FACULDADE DA CIDADE DE MACEIÓ

BACHARELADO EM DIREITO

PEDRO HENRIQUE SILVA DOS SANTOS

UMA ANÁLISE DA LEI DE CRIMES CIBERNÉTICOS NO ORDENAMENTO JURÍDICO BRASILEIRO

MACEIÓ-AL
2018

PEDRO HENRIQUE SILVA DOS SANTOS

UMA ANÁLISE DA LEI DE CRIMES CIBERNÉTICOS NO ORDENAMENTO JURÍDICO BRASILEIRO

Trabalho de conclusão de curso apresentado à Faculdade da Cidade de Maceió como requisito para obtenção do grau em Bacharel em Direito.

Orientador: Professor Especialista Rodrigo Monteiro de Alcântara.

Coorientadora: Solange Correia Tenório Costa.

Maceió - AL
2018

Ficha Catalográfica

S586i

Santos, Pedro Henrique Silva dos
Uma análise da Lei de Crimes Cibernéticos no ordenamento Jurídico Brasileiro. Pedro Henrique Silva dos Santos. – Maceió, 2018.
43f.

Orientador: Prof. Esp. Rodrigo Monteiro de Alcântara.
Co-orientação: Profa. Solange Correia Tenório Costa.
Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade da Cidade de Maceió - FACIMA, Maceió, 2018.

Bibliografia

1. Dirieto. 2. Globalização. 3. Adaptação. 4. Virtual. 5. Comunicação. I. Alcântara, Rodrigo Monteiro de. II. Costa, Solange Correia Tenório. Faculdade da Cidade de Maceió. Curso de Direito. III. Título

CDU 34

FACIMA
FACULDADE DA CIDADE DE MACEIÓ

RESULTADO FINAL DO TRABALHO DE CURSO

CURSO: Direito

ALUNO(S) ORIENTADO(S): Pedro Henrique Silva dos Santos

TÍTULO DO TRABALHO: Uma análise de lei de crimes Cibernéticos no ordenamento jurídico Brasileiro.

RESULTADO FINAL DO TRABALHO DE CURSO	**Nota**
Professor Orientador: RODRIGO MONTEIRO DE ALCÂNTARA	100
Membro Avaliador Nº 1: ALEXANDRE CÉSAR DOS SANTOS	90
Membro Avaliador Nº 2: MARLUCE FALÃO DE OLIVEIRA	100
MÉDIA FINAL	9,6

ALUNO(S):

PEDRO HENRIQUE SILVA DOS SANTOS

BANCA EXAMINADORA:

RODRIGO MONTEIRO DE ALCÂNTARA
(Orientador(a))

ALEXANDRE CÉSAR DOS SANTOS

MARLUCE FALCÃO DE OLIVEIRA

Maceió, 12 de junho de 2018.

DEDICATÓRIA

Dedico este trabalho aos meus pais, Selma Silva dos Santos e Edval Silva dos Santos, que apesar do começo conturbado, tanto torceram por mim nessa caminhada; minha irmã, Carla Caroline Silva dos Santos, um espelho de entusiasmo e fome pelo saber; e, a meu filho, Gabriel Henrique Dâmaso dos Santos, que, definitivamente e exclusivamente, foi meu maior motivador. Fica aqui registrada minha eterna gratidão pelo apoio em todos os momentos em que suas palavras fizeram meus passos se tornarem mais firmes, em que cada atitude me fez enxergar o quanto é importante tanto para mim, quanto para vocês, a conclusão deste curso, pois me trouxe um sentimento de dever cumprido e a sensação de que, de alguma maneira, a sociedade poderá ter um futuro melhor.

AGRADECIMENTO

A Deus.

EPÍGRAFE

"O criminoso produz uma impressão, que pode ser moral ou trágica; desta forma ele auxilia o movimento dos sentimentos morais e estéticos do público. Além dos manuais de Direito Penal, do Código Penal e dos legisladores, ele produz arte, literatura, romances e mesmo tragédias. O criminoso traz uma diversão à monotonia da vida burguesa; defende-a do marasmo e faz nascer essa tensão inquieta, essa mobilidade do espírito sem a qual o estímulo da concorrência acabaria por embotar. O criminoso dá, pois, novo impulso às forças produtivas…" — Karl Marx (apud Henri Lefebvre. Sociologia de Marx. Rio de Janeiro: Forense, 1968, pp. 79 e 80).

RESUMO

A ciência do Direito está diretamente interligada com a evolução da sociedade e a globalização mundial, a medida que o indivíduo muda em relação a seu comportamento individual, familiar e social, o Direito deve acompanhar essa evolução, pois é na forma em que a sociedade aceita ou não essa alteração comportamental que a base do Direito, estabelecerá limites na aplicação das normas internas e externas. Um marco da globalização mundial é a criação de um dispositivo comunicador que proporciona o compartilhamento de qualquer informação entre duas ou mais pessoas, individualmente ou simultaneamente, seja por voz, texto ou imagem, em qualquer lugar do mundo e a qualquer momento. O trabalho apresentado tem a pretensão de realçar a aplicação da lei federal que promoveu alterações no Código Penal Brasileiro, Decreto-Lei 2.848 de 7 de dezembro de 1940, tipificando os delitos ou crimes informáticos, que tramitou em tempo recorde no Congresso Nacional e as dificuldades em que o mundo jurídico se encontra para se adaptar ao dispositivo, ora mencionado, Internet.

Palavras Chave: Direito. Globalização. Adaptação. Virtual. Comunicação.

ABSTRACT

The science of law is directly intertwined with the evolution of society and global globalization, as the individual changes in relation to his individual, family and social behavior, the law must follow this evolution, since it is in the way society accepts whether or not this behavioral change that the basis of law, will establish limits in the application of internal and external norms. A milestone in global globalization is the creation of a communicating device that provides the sharing of any information between two or more people, individually or simultaneously, either by voice, text or image, anywhere in the world at any time. The paper presented has the pretension to present the difficulties in which the legal world is currently in order to adapt to the aforementioned device, Internet.

Keywords: Law. Globalization. Adaptation. Virtual. Communication.

SUMÁRIO

1. INTRODUÇÃO

O presente trabalho tem o objetivo de apresentar à sociedade a tipicidade criminal anteriormente vista no ordenamento jurídico em analogia as já existentes no Código Penal de 1940. Tendo como base a Constituição Federal, posteriormente o Código Penal Brasileiro e a Lei Federal nº 12.737/2012 que criou a tipificação criminal de delitos informáticos em conjunto com a 12735/2012.

Durante o curso de Direito, especificamente das matérias relacionadas ao Código Penal e Processual Penal, foi constatado o fato da analogia de crimes, principalmente no tocante a crimes de natureza informática, não se enquadrarem em nenhum dos tipos penais previstos no sistema jurídico-penal no Brasil. É imprescindível um estudo voltado não só aos futuros operadores do direito, como também ao público em geral, onde se apresente os elementos básicos na prática, combate, prevenção desse crime e a apresentação dos direitos legais que a sociedade precisa saber quando vítimas de crimes cibernéticos.

Atualmente, talvez por falta de conhecimento, o que é de se abismar nos dias de hoje com tanto meio de comunicação a postos, uma vítima de crime cibernético represente o ofensor, quando lesado e ainda sofra consequências gravíssimas, ficando o criminoso impune e na maioria das vezes oculto na criminalidade para a reiterada prática do ilícito.

Apesar da Lei Federal nº 12.737/2012 está em vigor a mais de cinco anos, não vemos uma aplicação dominante da tão divulgada, elogiada e comemorada norma. Haja vista que é imensurável a quantidade de delitos existentes e possíveis no espaço cibernético, bem como dos danos irreparáveis que podem ser causados a vítima. Percebemos isso, através de pesquisa jurisprudencial nos sites de julgados brasileiros, onde mostra que desde a vigência dos artigos criados, como também dos modificados através da mencionada lei não há uma aplicabilidade destes, considerando o baixo número de julgados.

Por outro lado, no ano de 2015 a 2016 o número médio de ataques cibernéticos revelados pela Pesquisa Global de Segurança a Informação, através de seu site oficial ao todo subiu 38% no mundo e só no Brasil o aumento foi de 274%, dados estes publicados na 18ª Edição anual da PWC, lançada em 2015. “Uma diferença muito relevante”, levando-se em conta que ao passar da “criação” legislativa do crime ter sido relativamente a pouco tempo, deveria haver uma inibição dos infratores em praticar tais ilícitos.

O computador é constituído por uma sequência de circuito interligados e relacionados

que permitem uma imensa variação de dados. É definido como um aparelho eletrônico que tem o poder de receber, processar e transmitir dados, através de operações aritméticas e lógicas, como o próprio nome já diz, em latim, computador significa “calcular”. (Wikipédia 2006).

Virtual é o termo utilizado para aquela pessoa que possui certa virtude, no entanto, a definição que pretendemos obter da palavra Virtual está ligada com aquilo que existe na sua aparência e não na sua existência física e real. Tentando explicar em palavras básicas para o nosso conteúdo, Virtual no mundo da tecnologia são a construção e execução de sistemas em formatos digitais.

Crime ou delito, pode-se entender através do instituto EJAM como uma desobediência a legislação penal atualmente aplicada, ou seja, ato praticado por ser humano, ilícito, punível pelo estado que tende a ser destruidor não apenas para um indivíduo que o pratica, mas também para sociedade e para o estado.

Internet consiste em ser um conjunto de empresas mundiais de computadores e sistemas interligados que permite o acesso simultâneo de informações sobre qualquer coisa e em qualquer lugar do mundo através não só de computadores, mas de outros dispositivos ligados a ele. (Frederico Westphalen, 2014).

A privacidade é um direito fundamental de todo cidadão brasileiro, está disposto dentre outras legislações, na Declaração Universal dos Direitos Humanos das Nações Unidas e pela Constituição Federal do Brasil em seu artigo 5º, incisos X que resguarda a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas e no artigo XII que visa proteger o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, por ordem judicial. A violação da privacidade gera vários transtornos, tais como, constrangimentos políticos e pessoais, discriminação social, econômica, étnica, religiosa, etc. O aumento das informações disponíveis em plataformas digitais e ferramentas de pesquisa nas redes virtuais possibilita imensuráveis modalidades para rastrear, cruzamento e análise de informações, elevando muito os riscos à privacidade, cada vez mais expondo os usuários, o que evidencia a necessidade de legislação específica para a devida garantia do direito fundamental supramencionado na Constituição Federal Brasileira, tratado como cláusula pétrea.

Diante dos vários conceitos dados a Cibernética é possível descrevê-lo como uma ciência de comunicação e de controle que deixa sistemas integrados e lógicos com um controle que regula o seu comportamento, nele compreende-se os processos e sistemas de transformação em sua concretização. Tal ciência que auxilia as demais ciências, baseada na

transferência de informação entre sistema e o meio deste, bem como o controle da função dos sistemas com respeito ao ambiente.

Uma Geografia móvel de informação, geralmente invisível, ciberespaço, foi a nomenclatura adotada por desenvolvedores e facilmente acolhida pelos usuários das redes digitais. Esse moderno espaço de comunicação adequado por uma ligação mundial de computadores e das intermináveis memórias que possuem, assim definiu Lévi. Incluindo aí todos os sistemas de comunicação eletrônica que possam transmitir informações nascidas em meio a fontes digitais ou que posteriormente sejam destinadas à digitalização. Lévi ainda define e persiste no aspecto primordial desse sistema que é a codificação digital, diz que está intrínseca e condicionada: “o caráter plástico, fluido, calculável com precisão e tratável em tempo real, hipertextual, interativo e, resumindo, virtual da informação” (Levi, 1999, p. 92). Este brilhante filósofo francês em uma de suas obras, Cibercultura, nos presenteou com o conceito mais claro e plausível de ciberespaço.

O estudo terá como base a pesquisa na literatura da legislação brasileira vigente, convenções, direito comparado, em julgados dos tribunais comumente conhecidos como jurisprudências, doutrinas, artigos e pesquisas efetuadas em diversos sítios de assuntos correlatos.

2. A HISTÓRIA DOS MEIOS DE INFORMÁTICA

Em tempos atuais o computador é um equipamento eletrônico quase considerado como eletrodoméstico, indispensável na vida cotidiana. Foi durante a II Guerra Mundial que foram criados os primeiros computadores. Cientistas da Marinha americana, em parceria com a Universidade de Harvard, desenvolveu o aparelho que hoje chamamos de computador. Mesmo com a evolução da tecnologia e transformações físicas nos computadores digitais tenham sido drasticamente alteradas pela adaptação aos tempos modernos, quase todos os computadores atuais ainda usam a arquitetura proposta no final da década de 40. O computador foi idealizado com o intuito de resolver problemas matemáticos para o calculo de trajetórias táticas, mas apenas veio a funcionar após o fim da guerra e os crimes os quais estamos estudando apareceram após décadas da existência.(Wikipédia 2013).

Os primeiros crimes virtuais começaram a aparecer no meio jurídico em torno das décadas de 50 e 60, com um novo marco histórico de conflitos, a guerra fria. Como a invenção dos anos 40 estava em pleno funcionando, agregando vantagem aos que possuíam, houve vários atos de sabotagem e espionagem. Já nos anos 70, os especialistas de má-fé, conhecedores do funcionamento das linhas telefônicas existentes, eram capazes de apossar-se das linhas telefônicas e alguns facilmente roubar informações das operadoras telefônicas, mas ao perceber a invasão as empresas mudaram suas formas de abordagens e sistemática. (KING, 2001).

O que hoje forma a Internet que permite o acesso a todo tipo de informações e de transferência de dados, teve início nos anos 70, criada para a guerra por uma subdivisão do Departamento de Defesa dos Estados Unidos, com o objetivo de ter maior segurança no armazenamento de dados, pois ele estaria arquivado em vários lugares do país, caso um viesse a ser danificado com a guerra.(Wikipédia 2013).

Em 1982 foi estabelecido o padrão IP/TCP, até hoje usado na rede, tornando-se obrigatório em 1983 e, somente nesse momento, pôde-se conceituar a Internet como um conjunto de redes interligadas. Com o crescimento da natalidade e a redução no tamanho dos aparelhos, os jovens eram encorajados a desmontá-los, ter conhecimento específico prático do detalhamento do software e hardware, e neste processo de entendimento e aprendizado sobre computadores surge o termo “hacker”. Nessa época, podemos dizer que os curiosos pelos aparelhos e seu funcionamento eram até incentivados, visando o maior conhecimento para futuras espionagens e digamos de maneira racional, se não fossem por eles “hackers” e seus desbravamentos na área tecnológica não haveriam tanta evolução no ramo da computação e

da internet. Foi realmente nos anos 90 que realmente chegamos ao conceito de hackers, como os criminosos da rede virtual, pois com o avanço desordenado do número de usuários de internet e seu alcance privativo, social e econômico, começaram a ocorrer inúmeras invasões a dados alheios, possibilitando aos hackers cometerem crimes no âmbito mundial. (KING, 2001).

3. LEGISLAÇÃO NACIONAL

A legislação penal encontra-se interligada com a internet e a rede de computadores, uma vez que a relação entre duas ou mais pessoas deve ser disciplinada através do Direito, uma vez que haja essa comunicação, as condutas devem ser disciplinadas na sociedade digital. O Código Penal retrata a punição de algumas condutas praticadas a partir do uso da tecnologia nos artigos 154-A e 154-B, porém, a Constituição Federal em seu artigo 5º, XXXIX, como uma garantia fundamental, deixa clara a exigir uma posterior intervenção legislativa com o intuito da elaboração de regras na punição de crimes virtuais, uma vez que no regramento jurídico-constitucional de 1988 não há termos técnicos próprios dos cibercrimes, dando margens a lacunas imensas para impunidade.

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

O que hoje chamamos no Brasil da Lei de Crimes Cibernéticos (Lei nº 12.737/12) passou a vigorar em abril de 2013, tal dispositivo altera o Código Penal para acrescentar na esfera penal crimes cibernéticos, ou seja, crimes que sejam praticados por meio de dispositivo virtual. Um assunto de tanta relevância social, cultural e até mesmo financeira merecia ter sido tratada com maior afinco, por se tratar de uma área que abrange diversidades de ciências, poderia esmiuçar melhor os prejuízos que o crime cibernético pode acarretar na vida de um indivíduo e da sociedade.

Num mesmo contexto, no mesmo ano foi aprovada a Lei 12.735/12, que esboça mais duas mudanças no Código Penal Brasileiro vigente, uma delas foi a determinação da criação em cada Estado Brasileiro de unidades ou setores especialistas para combate à ações criminosas em qualquer dispositivo informatizado ou de comunicação, visando diminuir tais

ações criminosas que continuam a ser recorrentes e de uma maneira midiática, inibir os criminosos.

> Art. 4º Os órgãos da polícia judiciária estruturarão, setores e equipes especializadas no combate à ações delituosas em rede de computadores, dispositivos de comunicação ou sistema informatizado.

Em suma, as polícias civis de todo o Brasil devem se adaptar à evolução tecnológica para o combate eficaz a novos crimes, no caso em questão, crimes virtuais. Foi realizada uma pesquisa em diversos estados acerca da aplicação da Lei 12.735/12 e, lamentavelmente, não encontramos tais unidades ou setores especializados de policias civis para o combate a este crime que cada vez mais vem causando transtorno, tanto a população em geral, quanto aos governantes, pois os crimes cibernéticos vêm atacando também a grandes empresas públicas, causando prejuízos financeiros que no final das contas sairão do bolso do menos favorecido. Para se ter uma real noção da aplicação da Lei 12.735/12, pesquisamos que dentre os 26 estados brasileiros mais o Distrito Federal, apenas 17 deles possuem Delegacia especializada em crimes virtuais.

Diante do exposto, as legislações que mais são aplicadas no meio jurídico, levando-se em conta a relação da sociedade com a rede de computadores e a internet são:

O Código de Defesa do Consumidor – Lei 8.078/1990 propõe em seu art. 72 e 73.

> Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros: Pena – Detenção de seis meses a um ano ou multa. Art. 73. Deixar de corrigir imediatamente informações sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata: Pena – Detenção de um a seis meses ou multa.

Outrossim, cabe-nos explanar ainda alguns dos atos já tipificados no ordenamento jurídico pátrio, e que são descritas criminais no Código Penal vigente.

> Art. 153, § 1° - A do Código Penal – Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública. Pena – detenção de 1 a 4 anos, e multa.
> Art. 313 – A do Código Penal – Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano. Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.
> Art. 313 – B do Código Penal – Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação

> de autoridade competente. Pena – detenção de 3 (três) meses a 2 (dois) anos, e multa.
> Art. 325, § 1°, incisos I e II - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação: Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave. § 1 o Nas mesmas penas deste artigo incorre quem: I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública; II – se utiliza, indevidamente, do acesso restrito.

Podemos ter por base ainda as Leis nº 8.137/90 e 9.504/97, onde especificam, respectivamente: utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública e constituir crimes, puníveis com reclusão, de cinco a dez anos, caso o criminoso obtenha acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos; desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral e/ou causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.

3.1. Direito Comparado

A maior legislação a nível internacional que encontra-se em vigor e é referência mundial no assunto desde a evolução constante da comunicação através do uso da internet é a da Convenção de Budapeste sobre o Cibercrime, que não foi assinado pelo Brasil, está fora aprovada pelo Conselho da Europa no ano de 2001. Convenção assinada por mais de quarenta países e ratificada por 21 das nações, como França, Itália, Portugal, Espanha, Estados Unidos, Canadá, Japão, África do Sul, Austrália, Chile e Argentina.

Na supramencionada Convenção estão previstos, crimes de acesso ilícito; interceptação ilícita; interferência em dados e em sistemas alheios; produção, venda, obtenção para utilização, importação e distribuição de dispositivos concebidos para a prática de crimes cibernéticos. Além destes a convenção relaciona os crimes de falsificação de dados em quaisquer dos sistemas informáticos; violação de direitos autorais quando ocorrer em grande escala e por meio de sistemas informatizados; e a pornografia infantil.

A Convenção também estabelece os procedimentos de investigação de crimes cibernéticos. Segundo o tratado internacional, a interceptação de dados de conteúdo e de

tráfego somente será permitida para a investigação de crimes graves. Determina ainda que os fornecedores de serviço deverão conservar de maneira “imediata” os dados de tráfego, visando assim a transparência na relação de contrato. Ela prevê a obrigação dos fornecedores de serviço de comunicarem às autoridades investigatórias, quando solicitados, os dados cadastrais e outros dados informáticos necessários à identificação do responsável por um crime cibernético.

Por se tratar de crimes onde os autores e vítimas podem facilmente e constantemente ser de diferentes federações e consequentemente de diferentes regimes jurídicos penais, existe uma grande importância em caráter mundial de haver uma certa uniformização na tipificação dos delitos virtuais e sua competência, uma vez que necessita constantemente de diligências no âmbito investigatório cível e criminal que variam de federações, trazendo tanto uma morosidade processual na aplicação da lei, quanto a impunidade do criminoso por falta de legislação específica pacífica que o defina.

4. EFICÁCIA DAS NORMAS EFICÁCIA DA NORMA (VALIDADE, VIGÊNCIA E VIGOR)

A atividade jurídica diária está baseada nas petições, sentenças, contratos e outros. Para que sejam necessárias as concretudes de todos os procedimentos é inevitável não se deparar com problemas de validade. O principal objetivo é saber se a norma jurídica que se pretende iniciar a produtividade da peça é legal e pode ser utilizada na finalidade em questão. A validade de uma norma é afirmar que ela está inserida no ordenamento jurídico, deste modo, já pertence a uma série de outras normas jurídicas. Para isso ela precisa ser de maneira formal e material. Para ser formal, precisa ser criada por autoridade competente, bem como por um instrumento adequado para a execução ideal ao destinatário.

Uma pessoa terá poder para criar normas contratuais se preencher requisitos estabelecidos por autoridade estatal, por meio de lei, claro, respeitada Constituição Republicana. Em concreto, o poder de criar normas jurídicas é chamado de capacidade, quando se tratar de pessoas físicas, ou de competência, quando se tratar de pessoas ou órgãos agindo em nome alheio. O Congresso Nacional, por exemplo, é competente para criar leis ordinárias e leis complementares; o Presidente da República não é competente para criar leis, mas pode criar decretos, regulamentos e medidas provisórias.

Para que haja validade formal de uma norma, nem sempre basta que o emissor tenha autoridade, algumas normas devem ser veiculadas em instrumentos específicos, os quais

precisam preencher requisitos determinados. Uma norma sentencial deve ser criada por uma autoridade competente, ou seja, um juiz de direito, e obrigatoriamente seguir procedimentos para ser válida. A mesma autoridade, juiz, não pode criar uma norma sentencial fora de um processo judicial. Uma norma legislativa deve ser criada pelo órgão competente, Poder Legislativo, e seguir um processo próprio para tornar a lei válida: iniciativa, discussão, votação, aprovação, sanção, promulgação e publicação.

Já a validade material, trata-se de uma investigação meticulosa, onde será analisado o conteúdo textual para saber se não é contraditório com o conteúdo de outras normas jurídicas superiores e/ou mais recentes. A análise da validade material exige o conhecimento do conteúdo de todas as normas jurídicas de hierarquia à da investigada. Preenchidas as condições supramencionadas, é possível concluir que se trata de norma válida, portanto, jurídica.

Todavia, dizer que uma norma possui validade não significa, necessariamente, dizer que ela pode ser utilizada pelos juristas. Para tanto, a norma, além de ser válida, deve ser vigente. A vigência de uma norma é a possibilidade dela produzir efeitos, limitando comportamentos e sendo utilizada pelos tribunais. Como regra, uma vez que a norma jurídica se torna válida ela passa a ter vigência (pode produzir efeitos). Agora se tratando das leis, há uma exigência especial derivada da Lei Complementar n. 95/98, artigo 8º: em que toda lei deve indicar, de modo expresso, o início de sua vigência. Em alguns casos, a depender da matéria e da repercussão da nova lei no cenário da sociedade, existe a necessidade de um prazo, após a publicação da lei, para que a sociedade tome conhecimento da mesma e preparar para seus efeitos, esse lapso temporal é chamado de período de vacância. Dizer que uma lei é vigente é o mesmo que dizer que ela já pode começar a produzir efeitos. Nem toda lei válida é, necessariamente, vigente, pois pode estar em seu período de vacância.

Agora chegamos a uma questão fundamental que dá título ao presente estudo, a eficácia da norma podem ter três sentidos: técnico, fático e social. A norma possui eficácia técnica se os requisitos estatais para a produção de efeitos forem preenchidos. Vemos: muitas vezes, a lei já é válida e vigente, mas para que produza efeitos, depende da criação de outras normas que a regulamente, ou da criação de órgãos que viabilizem a execução. A eficácia fática está diretamente ligada a requisitos sociais para a produção de efeitos, nesse caso, podemos dizer que a norma não pode produzir efeitos porque a sociedade, ainda não está preparada para ela, por algum motivo. Exemplo: Pode ser que a norma se refira a alguma tecnologia ainda não criada. O significado social de eficácia é que uma norma válida e vigente pode preencher todos os requisitos técnicos e fáticos de eficácia, entretanto, pode não produzir

nenhum efeito na sociedade. Vejamos: Uma norma possui eficácia social quando for respeitada pelas pessoas e/ou for acatada pelas autoridades estatais, noutro lado a norma será socialmente ineficaz quando os próprios julgadores não a utilizarem, ou for desrespeitada e os infratores não forem punidos.

Analisando friamente a questão, uma norma que pertença ao ordenamento jurídico é válida e somente perderá a validade se for retirada, por outra norma jurídica, do conjunto. Logo, dizer que uma norma é socialmente ineficaz não faz dela uma norma inválida, pois nenhuma outra norma jurídica a retirou do ordenamento. Será que faz sentido defender que uma norma não utilizada pelos tribunais e não respeitada pela população continua a ser jurídica? Em tese uma norma não utilizada pelos tribunais por um período longo deve ser excluída ou modificada no ordenamento jurídico. Um exemplo pode ser mencionado: um juiz deverá julgar um ato jurídico conforme a lei que era válida e vigente no momento de sua prática, ainda que essa lei, no presente, tenha sido revogada. Novamente, a lei conserva seu vigor, pois é obrigatória sua adoção pelo juiz.

Os conceitos analisados no item 3 do presente estudo(validade, vigência, eficácia e vigor) cumprem a função estrutural da norma e estabelece limites do ordenamento jurídico, apontando quais normas pertencem ao conjunto legal e em que situações elas podem produzir efeitos.

4.1. A Eficácia da Lei nº 12.737/12

A prática criminosa a dispositivos informáticos se dá através da utilização do computador bem como da internet, portanto se faz imprescindível conhecer os tipos de crimes informáticos tutelados por nosso ordenamento jurídico, pois ao praticá-los o autor não terá como se beneficiar da inocência legal, ou seja, afirmar não saber da existência de lei punitiva. Para tanto, uma conduta só pode ser considerada crime se houver previsão legal que a tipifique, assim demonstrado no art. 5º, inciso XXXIX, da Constituição Federal de 1988 - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal.

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

A lei em comento, ao defasado Código Penal (BRASIL, 1940) acresceu os artigos 154-A e 154-B, passando a disciplinar o seguinte:

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.

[...]

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.

Ocorre, todavia, que as sanções previstas nos debutantes artigos, somente serão aplicadas caso o dispositivo informático da vítima tenha sido invadido, mediante a violação de mecanismo de segurança.

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

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

> [...] tive a oportunidade de externar meu pessimismo em relação à eficácia penal da lei acima referida. A crença de que a lei penal possa ter efeito preventivo está cada vez mais discutida. [...]. O problemático é esperar que isso seja feito pela lei penal.

Confio mais em medidas civis (determinadas por juiz civil, como a remoção de uma notícia ofensiva), creio mais em indenizações. Gomes (2013) acrescenta que por mínimo que seja o conhecimento jurídico da sociedade Brasileira, ela não pode se iludir. Temos que tentar tomar medidas civis mais enérgicas, pois são mais eficazes na área. Em regra da maioria das leis dependentes de interpretação, as penas são baixas, portanto, as chances de ocorrer uma prescrição é grande. E é por todos esses motivos, a descrença na eficácia preventiva dessa lei, tendo a tutela civil condições de ser mais eficiente.

Ao externar seu pessimismo quanto à eficácia da Lei 12.737/12, Gomes (2013)

explana que a atual justiça criminal brasileira, não comporta mais regramentos jurídicos, em virtude da própria execução precária à Polícia Civil, por conseguinte, ante a demora na elucidação dos fatos, acredita ser mais realmente mais eficaz buscar a solução na seara civil, buscando indenizações.

Especialista em direito digital, Victor Auilo Haikal (2013) expõe uma das fragilidades da Lei em comento, ao salientar que o delito só se concretizará se houver a obtenção, instrução ou modificação dos dados, através de violação de algum mecanismo de segurança e ainda divulgue a informação a terceiros. Portanto se o dispositivo informático estiver ligado com e com livre acesso aos conteúdos, subentende-se que qualquer pessoa poderá espionar, subtrair ou modificar os dados, uma vez que por estar desprotegido, não haverá tipificação criminosa.

Mesmo que de algum modo no caso, haja penalidade, a pena estipulada é relativamente baixa e dificilmente alguma pessoa será reclusa por conta da lei federal 12.737/2012. No caso da referida lei, totalmente voltada aos crimes cibernéticos, poderia, por exemplo, esperar a aprovação do Marco Civil da Internet (Lei 12.965) que estava em tramitação à época da aprovação, cuja foi sancionada no dia 23 de abril de 2014. Ou seja, o carro foi posto na frente dos bois, pois, "como pode haver punição se ainda não há direitos declarados?", questiona. Agora, a uma virtude na lei precoce que contribuiu para o concurso de crimes. "Havendo o concurso de crimes e a responsabilização por vários crimes juntos, a impunidade do hacker não é certeza" (PALHARES, 2002).

5. A LEI 9.099/95 E OS INSTITUTOS DESPENALIZADORES

Com a recepção da Lei nº 12.737, de 30 de novembro de 2012, dispondo sobre a tipificação criminal de crimes informáticos, alterando o CP, uma ideia surge, o estudo do artigo 202 do Código Penal segundo o entendimento das novas tecnologias e, em especial, a normativa específica em epígrafe. Súplica o dispositivo legal, in verbis: "Invadir ou ocupar estabelecimento industrial, comercial ou agrícola, com o intuito de impedir ou embaraçar o curso normal do trabalho, ou com o mesmo fim danificar o estabelecimento ou as coisas nele existentes ou delas dispor: Pena - reclusão, de um a três anos, e multa".

No Código Penal Comentado, aprofunda o artigo 202 supracitado e traz alguns conceitos memoráveis na nossa análise, entre eles o de estabelecimento: "é o lugar onde se desenvolve um determinado tipo de atividade. No caso presente, ele deve ser industrial, comercial ou agrícola". Finaliza o autor sobre a palavra sabotagem, como sendo "o nome

dado para a invasão ou ocupação de estabelecimento com o intuito de destruir ou fazer estrago no local ou nos objetos dele constantes". Para Guilherme de Souza Nucci, um objeto material do crime é o local invadido ou as coisas nele existentes; os objetos jurídicos são a liberdade de trabalho e o patrimônio do proprietário.

Avaliando o texto da legislação, que trata, dentre outras coisas, da introdução de novos tipos ao Código Penal, o confronto com o artigo 202 é inevitável, já que o referido artigo traz a invasão e a interrupção de serviços, bem como a danificação do estabelecimento ou das coisas nele existentes. O dispositivo legal de Invasão volta a ter relevância no contexto onde as novas tecnologias se fazem presentes como o cometimento de ilícitos penais e, por encontrar-se na iminência de voltar a ser bastante utilizado.

Como todos sabemos na atualidade vários dos negócios e a maioria da economia se concretizam via web, pela rede mundial de computadores e a aplicação do conceito de estabelecimento engloba também aqueles que existem apenas virtualmente e operam em ambiente de web, como alguns sites de compras ou de prestação de serviços, deve ocorrer de forma natural.

Coelho (2009, p. 96) define estabelecimento empresarial como "o conjunto de bens reunidos pelo empresário para a exploração de sua atividade econômica". E finaliza: "A proteção jurídica do estabelecimento empresarial visa à preservação do investimento realizado na organização da empresa".

Para Oscar Barreto Filho(13: 75), estabelecimento empresarial é o "complexo de bens, materiais e imateriais, que constituem o instrumento utilizado pelo comerciante para a exploração de determinada atividade mercantil". Na mesma linha de pensamento, Carvalho de Mendonça interpela o instituto como sendo um conjugado de meios materiais e imateriais pelos quais o comerciante explora determinada espécie de comércio.

No Código Civil Brasileiro, em seu artigo 1.142, *in verbis*: "Considera-se estabelecimento todo complexo de bens organizado, para exercício da empresa, por empresário, ou por sociedade empresária". Como se vê nada descreve sobre espaço físico, sendo necessário para se configurar, apenas um complexo de bens, os quais não são precisados se físico ou virtual. O entendimento deixa a possibilidade jurídica da existência de um estabelecimento formado somente por dados eletrônicos, mas que organizou seus bens, ou seja, os dados que possui para download, em um local virtual, atuando efetivamente no mercado comercial.

Conclui-se pela existência do estabelecimento virtual como uma nova categoria jurídica, pois preenche os requisitos do art. 1.142 do Código Civil, possuindo características

próprias e a mesma natureza jurídica do estabelecimento empresarial físico podendo, portanto, a ele ser equiparado. Podemos dizer que, a invasão e interrupção dos serviços oferecidos na internet, enquadrar-se-ia no tipo penal do artigo 202, em especial, se, com a invasão, os dados e elementos da referida página web (equiparada a estabelecimento, nesta linha de raciocínio), fossem danificados ou utilizados pelo invasor. De maneira que o atual conceito de estabelecimento, comporta a interpretação acima sugerida sem, com isso ferir qualquer princípio penal (vedação da analogia), já que o referido conceito é aberto e pode – deve – variar no tempo para comportar as mudanças sociais, a fim de se evitar que novas leis tenham que ser elaboradas a cada minuto para abraçar as novas situações fáticas na evolução da sociedade e principalmente da tecnológica.

A Lei que traz a invasão de dispositivo informático exposto no artigo 154-A e também a conduta de interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, elencado no parágrafo 1, do artigo 266 e o artigo 202 servirão para punir a conduta de invadir estabelecimento privado, ainda que virtual ou digital.

Segundo entendimento de Nucci, a ideia conjunta dos dispositivos legais, é possível a observação de incongruências, como, a pena aplicada e a desproporção que surge. Assim, se um indivíduo interrompe um serviço de utilidade pública, através de ataques a sites por meio de negação de serviço, incorrerá na pena do artigo 266, qual seja, detenção, de um a três anos, e multa, podendo, se beneficiar dos institutos da Lei n. 9099/95, resultando na maioria das vezes no pagamento de cestas básicas, tendo ainda sua conduta processada e julgada pela Justiça Comum. Caso o indivíduo invada e interrompa os serviços de um site de comércio eletrônico, serviço privado, ele incorrerá na pena prevista no artigo 202 do Código Penal, com pena de reclusão, de um a três anos, e multa, consequentemente, não poderá fazer uso dos institutos despenalizadores da Lei 9099/95, apesar de fazer jus a algumas outras benesses penais, sendo ainda processado e julgado pela Justiça Federal.

A situação apresentada é que se houver um ataque a um site governamental, público e de interesse coletivo a forma de processamento do feito e a punição do agente será mais branda do que se o ataque for perpetrado contra site de empresa privada, ou de interesse particular. Entendemos então que uma análise do artigo 202 deveria ter sido feita quando da elaboração da Lei 12.737, já que a aplicação de ambas pode gerar a situação explanada. Atualmente a aplicação sistemática das normativas poderão gerar situações e conflitos assustadores, já que a lei especializada não consagrou a conduta anteriormente descrita no artigo 202 do Código Penal, mantendo-o em pleno vigor.

No Brasil entende-se ser mais favorável criar leis ao invés de renovar as já existentes, como bem destaca Vicente Greco Filho(2013), são quase que capazes de cobrir todas as condutas criminosas praticadas através das novas tecnologias, com exceções, ratificando, a imagem já consolidada de um País tendencioso à inflação legislativa, especialmente a penal.

Os institutos despenalizadores são a composição civil, a transação penal e a suspensão condicional do processo, que repisam nos delitos de menor potencial ofensivo, isto é, contravenções penais e crimes que a lei comine pena máxima não superior a dois anos. Vide art.61 da Lei 9.099/95. Esse modelo de justiça mais célere visa o acordo entre as partes, primordialmente a reparação voluntária dos danos sofridos pela vítima, mas a aplicação de pena não privativa de liberdade através da aplicação das medidas despenalizadoras, evitando, sempre que possível, a instauração de um processo penal, de acordo com o que dispõe o princípio da intervenção mínima, vetor da lei dos juizados criminais.

A composição civil mostra um objetivo de reparar civilmente à vítima, a terceira via do Direito Penal, pelo pensamento do doutrinador Claus Roxin. A reparação substituiria ou diminuiria a pena nos casos em que atendam os objetivos da pena e as necessidades do ofendido. Estão em pauta interesses patrimoniais não sendo necessária a participação do Ministério Público, salvo se envolver interesse de pessoas civilmente incapazes. Pós composição dos danos, o acordo será reduzido a termo e homologado por sentença irrecorrível, considerada título executivo judicial a ser executado no próprio Juizado Especial se o valor da causa não ultrapassar, 40 salários-mínimos no âmbito da Justiça Estadual, vide art.3º, § 1º, Lei 9.099/95.

Em relação a lei estudada, vale mencionar que a composição dos danos civis poderá ser feita em crimes de ação penal de iniciativa privada e de ação penal pública condicionada à representação, a doutrina e jurisprudência majoritárias compreendem que também é cabível na ação penal pública incondicionada, embora seus efeitos sejam distintos. Já na ação penal de iniciativa privada, o acordo homologado tem como deslinde a renúncia ao direito de queixa, acarretando a extinção da punibilidade, nos termos do art.107, V, do Código Penal.

A ação penal pública condicionada à representação, trata da renúncia ao direito de queixa conduz a inegável extinção da punibilidade. Conquanto, à ação pública incondicionada a celebração do acordo não acarretará a extinção da punibilidade, pois seu objetivo é apenas antecipar a certeza do valor da indenização, trazendo a imediata execução no juízo civil competente. Contudo, incorrendo a composição o processo continuará normalmente no termos do art. 75 da lei dispondo: Não obtida a composição dos danos civis, será dada imediatamente ao ofendido a oportunidade de exercer o direito de representação verbal, que

será reduzida a termo. Parágrafo único. O não oferecimento da representação na audiência preliminar não implica decadência do direito, que poderá ser exercido no prazo previsto em Lei."

6. BEM JURÍDICO TUTELADO

Condutas praticadas por hackers, tanto de invasão de sistemas quanto de modificar, alterar, inserir dados falsos, ou seja, que atinjam diretamente o software ou hardware do computador e só podem ser concretizados pelo comutador ou contra ele e seus periféricos.

Os crimes cibernéticos podem ser aqueles que atingem um bem jurídico comum, como o patrimônio, e utilizam dos sistemas informáticos apenas como *animus operandi*, ou seja, um novo meio de execução. Há certa dificuldade em se reconhecer os crimes cibernéticos praticados contra o patrimônio, por não se reconhecer na informação armazenada um bem material, mas sim imaterial, insuscetível de apreensão como objeto.

Rita de Cássia Lopes da Silva explana:

> "a informação neste caso, por se tratar de patrimônio, refere-se a bem material, apenas grafado por meio de bits, suscetível, portanto, de subtração. Assim, ações como alteração de dados referentes ao patrimônio, como a supressão de quantia de uma conta bancária, pertencem à esfera dos crimes contra o patrimônio."

A falta de legislação específica tornava muito difícil a apuração dos crimes virtuais, uma vez que a legislação até então vigente havia sido direcionada aos crimes de forma geral, independentemente do meio utilizado para a sua prática. O Código Penal (CP), o Estatuto da Criança e do Adolescente (Lei n. 8.069/90) e Lei antipirataria, Lei n. 9.609/98) e a Lei de Segurança Nacional (Lei nº 7.170/83) eram alguns dos meios que poderíamos ter para obtenção do direito tutelado. Era muito difícil a identificação dos sujeitos e a obtenção de provas para a condenação criminal quanto aos crimes virtuais, que exige certeza.

É importante destacar o art. 154-A do Código Penal, que trouxe para o ordenamento jurídico o crime novo de "Invasão de Dispositivo Informático", consistente na conduta de "invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com 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". A pena prevista para o crime simples é de

detenção de 3 meses a um ano e multa, havendo, entretanto, a previsão das formas qualificada e causas de aumento de pena.

Chega-se ao bem jurídico tutelado como sendo a liberdade individual, a privacidade e a intimidade das pessoas como um todo. O crime em questão é comum, o sujeito ativo do crime cibernético pode ser qualquer pessoa (física ou jurídica, de direito público ou de direito privado), o mesmo se dizendo em relação ao sujeito passivo, que pode ser qualquer pessoa passível de sofrer dano moral ou material decorrente da violação do seu sistema de informática.

Os crimes virtuais são aqueles em que o sujeito se utiliza necessariamente do computador o sistema informático do sujeito passivo, no qual o computador como sistema tecnológico é usado como objeto e meio para execução do crime nessa categoria de crimes está não só a invasão de dados não autorizados mais toda a interferência em dados informatizados como, por exemplo, invasão de dados armazenados em computador seja no intuito de modificar, alterar, inserir dados falsos, ou seja, que atinjam diretamente o software ou hardware do computador e só podem ser concretizados pelo computador ou contra ele e seus periféricos. Aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas, ou seja, dados.

Num raciocínio particular DAMÁSIO DE JESUS diz que:

> "Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado".

Os crimes virtuais também podem ser realizados com a utilização do computador, ou seja, por meio da máquina que é utilizada como instrumento para realização de condutas ilícitas que atinge todo o bem jurídico já tutelado, crimes, portanto que já tipificados que são realizados agora com a utilização do computador e da rede utilizando o sistema de informática seus componentes como mais um meio para realização do crime, e se difere quanto a não essencialidade do computador para concretização do ato ilícito que pode se dar de outras formas e não necessariamente pela informática para chegar ao fim desejado.

7. CRIMES VIRTUAIS MAIS RECORRENTES

Em 2015 foi divulgado que no Brasil havia mais de 12 milhões de usuários da internet, tendendo-se dia a dia o crescimento, devido a cada vez maior facilidade no acesso. Em

levantamento feito por alemães, o Brasil em 2015 era o país que mais possuía grupos de krackes do mundo, tal estudo demonstra o mercado negro aulas para a prática de delitos virtuais no Brasil. De acordo com o estudo, a civilização do cibercrimes no Brasil é o único país que possui esta sistemática de aulas habilitando as pessoas que queiram cometer a prática criminosa no mundo.

Páginas de instituições bancárias são umas das opções mais desejadas pelos criminosos no Brasil, visando obter dados que consigam fazer movimentações contas bancárias. O curso prometendo ensinar a invasão de computadores e dados pessoais de outros usuários são oferecidos por R$ 100,00 (cem reais) em média. Se contar das ferramentas oferecidas, que facilitam e possibilitam que pessoas, mesmo sem o maior conhecimento da tecnologia que um computador e seus softwares tragam, possa haver o cometimento, por exemplo, ferramentas que possibilitem a modificação de boletos bancários e um software que envia Spam via SMS.

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

O ambiente virtual que é a Internet nos proporciona uma sensação de liberdade, pois nos dá o direito ao anonimato, só que este falso sentimento é no mínimo frustrante aos olhos da Carta Magna que veda expressamente o anonimato, no inciso IV, artigo 5º. Neste ambiente imenso que temos acesso por um simples aparelho eletrônico oferece um mundo de possibilidade, sem fronteiras, dando margem fácil prática de crimes e de complexas resolutividades, mas que exigem uma solução tanto quanto mais ligeira e especializada, pois o aumento tecnológico é proporcional aos crimes dia a dia, praticados pelos criminosos que vem neste ambiente o meio mais “seguro” para o enriquecimento ilícito, fraudes de diversos tipos, estelionato, invasões de privacidade, crimes contra honra, propriedade intelectual, danos informáticos, pornografia infantil, modificação e inserção de dados falsos em sistemas informáticos, dentre outros.(TEXEIRA, 2007).

É uma atividade desgastante e minuciosa analisar as condutas criminosas que ocorrem pelo vasto meio cibernético, uma vez que é extremamente difícil, principalmente para a polícia não especializada e qualificada, verificar onde o agente que praticou o crime se encontra, haja vista que os crimes digitais não encontram barreiras territoriais na internet e se locomovem livremente pela rede. A maioria dos delitos praticados na rede, existem no mundo real e estão elencados na nossa legislação penal brasileira, porém o que ocorre é que existem

alguns com peculiaridades, que exige uma urgente adequação quanto ao seu tipo penal. Já expressa um dos mais respeitados princípios do Código Penal, contido no artigo 5º, inciso XXXIX da Constituição Federal do Brasil; *Nullum crimen, nulla poena sine praevia lege que siginifica: Não há crime, nem pena sem lei anterior que os defina*.

7.1. Crimes Contra a Honra

Um dos problemas mais recorrentes na internet são os crimes contra a honra, entendidos como injúria, calúnia e difamação através das redes sociais. A internet não é um mundo sem lei, onde as pessoas podem fazer o que quiserem sem obter as consequências. Isso é chamado de responsabilidade pelos atos e, de forma geral, a responsabilidade pelos atos na internet é a mesma ou ainda maior que aquela do mundo físico, devido a proporção imensurável que as informações podem tomar. Portanto, não há nenhuma regra que isente uma pessoa para praticar atos ilegais no mundo virtual. A responsabilidade civil em virtude dos atos praticados na rede mundial de computadores podem ser de múltiplas formas: através de transações comerciais, troca de arquivos ou e-mails, redes sociais, dentre outras.

Evidentemente os usuários da internet não precisam ficar preocupados, já que o uso normal da rede não gera qualquer tipo de responsabilidade, apenas os atos ilícitos. Ocorrendo um ato ilícito, ele pode gerar diferentes formas de responsabilidade. A responsabilidade civil é aquela criada quando uma pessoa causa dano a outra. Quando o dano atinge o patrimônio de alguém, trata-se de dano material, a exemplo de arquivo malicioso provocando problemas no computador alheio. Também ocorre responsabilidade civil quando uma pessoa causa dano psicológico a outra, isto é, dano moral, alguém ofende a honra de outro em redes sociais ou blogs, com mensagens, comentários ou outra forma de manifestação. No caso em comento, o ofensor poderá ser condenado a pagar uma indenização à vítima, de natureza econômica.

Pode ocorrer ainda, um mesmo ato provocar dano material e moral, ajuizada apenas uma ação de indenização por reparação de danos, a fim de que o ofensor pague pelos atos e consequências. Quando os atos são resultantes de contravenções penais, a responsabilidade penal além de uma possível indenização à vítima, o autor também está sujeito às consequências do Direito Penal, com prisão, penas restritivas de direitos, multa e outros efeitos da esfera criminal.

A prova é necessária para ajuizar qualquer ação, em caso de injúria, calúnia ou difamação que possa provocar a responsabilidade civil ou penal para o ofensor, a vítima sempre precisará provar os fatos e nos casos ocorridos pela internet, na maior parte das vezes,

a prova é simples e fácil, já que é possível gravar o texto, a imagem, o vídeo ou o som que represente o ato, podendo ser feito diretamente pela vítima ou por outra pessoa que tenha conhecimento do fato.

A comunicação constantemente tem alterado o relacionamento entre as pessoas, por conta da evolução do processo tecnológico que ultrapassa barreiras culturais, distância. A maior dificuldade no ramo do Direito, é impor limites em relação a liberdade de expressão na Internet.

Dispõe o artigo 11 da Declaração dos Direitos do Homem e do Cidadão:

> Artigo 11º. A livre comunicação dos pensamentos e opiniões é um dos direitos mais preciosos do homem: todo cidadão pode, portanto, falar, escrever, imprimir livremente, embora deva responder pelo abuso dessa liberdade nos casos determinados pela lei.

No mesmo passo, harmoniza o artigo 5º IV da Carta Magna "é livre a manifestação do pensamento, sendo vedado o anonimato". Este mesmo artigo, em seu inciso XIV consagra "é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional". Já o artigo 220 indica que "a manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão nenhuma restrição, observado o disposto na Constituição." Conjuntamente ao artigo nos §§ 1º e 2º diz que "nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no artigo 5º, IV, V, X, XIII e XIV" que "é vedada qualquer censura de natureza política, ideológica e artística".

A Constituição Federal do Brasil assegura a liberdade de manifestação do pensamento, vedando o anonimato. Caso durante a manifestação do pensamento se cause dano material, moral ou à imagem, assegura-se o direito de resposta proporcional ao agravo, além da indenização (LENZA, 2008, p.601).

Acredito não ser o Estado que deva dizer quais opiniões merecem ser válidas e aceitáveis; cabe ao público a que essas manifestações se dirigem. Daí o surgimento da garantia do art. 220 da Constituição brasileira. Compreende-se que censura, constitucionalmente falando, significa ação governamental, de ordem prévia. Proibir a censura significa impedir que as ideias e fatos que o indivíduo pretende divulgar passem, antes pela aprovação de um agente estatal. A proibição da censura não obsta, porém, a que o indivíduo assuma as consequências, não só cíveis como igualmente penais, do que expressou (MENDES, 2011, p.297).

É possível entender do texto de Mendes, é livre a manifestação de pensamento, desde que não implique na prática de ato vedado pelo ordenamento jurídico. O ser humano tem Direito a liberdade de expressão e opinião também consagrada na Declaração Universal dos Direitos Humanos que em seu artigo XIX, diz que: "Toda pessoa tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras".

Nada obstante, nem sempre é possível dizer o que se pensa, e ainda mais colocar isso por escrito publicado na Internet. Foi o que ocorreu com um jovem residente em Porto Alegre, que resolveu se suicidar e criou um blog para discutir o assunto. Embora muito inteligente, deixou-se levar pela depressão e pelos conselhos de seus amigos internautas. Teve seu pedido atendido e muitas formas de se cometer suicídio foram sugeridas. Acabou por acatar uma delas, e por fim, suicidou-se. Resultado: todos os internautas que postaram as mensagens foram investigados, pois ao se matar, consumou – se o crime das pessoas que o incentivaram, que é o crime da incitação ao suicídio (PECK, 2009, p.35).

Inobstante referido excerto não se enquadre em hipóteses de crimes contra a honra, pode-se dizer que se enquadra na categoria de crime. Deve ser vedada toda e qualquer prática de crime pela internet. Há limites na liberdade de expressão.

Os tribunais vêm decidindo sobre vários casos de ofensas praticadas na Internet. Na verdade, a Internet acaba agravando o caso, já que há uma consequência maior.

Para exemplificar o assunto houve o caso de um estudante universitário do interior de Minas Gerais criou uma comunidade com o nome de um colega de faculdade. Aplicou – lhe a foto do mesmo, e com o título "cabeça de alienígena''. O rapaz, vítima da ridicularização, pediu para que fosse tirado do ar o conteúdo. Devido à recusa do colega, autor da comunidade, o rapaz ajuizou ação judicial. O juiz entendeu que a liberdade de expressão tem seu limite, até onde não gere danos a outra pessoa. Logo, o criador da comunidade foi condenado a pagar uma indenização de aproximadamente três mil reais a vítima da ofensa. Em suma, há três tipos de crimes contra a honra. O primeiro é a calúnia que significa dizer que alguém praticou um crime e isso não ser verdade. Se a calúnia ocorrer através de um e-mail distribuído na internet, todas as pessoas que tiverem recebido o e-mail e passarem para frente podem ser envolvidas em coautoria. Pois diz que, a mesma pena incorre quem, sabendo que é falsa a imputação a propaga ou divulga. Os outros dois tipos são a difamação e a injúria. Ocorrendo uma ofensa e o ofensor se arrepender, pode fazer uma retratação pública (PECK, 2009, p. 09).

Vale apresentar o entendimento que tiveram os juízes do Tribunal de Justiça do

Distrito Federal e Territórios (TJDF) ao julgarem casos cibernéticos, em fevereiro de 2011, no Distrito Federal. Em todos os casos os réus tiveram que pagar indenização às vítimas.

O primeiro deles ocorreu em um caso julgado no Especial Cível e Criminal de Planaltina. Uma sobrinha foi condenada a pagar 700 mil em indenização ao tio, pois por motivos de indisposições em questões familiares com o mesmo, a jovem postou uma foto do tio, no Orkut, onde este aparece com um cifrão estampado no rosto. Sentindo-se desrespeitado, ele entrou com uma ação de danos morais. Outro caso aconteceu na Universidade de Brasília, onde a professora de tecnologia farmacêutica foi alvo de críticas de um grupo de discussão virtual. Pediu, assim, 13 mil de indenização. O processo se arrasta desde 2005 e ainda cabe recurso. A educadora venceu em primeira instância, onde a decisão determinou que os estudantes pagassem R$ 8,5 mil a vítima.

Semelhante ao tema, ocorreu na eleição presidencial de 2010, quando a então candidata Dilma Rousseff chegou a aproximadamente 70% de votos na região nordeste do país. Isso incentivou, no Twitter, uma série de mensagens preconceituosas, contra os nordestinos, supondo-os "culpados" pelo resultado satisfatório da candidata. Um dos casos de mais destaque foi o de Mayara Petruso, estudante de direito de São Paulo, que escreveu: "Nordestino não é gente, faça um favor a SP, mate um nordestino folgado!". Diante das denúncias e publicações da imprensa, no dia 3 de novembro de a OAB de Pernambuco entrou com a notícia – crime do Ministério Público Federal em São Paulo, contra a autora das citadas mensagens. Mayara foi condenada, no dia 16 de maio de 2012, a 1 ano e 5 meses e 15 dias de reclusão, pela juíza da 9ª Vara Criminal de São Paulo. A pena, entretanto, foi convertida em multa de 500 reais, e prestação de serviços comunitários, uma vez que Mayara, não possuía antecedentes criminais e já havia sofrido "forte punição moral".

Pode-se concluir que, o que colocamos na internet em regra é público, porém, faz-se necessário, a criação ou adequação na Lei, regulamentando os limites dessa manifestação de pensamento e opinião no ciberespaço, para que condutas como: calúnia, injuria e difamação, dentre outras possam ser tipificadas como crime e com as penas agravadas.

7.2. Estelionato Eletrônico

A evolução tecnológica dos computadores digitalizou diversas funções que o homem jamais pensou que executaria com um "clique". Todavia, as ferramentas de uso exclusivo de pesquisadores científicos passaram a fazer parte do cotidiano da população, esta menos instruída quanto aos "efeitos colaterais" que a praticidade virtual poderia trazer, assim como

aos riscos que seus bens jurídicos poderiam sofrer. Desse modo, gradativamente, diversos crimes que visam à lesão patrimonial ganharam nova feição, com etapas de execução realizadas no meio digital.

Outros julgados

> Paciente denunciado por falsidade ideológica, consubstanciada em exigir quantia em dinheiro para inserir falsa informação de excesso de contingente em certificado de dispensa de incorporação. Gravação clandestina realizada pelo alistando, a pedido de emissora de televisão, que levou as imagens ao ar em todo o território nacional por meio de conhecido programa jornalístico. (...) A questão posta não é de inviolabilidade das comunicações, e sim da proteção da privacidade e da própria honra, que não constitui direito absoluto, devendo ceder em prol do interesse público.
> [HC 87.341, rel. min. Eros Grau, j. 7-2-2006, 1ª T, DJ de 3-3-2006.]
> = RHC 108.156, rel. min. Luiz Fux, j. 28-6-2011, 1ª T, DJE de 10-8-2011

Conforme explicado pelo especialista Plantullo (2003, 87), no momento em que a vítima digita o número do cartão de crédito, o agente criminoso pode descriptografar os impulsos eletrônicos emitidos e, assim, obter acesso a todos os dados do cartão da vítima, incluindo sua senha.

Existem ainda duas outras maneiras da obtenção de vantagem ilícita mediante o emprego de fraude virtual, através da qual os criminosos enviam mensagens para celulares e smartphones de usuários, alegando que sua conta bancária ou seu cartão de crédito encontra-se com pendências e o estelionato virtual: elucidada por Sandro D'Amato Nogueira (2009) como o envio de e-mails enganosos, que servem como iscas, com a finalidade de disseminação de vírus, furto de dados pessoais e senhas, entre outros. Segundo mencionado autor, o agente criminoso manda um e-mail e o destinatário que o recebe, ao abrir "a isca", instala uma espécie de programa espião que furta suas senhas e seus dados guardados no seu computador.

Repercussão geral reconhecida com mérito julgado:

> O litígio constitucional posto se traduz em um confronto entre o direito ao sigilo bancário e o dever de pagar tributos, ambos referidos a um mesmo cidadão e de caráter constituinte no que se refere à comunidade política, à luz da finalidade precípua da tributação de realizar a igualdade em seu duplo compromisso, a autonomia individual e o autogoverno coletivo. Do ponto de vista da autonomia individual, o sigilo bancário é uma das expressões do direito de personalidade que se traduz em ter suas atividades e informações bancárias livres de ingerências ou ofensas, qualificadas como arbitrárias ou ilegais, de quem quer que seja, inclusive do Estado ou da própria instituição financeira. Entende-se que a igualdade é satisfeita no plano do autogoverno coletivo por meio do pagamento de tributos, na medida da capacidade contributiva do contribuinte, por sua vez vinculado a um Estado soberano

> comprometido com a satisfação das necessidades coletivas de seu povo. Verifica-se que o Poder Legislativo não desbordou dos parâmetros constitucionais, ao exercer sua relativa liberdade de conformação da ordem jurídica, na medida em que estabeleceu requisitos objetivos para a requisição de informação pela administração tributária às instituições financeiras, assim como manteve o sigilo dos dados a respeito das transações financeiras do contribuinte, observando-se um translado do dever de sigilo da esfera bancária para a fiscal. A alteração na ordem jurídica promovida pela Lei 10.174/2001 não atrai a aplicação do princípio da irretroatividade das leis tributárias, uma vez que aquela se encerra na atribuição de competência administrativa à Secretaria da Receita Federal, o que evidencia o caráter instrumental da norma em questão. Aplica-se, portanto, o art. 144, § 1º, do CTN. Fixação de tese em relação ao item a do Tema 225 da sistemática da repercussão geral: "O art. 6º da Lei Complementar 105/2001 não ofende o direito ao sigilo bancário, pois realiza a igualdade em relação aos cidadãos, por meio do princípio da capacidade contributiva, bem como estabelece requisitos objetivos e o translado do dever de sigilo da esfera bancária para a fiscal". Fixação de tese em relação ao item b do Tema 225 da sistemática da repercussão geral: "A Lei 10.174/2001 não atrai a aplicação do princípio da irretroatividade das leis tributárias, tendo em vista o caráter instrumental da norma, nos termos do artigo 144, § 1º, do CTN."
> [RE 601.314, rel. min. Edson Fachin, j. 24-2-2016, P, DJE de 16-9-2016, Tema 225.]

Destacamos julgados do Supremo Tribunal Federal de grande repercussão nacional e internacional, acerca da quebra de sigilo telefônico e/ou telemático:

> A quebra de sigilo não pode ser manipulada, de modo arbitrário, pelo poder público ou por seus agentes. É que, se assim não fosse, a quebra de sigilo converter-se-ia, ilegitimamente, em instrumento de busca generalizada e de devassa indiscriminada da esfera de intimidade das pessoas, o que daria ao Estado, em desconformidade com os postulados que informam o regime democrático, o poder absoluto de vasculhar, sem quaisquer limitações, registros sigilosos alheios. (...) Para que a medida excepcional da quebra de sigilo bancário não se descaracterize em sua finalidade legítima, torna-se imprescindível que o ato estatal que a decrete, além de adequadamente fundamentado, também indique, de modo preciso, dentre outros dados essenciais, os elementos de identificação do correntista (notadamente o número de sua inscrição no CPF) e o lapso temporal abrangido pela ordem de ruptura dos registros sigilosos mantidos por instituição financeira.
> [HC 84.758, rel. min. Celso de Mello, j. 25-5-2006, P, DJ de 16-6-2006.]

> Utilização de gravação de conversa telefônica feita por terceiro com a autorização de um dos interlocutores sem o conhecimento do outro quando há, para essa utilização, excludente da antijuridicidade. Afastada a ilicitude de tal conduta – a de, por legítima defesa, fazer gravar e divulgar conversa telefônica ainda que não haja o conhecimento do terceiro que está praticando crime –, é ela, por via de consequência, lícita e, também consequentemente, essa gravação não pode ser tida como prova ilícita, para invocar-se o art. 5º, LVI, da Constituição com fundamento em que houve violação da intimidade (art. 5º, X, da Carta Magna).
> [HC 74.678, rel. min. Moreira Alves, j. 10-6-1997, 1ª T, DJ de 15-8-1997.]

= HC 91.613, rel. min. Gilmar Mendes, j. 15-5-2012, 2ª T, DJE de 17-9-2012

Inadmissibilidade, como prova, de laudos de gravação de conversa telefônica e de registros contidos na memória de microcomputador, obtidos por meios ilícitos (art. 5º, LVI, da CF); no primeiro caso, por se tratar de gravação realizada por um dos interlocutores, sem conhecimento do outro, havendo a de gravação sido feita com inobservância do princípio do contraditório, e utilizada com violação à privacidade alheia (art. 5º, X, da CF); e, no segundo caso, por estar-se diante de microcomputador que, além de ter sido apreendido com violação de domicílio, teve a memória nele contida sido degravada ao arrepio da garantia da inviolabilidade da intimidade das pessoas (art. 5º, X e XI, da CF).
[AP 307, rel. min. Ilmar Galvão, j. 13-12-1994, P, DJ de 13-10-1995.]

8. COMPETÊNCIA JURÍDICA PARA INVESTIGAR, PROCESSAR E JULGAR

Na legislação penal brasileira não existe um sujeito determinado pelo tipo pelos crimes praticados no em ambiente cibernético, isto é, esses tipos de crimes não podem ser classificados como próprios. Segundo Coelho (2008. p 37) expõe no trabalho "Crimes Virtuais: Análise da Prova", a sociedade está desabrigada quanto ao tipo de criminoso nesse meio, o criminoso virtual, não necessita preencher qualquer requisito que o torne habilitado para a prática do delito, bastando apenas ter acesso a um aparelho eletrônico e a internet, a partir de então o indivíduo disposto a prática do crime, poderá atacar a diversos bens jurídicos tutelados da pessoa física ou jurídica alheia em qualquer lugar do mundo.

Não é nada difícil encontrar casos de repercussão geral reconhecida com mérito julgado no Supremo Tribunal Federal, a respeito do debatido neste capítulo, tais como:

I - À luz do preconizado no art. 109, V, da CF, a competência para processamento e julgamento de crime será da Justiça Federal quando preenchidos três requisitos essenciais e cumulativos, quais sejam: a) o fato esteja previsto como crime no Brasil e no estrangeiro; b) o Brasil seja signatário de convenção ou tratado internacional por meio do qual assume o compromisso de reprimir criminalmente aquela espécie delitiva; e c) a conduta tenha ao menos se iniciado no Brasil e o resultado tenha ocorrido, ou devesse ter ocorrido no exterior, ou reciprocamente. (...) Basta à configuração da competência da Justiça Federal que o material pornográfico envolvendo crianças ou adolescentes tenha estado acessível por alguém no estrangeiro, ainda que não haja evidências de que esse acesso realmente ocorreu. A extração da potencial internacionalidade do resultado advém do nível de abrangência próprio de sítios virtuais de amplo acesso, bem como da reconhecida dispersão mundial preconizada

no art. 2º, I, da Lei 12.965/2014, que instituiu o Marco Civil da Internet no Brasil. Não se constata o caráter de internacionalidade, ainda que potencial, quando o panorama fático envolve apenas a comunicação eletrônica havida entre particulares em canal de comunicação fechado, tal como ocorre na troca de e-mails ou conversas privadas entre pessoas situadas no Brasil. Evidenciado que o conteúdo permaneceu enclausurado entre os participantes da conversa virtual, bem como que os envolvidos se conectaram por meio de computadores instalados em território nacional, não há que se cogitar na internacionalidade do resultado. Tese fixada: "Compete à Justiça Federal processar e julgar os crimes consistentes em disponibilizar ou adquirir material pornográfico envolvendo criança ou adolescente (arts. 241, 241-A e 241-B da Lei 8.069/1990) quando praticados por meio da rede mundial de computadores." [RE 628.624, rel. p/ o ac. min. Edson Fachin, j. 29-10-2015, P, DJE de 6-4-2016, Tema 393.]

A materialidade é quem representará a ocorrência do crime virtual, de maneira tal que evidencie a conduta ilícita do agente ativo. Comprovar a materialidade de um crime é tão precípuo quanto apresentar a autoria, pois ambas são indispensáveis para se proferir uma sentença de mérito que condene o réu.

> [...] por ser o delito ação humana, indubitável que seu sujeito ativo é o homem. Não se trata, porém, de parte inerente à conduta que a lei descreve como crime, e, sim, daquele a quem pode ser atribuída a prática de ação ou omissão que tem a configuração legal do delito. As qualidades pessoais de quem pratica o delito, sua situação particular, as relações que tenha com o ofendido constituem elementos que se referem ao sujeito ativo, mas que não se identificam com este. (Damásio de Jesus, 2003, p. 165).

Como uma maneira de ilustrar e tornar mais rico o estudo, levo ao conhecimento as jurisprudências infrafirmadas:

> Processo: CC 121215 / PR. CONFLITO DE COMPETÊNCIA
> 2012/0036333-8
> Relator(a): Ministra ALDERITA RAMOS DE OLIVEIRA
> (DESEMBARGADORA CONVOCADA DO TJ/PE)
> Órgão Julgador: S3 - TERCEIRA SEÇÃO
> Data do Julgamento: 12/12/2012
> Data da Publicação/Fonte: DJe 01/02/2013
> CONFLITO DE COMPETÊNCIA. CRIMES RELACIONADOS À DIVULGAÇÃO DE MATERIAL PORNOGRÁFICO ENVOLVENDO CRIANÇAS E ADOLESCENTES POR MEIO DA INTERNET. INEXISTÊNCIA DE ELEMENTOS DE INTERNACIONALIDADE. COMPETÊNCIA DA JUSTIÇA ESTADUAL. PRECEDENTES DO STJ.
>
> Processo: CC 116926 / SP. CONFLITO DE COMPETÊNCIA
> 2011/0091691-2

> Relator(a): Ministro SEBASTIÃO REIS JÚNIOR (1148)
> Órgão Julgador: S3 - TERCEIRA SEÇÃO
> Data do Julgamento: 04/02/2013
> Data da Publicação/Fonte: DJe 15/02/2013, RT vol. 934 p. 468
> PENAL. CONFLITO DE COMPETÊNCIA. CRIME DE RACISMO PRATICADO POR INTERMÉDIO DE MENSAGENS TROCADAS EM REDE SOCIAL DA INTERNET. USUÁRIOS DOMICILIADOS EM LOCALIDADES DISTINTAS. INVESTIGAÇÃO DESMEMBRADA. CONEXÃO INSTRUMENTAL. EXISTÊNCIA. COMPETÊNCIA FIRMADA PELA PREVENÇÃO EM FAVOR DO JUÍZO ONDE AS INVESTIGAÇÕES TIVERAM INÍCIO.

Entendemos que a materialidade do crime virtual, deve ser considerado sempre como o primeiro ponto a ser almejado pelo investigador, com o objetivo de ratificar com maior clareza a existência real do delito. Todas as informações no meio virtual são bastante volúveis e inconstantes, o que é preciso na maioria das vezes, a impressão e/ou autenticação das informações sempre que encontradas no espaço virtual. Se a destruição dessas provas não fosse possível, desnecessária seria uma continuação da investigação visando encontrar a autoria do crime. Ainda que haja alguma dúvida acerca da materialidade, o julgador, durante a fase final do processo penal, não poderá prolatar sua decisão e o réu deverá ser absolvido, na fundamentação legal da insuficiência de provas que comprovem a denúncia.

Em regra, partindo-se do princípio da circunscrição jurídica em que o fato foi noticiado, deve-se observar antecipadamente, onde se desenvolveu a ação criminosa. A objeção será maior em virtude da internet não estabelecer um alcance limitado territorial, bem como as relações pessoais ou jurídicas podem ser de países distintos e inclusive de diferentes culturas, o que em alguns casos, mesmo após a constatação da autoria e materialidade do fato, subjetivaria a ocorrência do crime, tendo em vista que há crimes elencados no Código Penal Brasileiro que não são considerados crimes em outros países e vice-versa.

> Processo: CC 150564 / MG. CONFLITO DE COMPETÊNCIA 2016/0338448-1
> Relator(a): Ministro REYNALDO SOARES DA FONSECA
> Órgão Julgador: S3 - TERCEIRA SEÇÃO
> Data do Julgamento: 26/04/2017
> Data da Publicação/Fonte: DJe 02/05/2017
> CONFLITO NEGATIVO DE COMPETÊNCIA. JUSTIÇA FEDERAL X JUSTIÇA ESTADUAL. INQUÉRITO POLICIAL. DIVULGAÇÃO DE IMAGEM PORNOGRÁFICA DE ADOLESCENTE VIA WHATSAPP E EM CHAT NO FACEBOOK. ART. 241-1 DA LEI 8.069/90. INEXISTÊNCIA DE EVIDÊNCIAS DE DIVULGAÇÃO DAS IMAGENS EM SÍTIOS VIRTUAIS DE AMPLO E FÁCIL ACESSO. COMPETÊNCIA DA JUSTIÇA ESTADUAL

O que não há na atualmente é uma linha fincada para determinar qual a legislação aplicável ao caso concreto, o que temos são diversos princípios, como o princípio do (IP), endereço eletrônico, o do local em que a conduta ilícita se realizou ou exerceu seus efeitos, o do domicílio do consumidor ou réu e o da eficácia na execução judicial. No ordenamento pátrio, aplicam-se os artigos 5° e 6° do Código Penal Brasileiro, no que se refere a competência para processar e julgar os crimes praticados na internet, sejam eles:

> Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.
>
> Art. 6º - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.

Como se pode verificar, a Constituição Federal aderiu a teoria da ubiquidade, também disposto no art. 6° do Código Penal, sendo determinado que a cidadãos brasileiros, tanto os delitos praticados em território nacional quanto os praticados fora, será aplicado à lei brasileira. O que se pode pensar é encontrar um equilíbrio entre a liberdade de expressão/informação e a proteção de dados pessoais, para que os bens jurídicos tutelados sejam reconhecidos no meio virtual e os bens jurídicos provenientes do meio virtual sejam reconhecidos como um todo. Ocorre que passamos por um período desprovido, com uma enorme inflação legislativa e uma lei penal sobre crimes virtuais que só veio a aumentar as estatísticas de leis editadas e vigentes que não tem a devida eficácia. É de suma importância dizer que hiperplasia penal inflamou com o modelo socialista de Estado A exemplo desta ineficácia temos a Lei dos Crimes Hediondos que ao contrário do que se pensavam não fez diminuir os crimes da espécie. Com o pensamento do professor Salo de Carvalho (2003): O Estado está se tornando mais penitenciário do que previdenciário, esculpindo este primeiro ser uma máxima: “Estado social mínimo, Estado penal máximo”. Na mesma ideologia a saída verossímil para aqueles que foram absolvidos e/ou não tiveram uma cidadania digna: a marginalização social é incrementada pelo controle dela.

Trago logo abaixo mais um exemplo de conflito de competência acerca de crime envolvendo o computador e a internet:

> Processo: RHC 85605 / RJ.
> RECURSO ORDINÁRIO EM HABEAS CORPUS 2017/0139017-4.
> Relator(a): Ministro REYNALDO SOARES DA FONSECA
> Órgão Julgador: T5 - QUINTA TURMA
> Data do Julgamento: 26/09/2017

> da Publicação/Fonte: DJe 02/10/2017
> RECURSO ORDINÁRIO EM HABEAS CORPUS. TROCA DE IMAGENS PORNOGRÁFICAS COM ADOLESCENTE VIA WHATSAPP E SKYPE. ART. 241-1 DA LEI 8.069/90. ÂMBITO PRIVADO DAS MENSAGENS. COMPETÊNCIA ESTADUAL. ALEGAÇÃO DE LITISPENDÊNCIA. NÃO CONSTATAÇÃO. PRISÃO PREVENTIVA. NECESSIDADE DE GARANTIA DA APLICAÇÃO DA LEI PENAL. PREVENÇÃO DA REITERAÇÃO DELITIVA. FUNDAMENTAÇÃO IDÔNEA. EVENTUAIS CIRCUNSTÂNCIAS PESSOAIS FAVORÁVEIS. IRRELEVÂNCIA. MEDIDAS CAUTELARES ALTERNATIVAS. INSUFICIÊNCIA. CONSTRANGIMENTO ILEGAL NÃO EVIDENCIADO. RECURSO DESPROVIDO.

Não obstante as ações não estejam apropriadamente codificadas em leis, tendo em vista o caráter globalizado, tecnológico do tema bastante flexível, as condutas de agente em crimes digitais ao longo do tempo vão sendo adequadas à legislação vigente, ainda que de modo incidental e variando a tipificação de acordo com o bem jurídico violado.

Na incerteza dessa jurisdição no ciberespaço, como e a quem aplicar a lei, enfrentamos na Internet um problema geográfico de desterritorialização, devido a ilimitada fronteira física, deixando assim relativizado o conceito de soberania do Estado, bem como o do tempo que ocorrera algum ato. Somente a cooperação global na Internet virá nos acalentar e possivelmente trazer resultados a contento eficientes que vinguem perante a sociedade e as constantes atualizações tecnológicas. Ou seja, problemas mundiais exigem soluções globais, a cada passo dado pela inovação do ciberespaço, deve ser observada as limitações e a atuação conjunta internacional para em trabalho conjunto disciplinar o ciberespaço. Devemos ainda salientar que esta não é um dever somente intrínseca do Direito, mas sim de várias áreas que possam estreitar os laços entre a vida real e a vida no meio cibernético.(ROSSINI, 2004).

É na investigação policial que se encontra a problemática do discutido. Para termos uma ideia e modelo, algumas Polícias, tais como a Scotland Yard, que há mais de 10 anos forma policiais especializados e extremamente treinados para combater a prática dos crimes virtuais que se pode chamar de o pior desafio criminal do próximo século. Estes especialistas, reiteradamente enfatizam a falta de controle e a forma totalmente desordenada em que Internet se alastra pelo mundo. (MIRANDA 1999).

Destarte, as condutas chamadas de crimes virtuais, embora já exista legislação específica, ainda encontra-se oculta ou digamos indeterminada, quando se trata de fundamentação jurídica para a denúncia e posterior julgamento e condenação do réu, pois existe a novidade que é como o criminoso tem feito uso das novas tecnologias, fazendo com que os estudiosos e os aplicadores do Direito tenham que renovar/ampliar o seu pensamento. Para ilustrar a temática do consolidado, a norma específica brasileira que define Crimes de

Informática no código penal, já tem 5 anos e atualmente foi possível encontrar alguns poucos embates quanto a aplicação da mesma, ressalto, ainda não pacificada, conforme demonstrado durante este capítulo.

8. CONCLUSÃO

Ante o exposto uma interrogação merece ser analisada: Com a legislação acerca do crime estudado, é possível uma aplicação à altura do dano que pode ser causado através da internet nos dias atuais?

Está mais que comprovado à luz das pesquisas, dos acontecimentos que temos como elemento principal no meio cibernético, que a Lei Federal nº 12.737/2012, ao longo dos seus breves quatro artigos, deixou a desejar tanto em relação à pena aplicada ao criminoso, tanto quanto própria eficácia da norma, haja vista que a legislação penal de 1940 é suficiente para a tutela dos bens jurídico-penais violados pela internet, em que o sistema informacional seria apenas mais um meio a ser utilizado para a concretização do mesmo.

O presente estudo mostrou que a aplicação das normas do Código Penal aos chamados dados informáticos não são feitos por analogia, mas sim por uma interpretação extensiva. A analogia supera as omissões das normas por meio da aplicação de situação semelhante, equivalente. A interpretação extensiva acontece pela intenção da lei não expressar verbalmente o que é distintamente aplicável no Direito Penal, inclusive aceito pelo STF, conforme demonstrado. Conclui-se assim, pela desnecessidade de uma legislação específica para a tutela de crimes informáticos.

Durante todo o trabalho, principalmente baseado na jurisprudência, nos mostrou através de dados estatísticos do maior site brasileiro de julgados da legislação vigente, bem como de pesquisa global, acerca de crimes cibernéticos a inutilização do art. 154-A e 154-B acrescidos pela lei federal em epígrafe.

O direito penal é suficiente para a tutela dos dados informáticos, interpretação extensiva, pois são igualados ao termo “coisa” previsto, por exemplo, no crime de estelionato, artigo 171 do Código Penal, o que também foi demonstrado, ao longo, entendimento jurisprudencial.

A desnecessidade da lei 12.737/2012, conhecida como Carolina Dieckmann, veio apenas para ratificar a tutela de crimes e bens jurídicos abarcados pelo Código Penal, segundo demonstração jurisprudencial. Conforme já foi dito, o Direito Penal deve está se adequando às novas realidades sociais, assim como o julgador deve aplicá-lo de forma a interpretar o direito e revelando a real intenção da lei a cada caso.

REFERÊNCIAS BIBLIOGRÁFICAS

BAUMAN, Zygmunt, **"Extimidade": o fim da intimidade.** Tradução Moisés Sbardelotto. La Repubblica, 09/04/2011. Disponível em: < http://www.ihu.unisinos.br/noticias/42263-extimidade-o-fim-da-intimidade> Acesso em: 05 fev. 2018

BETIOLI, Antônio Bento. **Introdução ao Direito.** 11 ed. São Paulo: Saraiva, 2011. (Lição XVI).

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

Código Penal brasileiro. Disponível em:
https://www.conteudojuridico.com.br/pdf/cj054548.pdf

COMPUTADOR. In: WIKIMEDIA FOUNDATION. Wikipédia: a enciclopédia livre. 25 mar. 2006. Disponível em: Acesso em: 14 abr. 2016.

CONVENÇÃO DE BUDAPESTE. 2011. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf> Acesso em: 12 dez. 2017.

CRESCE EM 274% O NÚMERO DE ATAQUES CIBERNÉTICOS NO BRASIL. REVISTA BRASIL. Disponível em: <radios.ebc.com.br/revista-brasil/edicao/2016-02/pesquisa-revela-crescimento-de-274-em-numero-de-ataques-ciberneticos>. Acesso em: 08 ago. 2017.

CUNHA, Rogério Sanches. **Manual de Direito Penal** - Parte especial 7 ed. Salvador: JusPodivm, 2015. (arts. 121 ao 361).

DECLARAÇÃO DOS DIREITOS DO HOMEM E DO CIDADÃO: ÍNTEGRA DO DOCUMENTO ORIGINAL. Assembleia Nacional. UOL Educação, 18/03/2006. Disponível em: <https://educacao.uol.com.br/disciplinas/historia/declaracao-dos-direitos-do-homem-e-do-cidadao-integra-do-documento-original.htm> Acesso em: 16 Nov. 2017.

DINIZ, Maria Helena. **Lei de Introdução ao Código Civil Brasileiro Interpretada**. 16 ed. São Paulo: Saraiva, 2011. (art. 1º)

Disponível em: http://www.institutoejam.com.br/>; Consulta em 13 abr. 2016.

Disponível em: https://www.jusbrasil.com.br/topicos/28004011/artigo-154a-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940/jurisprudencia Acesso em 20 nov . 2017

Disponível em: http://www.conteudojuridico.com.br/artigo,a-extimidade-da-sociedade-digital-e-a-eficacia-da-lei-1273712-invasao-de-dispositivo-informatico,53339.html

Disponível em: https://edufranco91.jusbrasil.com.br/artigos/142294529/os-entraves-a-repressao-aos-crimes-ciberneticos?ref=news_feed

ESTEFAM, Andres; GONÇALVES, Victor Eduardo Rios. **Direito penal esquematizado** – Parte Geral. 3. Ed. São Paulo: Saraiva, 2014, p. 238.

FERRAZ JÚNIOR, T. S. **Introdução ao Estudo do Direito:** Técnica, Decisão e Dominação. 4ª edição. São Paulo: Atlas, 2003. (4.3.2)

FRANCO, Alberto Silva. **Doutrinas e Jurisprudências.** Código Penal e sua interpretação. 8 ed. RT, 2007.

JORGE, Higor Vinicius Nogueira; WENDT, Emerson. **Crimes Cibernéticos**: ameaças e procedimentos de investigação. 2 ed. Rio de Janeiro: Brasport, 2013.

BRASIL. LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Diário Oficial [da] Republica Federativa do Brasil, Brasília, DF. 03. dezembro. 2012

BRASIL. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial [da] Republica Federativa do Brasil, Brasília, DF. 03. dezembro. 2012.

LÉVY, Pierre. **Cibercultura.** Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999. 264 p. (Coleção TRANS). Disponível em: <https://edisciplinas.usp.br/pluginfile.php/4091443/mod_resource/content/1/Cibercultura%20%28LEVY%29.pdf>. Acesso em: 06 ago. 2017

LIMA, Simão Prado. Crimes virtuais: uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade. **Âmbito Jurídico**, Rio Grande, XVII, n. 128, set 2014. Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=15260&revista_caderno=3>. Acesso em: abril 2018.

MIRANDA, Marcelo Baeta Neves. Abordagem dinâmica aos crimes via Internet . Jus Navigandi, Teresina, a. 4, n. 37, dez. 1999. Disponível em: . Acesso em: 01 set. 2017.

MURARD, Ana Beatriz Conte. **Crimes contra a honra na Internet.** Jusbrasil, 25/02/2015. Disponível em: <https://anabmurard.jusbrasil.com.br/artigos/169528179/crimes-contra-a-honra-na-internet>. Acesso em: 06 ago. 2017

NICOLAU, Aldemir. O que é ciberespaço? **WEBARTIGOS**, 06 agosto 2009. Disponível em: < https://www.webartigos.com/artigos/o-que-e-ciberespaco/22537/#ixzz4wjDIh9zR> Acesso em: 22 jul. 2017

OLIVEIRA, Luiz Gustavo Caratti de; DANI, Marília Gabriela Silva. Os crimes virtuais e a impunidade real. **Âmbito Jurídico**, Rio Grande, XIV, n. 91, ago 2011. Disponível em: <http://www.ambito-

juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9963>. Acesso em abril 2018.

PESQUISA GLOBAL DE SEGURANÇA DA INFORMAÇÃO 2017. **PWC Brasil.** Disponível em: <https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2017/pesquisa-global-seguranca-2017.html>. Acesso em: 22 jul. 2017

PLANTULLO, Vicente Lentini. **Estelionato Eletrônico: segurança na Internet**. É o dinheiro digital que substitui o numerário em espécie. Curitiba: Juruá, 2003, P. 87.

ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal.** São Paulo: Memória Jurídica, 2004.

SILVA, Camila Requião Fentanes da. Análise das Leis nº 12.735/2012 e 12.737/2012 e a (des)necessidade de uma legislação específica sobre crimes cibernéticos**. Jus.com.br**, Set.2014. Disponível em:<https://jus.com.br/artigos/32265/analise-das-leis-n-12-735-2012-e-12-737-2012-e-a-des-necessidade-de-uma-legislacao-especifica-sobre-crimes-ciberneticos/2>. Acesso em: 20 jul. 2017

SILVA, E. F. da. **Direito à Intimidade**. São Paulo: Oliveira Mendes, 1998, p. 131.

SUPERIOR TRIBUNAL DE JUSTIÇA – STJ. Conflito de Competência: CC 150564 MG 2016/0338448-1. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/465717092/conflito-de-competencia-cc-150564-mg-2016-0338448-1>. Acesso em: 29 de set de 2017

SUPERIOR TRIBUNAL DE JUSTIÇA – STJ. Habeas Corpus: HC 415530/0229976-0. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/560815346/habeas-corpus-hc-415530-pr-2017-0229976-0>. Acesso em: 29 de set de 2017

SUPERIOR TRIBUNAL DE JUSTIÇA – STJ. Recurso em Habeas Corpus: 85605 – RJ. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/514557015/recurso-ordinario-em-habeas-corpus-rhc-85605-rj-2017-0139017-4/relatorio-e-voto-514557067?ref=juris-tabs>. Acesso em: 29 de set de 2017

TABET, Arthur Gomes; PEREIRA, Luiza Barbosa; JORGE, Ricardo Clemente. Uma análise da ineficácia do direito penal brasileiro em relação à internet. **Jornal Eletrônico Faculdades Integradas Vianna Júnior**, ano 8, ed.2, dezembro 2016. Disponível em: <http://portal.viannajr.edu.br/files/uploads/20170320_090949.pdf> Acesso em: 20 ago. 2017

TANGERINO, Dayane A. Fanti. Análise do artigo 202 do Código Penal à luz das novas tecnologias e da nova Lei 12.737/2012 – delitos informáticos. **Revista Jus Navigandi**, Teresina, ano 18, n. 3724, 11 set. 2013. Disponível em: <https://jus.com.br/artigos/25269>. Acesso em: 26 abr. 2018.

TEIXEIRA, Tarcisio. **Direito Eletrônico**. São Paulo: Editora Juarez de Oliveira, 2007.

WESTPHALEN, Frederico. **Rede de Computadores.** 2014 p. 15.