia *e-mail* falso e não o inocente que passa para frente um *e-mail* falso sem saber que está mandando vírus para outra pessoa”.

Desta feita, todos os lesados tem direito à tutela do Estado no tocante à justa punição aos que invadem seus dispositivos informáticos e violam sua intimidade e vida privada.

5.5. RESPONSABILIZAÇÃO PENAL DAS PESSOAS JURÍDICAS PROVEDORAS DE ACESSO E CONTEÚDO

Segundo Auriney Brito (2013) há uma resistência no Brasil para a responsabilização penal do provedor de acesso, inclusive, os argumentos jurídicos que são ofertados para sua impossibilidade são muito fortes.

Sobre o tema, colaciona-se o entendimento do ilustre Professor Augusto Rosssini:

> Há necessidade de se quebrar paradigmas até então arraigados, dentre eles a capacidade de a empresa delinquir, de encontrar sua vontade (corolário inquestionável de que há consciência do ente moral e consequentemente sua imputabilidade), elemento autorizador da repressão penal, independente da administrativa ou civil. (ROSSINI, 2004, p. 83).

Nesse diapasão, Auriney Brito acredita que é importante trazer à baila a recomendação do artigo 12 da Convenção de Budapeste, o qual preconiza a responsabilização penal dos provedores de acesso:

> **Art. 12 – Responsabilidade de pessoas Colectivas**
> 1. Cada parte adotará as medidas legislativas e outras que se revelem necessárias para assegurar que as pessoas colectivas possam ser consideradas responsáveis por infracções estabelecidas de acordo com a presente Convenção, quando cometidas em seu benefício por uma pessoa singular agindo quer individualmente, quer como membro de um órgão da pessoa colectiva que exerça no seu seio uma posição de direcção, com base no seguinte:
> a) Poder de representação da pessoa colectiva;
> b) Autoridade para tomar decisões em nome da pessoa colectiva;
> 2. Além dos casos já previstos no n. 1 deste artigo, cada parte adoptará as medidas necessárias para assegurar que uma pessoa colectiva possa ser considerada responsável **quando a ausência de supervisão ou de controlo por parte de uma pessoa singular, mencionada no n. 1 tornou possível a prática de infracções previstas na presente Convenção, em benefício da referida pessoa colectiva por uma pessoa singular agindo sob a sua autoridade.**
> 3. De acordo com os princípios jurídicos da Parte, a responsabilidade de uma pessoa colectiva pode ser criminal, civil ou administrativa.
> 4. Essa responsabilidade deve ser determinada sem prejuízo da responsabilidade criminal das pessoas singulares que cometeram a infracção. (BRITO, 2013, p. 101-102, grifo nosso).

O autor explana que há uma limitação constitucional no que tange a responsabilização dos provedores, pois os arts. 173, §5º e 225, §3º da CF/88, preveem hipóteses taxativas de responsabilização, limitando-se a crimes contra a ordem econômica e financeira, contra a economia popular – nesses casos ainda

discutíveis – modalidades de delitos informáticos impróprios – mas que a eles estão limitados.

No entanto, Brito (2013) afirma que é de absoluta necessidade a atuação dos órgãos estatais e das empresas, uma vez que os delitos cibernéticos são da de espécie de infrações que deixam vestígios, e são os provedores, em especial os de acesso e armazenamento, que possuem as informações privilegiadas e necessárias sobre os rastros deixados pelos criminosos e seus comparsas, razão pela qual apresenta duas alternativas que podem ajudar na solução do problema:

> A criação de medidas de responsabilização pela omissão nos casos em que poderiam evitar os delitos cibernéticos e de medidas que forcem a contribuição com as investigações são imprescindíveis para o sucesso da repressão desses crimes. No entanto, para o primeiro caso faz-se necessária a edição de emenda constitucional para incluir os delitos cibernéticos no rol dos crimes passíveis de responsabilização das pessoas jurídicas.
> Outra alternativa é a recepção da Convenção de Budapeste, nos termos do art. 5º, §3º, da CF/88. Como ela versa, sem dúvida alguma, sobre matéria de direitos humanos – a segurança informática -, sendo aprovada com quórum exigido poderíamos utilizar seus dispositivos que regulam a matéria. (BRITO, 2013, p. 102-103).

Como já foi afirmado por Brito (2013, p. 103), nossa Constituição possui o que a doutrina chama de cláusula aberta em seu art. 5º, §2º, em que relata: "*Os direitos e garantias expressos nesta constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte".*

Mesmo assim, somente esse dispositivo não seria suficiente para cogitarmos a possibilidade de responsabilidade penal do provedor de acesso, se não fosse, dentre as inovações trazidas pela Emenda Constitucional n. 45, a possibilidade de os tratados internacionais de direitos humanos ingressarem na ordem jurídica interna com *status* de norma constitucional, com a seguinte dicção do introduzido §3º:

> Os tratados e convenções internacionais sobre direitos humanos que forem aprovados, em cada Casa do Congresso Nacional, em dois turnos, por três quintos, dos votos dos respectivos membros, serão equivalentes às emendas constitucionais. (BRITO, 2013, p. 103).

Com efeito, o autor afirma que devido a Convenção de Budapeste tratar de matéria de direitos humanos sobre o Cibercrime, ter-se-á um permissivo constitucional para a criação de lei específica para a responsabilização penal dos entes morais denominados provedores. Da mesma forma, considerando-se a

proteção de sistemas de computador ou da informação em meios eletrônicos como um direito fundamental, com esteio no §2º do art. 5º da CF, ter-se-á a responsabilização penal como forma de garantia a esse direito, qual seja, um ambiente virtual seguro e com dignidade.

Num segundo raciocínio, e com o escopo de determinar a imprescindível colaboração dos provedores, Auriney Brito elucida (2013, p. 104) que "o magistrado pode se valer de seu poder geral de cautela, visando garantir a integridade dos rastros eletrônicos – sempre deixados pelos criminosos -, caracterizados principalmente por sua volatilidade". Desta feita, sem qualquer alteração legislativa, resta autorizado o uso dessas medidas quando existir fundada suspeita da ocorrência de um delito cibernético (*fumus comissi delicti*) em razão da perenidade dessas provas (*periculum in mora*).

Nesse contexto Gustavo Artese (2013) expõe uma decisão na esfera jurisprudencial sobre a responsabilidade dos provedores de aplicações:

> […], Em 23 de agosto de 2011, decidiu a Terceira Turma do Superior Tribunal de Justiça, ao julgar o Recurso Especial nº 1.186.616-MG (Dje 31.08.11), em acórdão relatado pela Ministra Nancy Andrighi e que, por sua extensão e amplitude, tende a orientar novos julgados a respeito do tema, que "os provedores de aplicações: (i) não respondem objetivamente pela inserção no *site*, por terceiros, de informações ilegais; (ii) não podem ser obrigados a exercer um controle prévio de conteúdo das informações postadas no *site* por usuários; (iii) devem, assim que tiverem conhecimento inequívoco da existência de dados ilegais no *site*, removê-los imediatamente, sob pena de responderem pelos danos respectivos; (iv) devem manter um sistema minimamente eficaz de identificação de seus usuários, cuja efetividade será avaliada caso a caso". (ARTESE, 2013, p. 30).

Gustavo Artese (2013) elucida que a referida decisão teve o mérito de sedimentar, de forma muito bem fundamentada o que era consenso entre especialistas, muito embora não seja pioneira. No entanto, a polêmica persiste, quanto ao item que diz respeito à possibilidade de responsabilização dos provedores de aplicações no caso de recusa na remoção de conteúdo de terceiros.

O autor explana que a posição do STJ carrega consigo notável afinidade com o sistema estadunidense do *notice and takedown* – o qual permite a remoção automática do conteúdo da internet sem qualquer intervenção judicial. Neste, o provedor não é, *a priori*, responsável pelo conteúdo ilícito. Passará a ser passível de responsabilização, na hipótese em que foi notificado de sua existência e optou por não retirá-lo do ar. Há que se falar, no caso do direito autoral, em que as

infrações ao direito do autor e conexos, serão retiradas imediatamente – sem intervenção judicial, tratamento específico conquistado devido a pressão da indústria de mídia.

Nesta oportunidade, o autor leciona que a proposta do Marco Civil da Internet, aloca as responsabilidades do provedor de modo diferente, onde somente se efetivará a responsabilização civil por danos, no caso em que o provedor se recuse a cumprir ordem judicial que especificamente determina a retirada/derrubada do conteúdo (*takedown*).

Para melhor colacionar esse entendimento, é mister trazer à baila o disposto nos artigos 19 e 20 da já promulgada Lei 12.965 de 23 de abril de 2014, também conhecida Marco Civil da Internet:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, **o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente**, ressalvadas as disposições legais em contrário.
> […],
> Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, **caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário**. (Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 28 abr 2014, grifo nosso).

.

Gustavo Artese (2013, p. 30) relata que cada uma das abordagens traz em si vantagens e desvantagens, pois: “Se, por um lado, o *notice and takedown* tira proveito dos benefícios da autorregulamentação, por outro – e a experiência americana comprova esta hipótese – dá margem ao exercício abusivo do direito de notificar”.

Destarte, o autor conclui *no notice and takedown*, ao se punir a opção de manter o conteúdo potencialmente lesivo com eventual responsabilização, cria-se para o provedor o incentivo de realizar o *takedown*, independente da notificação, pois: entre correr o risco de prever mal os rumos de eventual decisão judicial na qual será o corresponsável, o provedor optará, invariavelmente, por realizar o *takedown* preventivo, para fugir do risco da responsabilização.

5.6. ADESÃO A TRATADOS E CONVEÇÕES INTERNACIONAIS COM VISTAS À UNIFORMIZAÇÃO DA LEGISLAÇÃO PENAL PARA DELITOS CIBERNÉTICOS

Em meio a uma gama de crimes cibernéticos que ultrapassam as fronteiras nacionais, Patricia Peck Pinheiro (2010) faz várias indagações: Será que a sociedade digital caminha no sentido de se criar um ordenamento jurídico global? Como tratar as situações de obrigações ou mesmo de ilícitos ocorridos nos meios eletrônicos e que envolvam múltiplos países ou ordenamentos jurídicos? Seria possível assinar uma carta de princípios gerais, aplicável a qualquer um e em qualquer lugar, que pudesse contribuir e facilitar o tratamento das questões digitais, aumentando o grau de segurança jurídica das relações eletrônicas?

A autora explana que não há como garantir o devido processo legal nem o exercício dos direitos individuais sem que se aceite e compreenda que vivemos em um mundo plano – sem fronteiras – considerando que todas as possibilidades foram abertas com o advento da internet e, mais recentemente, com as redes sociais. Razão pela qual muitos crimes digitais ficam sem solução, pois:

> Muitos crimes digitais ficam sem solução por envolver países distintos daqueles onde se localizam as vítimas, **o que dificulta as investigações e aumenta sobremaneira o tempo de uma ação judicial**. Ocorre que o fator tempo é crucial na sociedade que vive em tempo real! **A demora gera perda das provas, bem como desestimula o cidadão a socorrer-se do Judiciário**. (PINHEIRO, 2010, p. 47, grifo nosso).

Patricia (2010) alerta que nas próximas reuniões relacionadas à sustentabilidade da internet, há que se assumir a necessidade de criação de uma corte internacional para o julgamento de ilícitos digitais, a qual seja regida pelos princípios do acesso e da celeridade, bem como se utilize dos recursos da mediação ou arbitragem para decidir os casos submetidos à apreciação, com base em um direito inspirado nos princípios do Direito Digital Global, dentre os quais destacam-se: Princípio da Transparência, Princípio do Uso Ético da Tecnologia, Princípio do a Ninguém Lesar, Princípio da Proteção da Privacidade dos Indivíduos e dos seus Dados, Princípio da Proteção da Imagem e da Reputação, Princípio da Segurança da Informação (disponibilidade, autenticidade, integridade, confidencialidade, legalidade), Princípio da Cooperação Internacional para Investigação de Casos Digitais e outros.

Desta feita, o referido direito digital supranacional não retiraria a soberania dos Estados, pelo contrário:

> […], Seria a única forma de garantir a aplicação da justiça na era das fronteiras da informação, em que o espaço e tempo foram relativizados. Nesse sentido**, se os Estados não encontrarem uma solução viável para os conflitos da era digital, corremos o risco de voltar ao estado de natureza, a se "fazer justiça com o próprio *mouse***". (PINHEIRO, 2010, p. 47, grifo nosso).

No mais, Auriney Brito (2013) evidencia que o único instrumento internacional multilateral referente à legislação sobre Cibercrimes é a Convenção de Budapeste, a qual recomenda aos Estados signatários a criação ou adaptação de seus respectivos arcabouços legislativos de modo que tornem-se uniforme, com vistas a não existir falhas decorrentes da transindividualidade global dos atos praticados no ciberespaço, pois só com a cooperação, a criminalidade digital será combatida. Assim:

> Corolário inequívoco de que os tradicionais aspectos relacionados ao exercício da soberania desses mesmos países também merecem reformulação, em evidente decorrência de que a criminalidade informática é também globalizada, da mesma forma com a economia, a cultura etc., sem descurar da necessidade de a iniciativa privada, em todos os seus níveis, cooperar efetivamente no contexto, sem o que a efetividade de combate não ocorrerá. A título de exemplo, espera-se que os provedores de acesso tenham o compromisso de colaborar com os órgãos de persecução, sem o que, repita-se, não haverá eficiência no combate a esse tipo de criminalidade. (BRITO, 2013, p. 50).

Auriney Brito (2013) afirma que a Segurança Informática é um bem jurídico permanente e autônomo a ser protegido pelo Direito Penal, pois sempre existirá quando se tratar de conduta praticada no ambiente virtual, por isso é importante que os países façam adesão a Convenção que busca tipificar cada uma das condutas possíveis de serem praticadas na rede, quer comissiva, quer omissivamente, de maneira que o trato seja uniforme para aniquilar a criminalização cibernética, bem como punir de forma justa os que se voltam contra os direitos protegidos pelos tipos penais:

> Convencidos de que a presente Convenção é necessária para prevenir ações diretas contra a **confidencialidade**, a **integridade** e a **disponibilidade** de sistemas de computador, redes e dados de computador, assim como a má utilização desses, provendo a criminalização de cada conduta, conforme descrito nessa convenção, e a **adoção de poderes suficientes para combater efetivamente cada ofensa criminal**, atuando na detecção, na investigação e na perseguição de cada ofensa criminal, **tanto no nível nacional quanto internacional, e proporcionando um planejamento para**

> **uma cooperação internacional rápida e eficaz**. (BRITO, 2013, p. 51, grifo nosso).

O autor expõe ainda que a Convenção de Budapeste prestigia o Princípio da Proporcionalidade, uma vez que utiliza o termo equilíbrio de forma que os meios não justifiquem os fins, reafirmando que, ao perseguir condutas criminosas, o operador do Direito (delegado, promotor de justiça, juiz etc.), mesmo imbuído dos mais legítimos interesses, nunca, absolutamente nunca, deve desrespeitar os direitos humanos aplicáveis tais quais: o direito individual de manter opiniões sem interferências, o direito à liberdade de expressão, incluindo a liberdade de busca, recebimento e transmissão de informações e ideias de todos os tipos, sem se preocupar com fronteiras e os direitos relativos ao respeito à privacidade.

Nesse contexto, Auriney Brito (2013) destaca que a pressão internacional para que o Brasil assine a Convenção é muito grande, motivo pelo qual o Poder Legislativo, vem unindo forças para efetuar as modificações pertinentes junto ao Código Penal e legislação especial.

Por fim, Patricia Peck Pinheiro (2013) elucida que devemos acompanhar atentamente todos os projetos e tratados para Internet, sobretudo o de delitos informáticos para juntos quebramos os paradigmas, uma vez que legislar sobre estes novos temas não é fácil – há desafios para serem vencidos – de modo que, não há lei perfeita, mas lei necessária.

CONCLUSÃO

Diante do exposto, reitera-se que à intimidade, à vida privada, à honra e a imagem das pessoas são direitos fundamentais invioláveis, razão pela qual são tutelados pela Constituição Federal. Neste sentido, uma vez ofendidos merecem indenização pelo dano causado e justa punição pelo Estado. Dentre todos, a privacidade é o bem da vida mais caro ao ser humano, uma vez que, sem ela, o homem expõe-se de modo a violar a sua própria personalidade.

Os avanços tecnológicos, sobretudo da internet e demais meios eletrônicos, desempenharam papel fundamental para o crescimento da sociedade digital. No entanto, desencadearam riscos, incertezas e a prática de crimes ofensivos aos direitos fundamentais, razão pela qual fez surgir o novo bem jurídico a ser a tutelado denominado “segurança da informação”. Este bem dividiu a opinião dos doutrinadores: se seria a hipótese de deslocar o direito penal do ramo do ordenamento jurídico do caráter de *ultima ratio* do controle social, para desafiá-lo a acompanhar a evolução da sociedade. Há que se falar que o Direito Penal Clássico, elucida que só haverá crime se houver lesão ou ameaça concreta de lesão ao bem jurídico protegido (princípio da lesividade), mas há que considerar que em alguns casos, a atuação do Direito Penal com antecipação de tutela faz-se necessária, devido a característica do contexto social, sendo muito mais forte que qualquer paradigma antiquadro. Assim, torna-se mais razoável pensar na possibilidade de relativização de alguns princípios constitucionais do Direito Penal Clássico - em especial o da lesividade - para garantir que o Direito Penal atual seja o instrumento legítimo para a proteção de bens jurídicos supraindividuais na sociedade da informação, respeitando sobretudo a subsidiariedade, a fragmentalidade e a legalidade.

A Lei Carolina Dieckmann foi um marco importante para a sociedade digital, adentrou no ordenamento jurídico com a dura missão de combater a atuação de mentes perversas capazes de invadir os dispositivos informáticos alheios, interromper serviços telemáticos ou de utilidade pública e até mesmo falsificar cartões de crédito e débito, ou seja, evitar a impunidade dos crimes cibernéticos. A intenção foi muito boa, mas deixou a desejar.

Em linhas gerais foram identificadas mais lacunas que avanços, pois os textos ambíguos e lacunosos trouxeram divergências entre juristas e doutrinadores, como por exemplo sobre o termo “invasão”: se o dispositivo estiver completamente desprotegido, não há que se falar em punição pelo crime de invasão, uma vez que não está presente a violação indevida do mecanismo de segurança. É relevante o posicionamento de Wanderlei José (2013) ao dizer que legislador pecou na qualidade técnica do artigo 154-A, onde solução legal seria substituir o verbo “invadir” por “acessar”, uma vez que o agente não opera com violência, mas tão somente com o emprego de ardil para a obtenção de dados, ou seja, na prática o *modus operandi* não se coaduna com a maior parte dos delitos cibernéticos, nos quais o agente se utiliza da estratagema para enganar e alcançar o seu desiderato criminoso. Outra divergência se deu pelo verbo “obter” quanto a mera espiadinha, segundo Renato Opice Blum (2012) a lei já nasce com brecha, pois não prevê punição para alguém que invade o computador e não rouba nada - o faz apenas por curiosidade - ou tenta invadi-lo mas não consegue.

O maior questionamento se deu em virtude das penas atribuídas aos delitos informáticos para a proteção da intimidade, pois foram consideradas insignificantes - uma verdadeira ciranda despenalizante - pois: a pena máxima cominada em 1 (um) ano, arrasta o crime para o rito sumaríssimo dos Juizados Especiais, onde se estimulará a conciliação, a composição civil dos danos e a transação penal, além disso, se o réu for primário, penas inferiores a quatro anos podem ser convertidas, por exemplo, à prestação de serviços à comunidade. Ou seja, ninguém vai para a cadeia por esse crime. A depender do caso delinquir pode compensar, pois tem muito computador por aí com informações bem mais valiosas que uma cesta básica. Ademais as penas por serem pequenas prescrevem rapidamente, inviabilizando a punição.

Os ataques de negação de serviço feitos a particulares ficaram órfãos no diploma e comprometeram a credibilidade, pois a lei só fala em serviços públicos, cabendo ao agente que comete o crime de interrupção ou perturbação nas organizações privadas, o crime de dano, com pena de 1(um) a 6 (seis) meses. Pena ainda mais branda que na Lei 12.737/12, a qual seria de 1 (um) a 3 (três) anos.

O Brasil ainda carece de um corpo representativo de profissionais treinados para lidar com delitos informáticos, embora já conte com alguns profissionais. Hoje, por exemplo, leva-se em média 03 (três) meses para se registrar

um boletim de ocorrência. A lei tem penas pequenas, assim os crimes vão prescrever rapidamente e não haverá nada mais a fazer para punir os infratores que em poucos minutos, destroem reputações ou revelam dados sigilosos de uma empresa.

O fato de as fotos da atriz Carolina Dieckmann ainda serem acessíveis a qualquer usuário disposto a fazer uma breve pesquisa na rede revela o nível de complexidade jurídica que envolve o ambiente virtual e a fragilidade para retirada de conteúdo da Internet, uma vez que a maioria dos *crackers* utilizam servidores hospedados fora do Brasil. Noutro viés é ainda mais assustadora a utilização da *Deep Web* (*internet* invisível) a qual não tem como identificar o infrator.

A Lei Dieckmann precisará de jurisprudência e leis complementares para funcionar plenamente devido ao seu texto ambíguo e lacunoso.

Por fim, o diploma legal gerou um conflito de competência nas esferas civil e penal, pois embora muitos crimes estejam tipificados no Código Penal (Calúnia - art. 138, Injúria - art. 140 e Difamação - art. 139), quando tratados no campo digital, como *Cyberbullying*, são julgados na área cível. Nesse sentido, o jurista Luiz Flávio Gomes (2013) alega a Lei Carolina Dieckmann não vai surtir efeitos práticos visto que a justa punição para situações oriundas do meio eletrônico, configura-se na apuração das responsabilidades do sujeito, bem como na aplicação de indenização contundente, capaz de aniquilá-lo economicamente.

Melhor assiste a opinião dos doutrinadores que acatam a esfera penal como detentora do direito de punir, pois tratam-se de delitos transacionais em que ação de um pode atingir e gerar consequências e riscos sistêmicos a todos, além de trazer danos irreparáveis para as vítimas, tais como a perda do trabalho, rejeição da sociedade, depressão e morte. Tendo em vista que o conteúdo que entra na rede, ainda que falso, dificilmente será apagado.

Nesse diapasão é possível provar que o direito penal funciona para os crimes informáticos, a partir do instante em que a pena é contundente e capaz de inibir a conduta do agente, como no caso da legislação francesa, em que o crime semelhante a instalação de vulnerabilidades para obter vantagem ilícita no Brasil (art. 154-A, segunda final) é punível com 05 (cinco) anos de prisão e multa de R$ 232.500,00 (duzentos e trinta e dois mil e quinhentos reais), bem diferente da legislação brasileira em que a pena é de 03 (três) meses a 01 (um) ano com multa a definir pelo juiz.

Desta feita, propõe-se cotejar a legislação pátria, com a legislação alienígena bem como tratados e convenções internacionais - a exemplo da Convenção de Budapeste - com vistas ao combate aos crimes cibernéticos a nível mundial. Há que se pontuar que o Brasil já possui boa parte das condutas compatíveis com a referida convenção, mais ainda é preciso quebrar os paradigmas, uma vez que legislar sobre estes novos temas não é fácil – há desafios para serem vencidos – de modo que, não há lei perfeita, mas lei necessária.

Ademais, o direito digital obriga toda corte que atua no processo judiciário: juízes, procuradores, advogados, delegados, investigadores, peritos e demais, a realizar uma atualização tecnológica. Tal postura é necessária para que se atinja uma sociedade digital segura; do contrário, o ordenamento jurídico restará prejudicado e colocará a sociedade em risco.

Para os usuários é preciso atentar-se pois o mundo digital é acessível e a internet, um território aberto e incontrolável, onde tudo o que postamos no computador é passível de ser visto por todos. Por isso, é necessário ter cuidado para não expor sua intimidade e vida privada na rede, para não ser a próxima vítima dos delitos informáticos. Desta feita, evitem o “clique aqui”, façam a manutenção preventiva de seus dispositivos informáticos e sobretudo, controlem suas atitudes.

Elucida-se que este trabalho não tem a pretensão de esgotar o assunto proposto, pelo contrário, visa despertar o interesse da sociedade e da corte legislativa para garantir uma qualidade de vida *on-line* segura; uma vez que a privacidade - bem maior do indivíduo - merece proteção e justa punição por parte do Estado.

REFERÊNCIAS

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

ARTESE, Gustavo. **As trancas da lei da internet**. In: Revista Jurídica Consulex, v. 17, n. 405, p.29-31, dez./2013.

ATHENIENSE, Alexandre. **Ataques de hackers e insegurança jurídica**. In: Revista Jurídica Consulex, v. 15, n. 348, p.14-15, jul./2011.

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

BLUM, Renato Opice. **A lei da bela contra o crime**. In: Veja, ed. 2295, v. 45, n. 46, p.110, nov./2012.

BRASIL. **Constituição Federal, out. 1988**. Diponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>. Acesso em 29 mar 2014.

_____.**Código Penal, dez. 1940**. Diponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 21 abr 2014.

_____. **Cotação do Euro**. Disponível em: <http://www.wap.economia.uol.com.br/cotacoes>. Acesso em 26 abr 2014.

_____. **Lei 12.737, nov. 2012**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 18 abr 2014.

_____. **Lei 12.935, abr. 2014**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 28 abr 2014.

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

BRENNER, Susan W. ***Cybercrime: re – thinking crime control strategies.*** *In: Crime online*. Willian *Publishing*, Devon, 2007.

BRESSAN, Hélio; CARVALHO, Caio César; CRESPO, Marcelo; MANZONI, Marcos e TAVARES, Thiago. **Banditismo em Rede: Nova Legislação do país sobre crimes cibernéticos traz avanços, mas estabelece penas brandas e deixa lacunas em meio à variedade de delitos cometidos na *Web***. In: Rev. Imprensa Jornalismo e Comunicação, v. 4, n. 286, p. 58-61, jan./fev. 2013. Reportagem concedida a Guilherme Sardas.

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

BUSCATO, Marcela. Et al. **Liberdade Vigiada**. In: Revista Época, n. 730, p. 82-88, 14 maio 2012.

CANOTILHO, J.J. Gomes. et al. **Comentários à Constituição do Brasil**. - São Paulo: Saraiva/Almedina, 2013.

CANOTILHO, Joaquim José Gomes. **Direito constitucional e teoria da constituição**. Coimbra:Almedina, 2003.

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

COSTA JÚNIOR, Paulo José da. **O direito de estar só**. São Paulo: Revista dos Tribunais, 1995.

DONEDA, Danilo. **A proteção de dados pessoais como direito fundamental**. Revista Espaço Jurídico 12/103. Joaçaba: Unoesc, 2011.

ESTRADA, Manuel Martin Pino. **Os crimes informáticos na internet profunda ou *Deep Web*.** In: Revista Jurídica Consulex, v. 17, n. 405, p.36-40, 1º dez./2013.

FERRARI, Eduardo Reale. **Direito penal contemporâneo: direito penal do consumidor e a tutela de bens jurídicos supraindividuais: uma análise constitucional**. São Paulo: Revista dos Tribunais, 2007.

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

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

GOMES, Luiz Flávio. **V Congresso de Crimes Eletrônicos, realizado nos dias 12 e 13 de agosto pela Fecomercio SP**. Disponível em <http://atualidadesdodireito.com.br/lfg/2013/08/14/jurista-luiz-flavio-gomes-fala-sobre-a-lei-carolina-dieckmann> Acesso em 19 abr 2014.

_____. Direito penal: **introdução e princípios fundamentais**. São Paulo: Revista dos Tribunais, 2007.

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.

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

HOUAISS, Antônio; VILLAR, Mauro de Salles. **Dicionário Houaiss da língua portuguesa**, elaborado pelo Instituto Antônio Houaiss de Lexicografia e Banco de Dados da Língua Portuguesa S/C Ltda. 1.ed. - Rio de Janeiro: Objetiva, 2009.

JORGE, Higor Vinicius Nogueira. **Vulnerabilidades da Rede x Segurança da Informação**. In: Revista Jurídica Consulex, v. 15, n. 349, p. 6-9, ago./2011.

_____. ***Cyberbulling* e Crimes Cibernéticos**. In: COAD Informativo, n. 27, p.443-446, jul./. 2011

KAYSER, Pierre. ***La protecion de la vie privée***, Paris: Econômica, 1984.

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

LÓPEZ DIAS, Claudia (tradutora): ***"Código Penal Alemán (STGB), de 15 del 15 de mayo de 1871, com la sexta reforma del Derecho penal del 26 de enero de 1998"***, Universidad Externado de Colombia, 1. Edicíon, Columbia, 1999).

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

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

MORAES, Alexandre de. **Constituição do Brasil interpretada e legislação constitucional**. 7.ed. atualizada até a EC n.º 55/07 – São Paulo: Atlas, 2007.

MOREIRA, Rômulo de Andrade. **A nova lei sobre a tipificação de delitos informáticos: até que enfim um diploma legal necessário**. In: Revista Jurídica, v.61, n. 423, p. 89-103, jan./2013

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

_____. **Código penal comentado.** 13. ed. rev. atual e ampl. – São Paulo: Ed. Revista dos Tribunais, 2013.

PAESANI, Liliana Minardi. et al. **A evolução do direito digital: sistemas inteligentes, a Lei nº 12.737/2012 e a privacidade**. In: PAESANI, Liliana Minardi (Coord). O direito na sociedade da informação III. São Paulo: Ed. Atlas, 2013.

PENIDO, Flávia. **Os crimes previstos na Lei Dieckmann**. In: Informativo Jurídico Consulex, v. 24, n. 17, p.3, abr./2013.

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

_____. **Direito digital**. 5. ed. – São Paulo: Saraiva, 2013.

PRADO, Luiz Regis; CARVALHO, Érika Mendes de; CARVALHO, Gisele Mendes de. **Curso de direito penal brasileiro.** – 13. ed. rev. atual. e ampl. – São Paulo: Ed. Revista dos Tribunais, 2014.

PROSSER, Willian. ***Privacy - a legal analysis, in Philosophical dimentions of privacy***, Cambridge: Schoeman (ed.), 1984.

RADFAHRER, Luli. **Pandemia cibernética**. Jornal Folha de São Paulo. Caderno TEC, 25 fev. 2013.

REINDENBERG, J. (2004). ***States and internet enforcement. University of Ottawa Law and Technology journal***, 1 (213), apud JEWKES, Yvonne (Ed.). Crime online: Willian Publishing, 2003.

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

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

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

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

SÁNCHEZ, Jesús María Silva. **A expansão do direito penal: aspectos da política criminal nas sociedades pós-industriais**. Trad. Luiz Otávio de Oliveira Rocha. São Paulo: Revista dos Tribunais, 2002.

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.

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

TIEDEMANN, Klaus. ***Poder económico y delito***. Barcelona: Ariel, 1985, p. 124.

VAINZOF, Rony. **Leis dos Crimes Virtuais (Lei Carolina Dieckmann). Análise da Lei nº 12.737/12: Avanços e Lacunas**. In: PAESANI, Liliana Minardi (Coord.). O Direito na Sociedade da Informação III. São Paulo: Ed. Atlas, 2013, p. 27-28.

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

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

_____. **A convenção de Budapeste sobre crimes cibernéticos e o ordenamento jurídico nacional**. In: Revista de Direito de Informática e Telecomunicações - RDIT, Belo Horizonte: Ed. Fórum, v. 4, n. 6, p. 197-232, jan./jun. 2009.

WEST, Alan. ***Privacy and freedom***. New York: Atheneum, 1967.

WRIGHT, Alex. ***Exploring a “deep web” that Google can´t grasp***. Disponível em: <http://www.nytimes.com/2009/02/23/technology/internet/23search.html?th&emc=th&_r=1&>. Acesso em: 17.09.13.