Interdisciplinary
LINKSCIENCEPLACE
Scientific Journal
ISSN: 2358-8411
DOI: 10.17115
Interdisciplinary Scientific Journal. ISSN: 2358-8411
Nº 6, volume 5, article nº 13, December 2018
D.O.I: http://dx.doi.org/10.17115/2358-8411/v5n6a13
Accepted: 18/08/2018 Published: 30/12/2018
VIII SEMINÁRIO E IV CONGRESSO INTERDISCIPLINAR DIREITO E MEDICINA
CUIDADOS PALIATIVOS – 20 A 22 DE AGOSTO DE 2018 – ITAPERUNA

CRIMES DIGITAIS: UMA NECESSÁRIA RELEITURA DO DIREITO PENAL À LUZ DAS NOVAS TECNOLOGIAS

Fernanda Rosa Acha [1]
Mestranda pela Universidade Estadual do Norte Fluminense (UENF) em Cognição e Linguagem. Pós Graduada em Direito Penal. Advogada e Professora de Direito Penal e Processual Penal.

Resumo - A análise da nova forma de criminalidade mostra-se relevante na medida em que se observam avanços tecnológicos, notadamente com o advento da *internet* e desenvolvimento da globalização, capazes de alterar a forma de cometimento de crimes, bem como os processos investigativos relacionados ao seu esclarecimento. Nessa toada, estudar a repercussão dessas novas modalidades de cometimento ou mesmo, novos tipos penais, apresenta-se necessário a fim de compatibilizar com o estudo do direito penal e processual penal, promovendo uma releitura em alguns importantes institutos. Assim, o objetivo no artigo é situar o direito penal e processual nessa nova dinâmica delitiva, traçando os avanços já observados e algumas práticas que devem ser adotadas para efetividade da investigação e aplicação da lei. Utiliza-se, para tanto, no trabalho, o método de pesquisa qualitativo, analisando as opiniões e reflexões já realizadas por estudiosos do assunto, as quais permitirão concluir pela necessária caminhada do direito penal rumo às novas tecnologias. Assim, serão abordados, no presente estudo, a origem e evolução da *internet* no Brasil, passando, logo em seguida, às mudanças realizadas pela introdução das novas tecnologias no aspecto comportamental, finalizando com a adaptação do direito penal e processual penal a essa nova realidade, bem como as mudanças e avanços legislativos nessa seara.

Palavras Chave: Crimes, internet, globalização, tecnologia, direito penal.

Abstract - The study of this new way of criminality is relevant because it can be seen technologies advances, especially with the internet and globalization, which is capable to modify the crimes and the investigations. Following that line, study the consequences of these new way of crimes

[1] UENF. Campos dos Goytacazes. E-mail: ferosaacha@hotmail.com

seems necessary so that it can be aligned with the penal law and processual law, increasing a rereading of some important institutes. So that, the objective of this article is situate the penal law in this new dynamic, showing the advances and practices that must be taken for the effectivity of the investigation and law appliance. This article uses the qualitative method, studying the opinions of the persons who have the knowledge of the subject, which will help to find the conclusion of the penal law to these new technologies. As a conclusion, the study will analyze the origin and evolution of internet in Brasil, following by the changes caused by the introduction of these new technologies in the behavior aspect, ending with the penal law adaptions to this new reality and the law advances in this issue.

Key words: Crimes, internet, globalization, technology, penal law

1- INTRODUÇÃO

Há muito já se discutem as repercussões da *internet* e do implemento e disseminação das tecnologias no contexto social, destacando, no presente artigo, a sua importância no aspecto criminal. Sabendo-se que o direito penal tutela os bens jurídicos considerados mais relevantes, mostra-se relevante estudar a repercussão da *internet* nas práticas criminosas e no surgimento de outros tipos penais. A utilização massificada da *internet*, além de proporcionar melhorias, facilidade e economia de tempo, também revelou seus aspectos negativos, com o aumento de pessoas que a utilizam para práticas perversas e criminosas, com destaque para furtos, pornografia infantil e crimes contra a honra. Assim, revela-se necessário o acompanhamento da ciência do direito nas suas várias vertentes, sobretudo no direito penal e processual penal, contando, agora, com um novo inimigo que utiliza o anonimato da rede global para prática de crimes de cada vez mais difícil elucidação.

Na linha do exposto, o artigo pretende estabelecer a origem da *internet* no Brasil e suas repercussões sociais, provocando o direito a se manifestar sobre as várias práticas utilizadas e disseminadas. Após, serão desenvolvidos os conceitos de crimes digitais, com enfoque na elucidação dos bens jurídicos protegidos, questionando acerca da necessidade ou não de criação de novos tipos penais para maior proteção social. Em seguida, passa-se à análise da adequação do direito penal e processual penal a essas novas práticas, demandando releituras e adaptação dos seus institutos, bem como preparo do pessoal para investigar esses

crimes de autoria cada vez mais oculta, sem olvidar dos avanços legislativos já operados em nosso Ordenamento Jurídico.

Para sedimentação e conclusão do objetivo acima destacado, serão utilizados referenciais doutrinários capazes de conduzir a uma resposta sobre a importante questão do comportamento do direito penal e processual penal diante das novas tecnologias.

2 - ORIGEM E EVOLUÇÃO DA INTERNET NO BRASIL

A internet encontra sua origem em meados do século XIX, quando se iniciou a difusão no mundo dos conceitos de redes de transmissão de informações através do Telégrafo. Desde esse momento, as redes de telecomunicações começaram a se multiplicar a partir dos anos 1950 com a revolução da Microeletrônica.

O rápido desenvolvimento das tecnologias de informação e comunicação (TIC) começaram a se difundir no governo norte-americano, principalmente no período pós-Guerra, estimulados por grandes investimentos em novos modelos de informação. (MOWERY; SIMCOE, 2002). Essa grande massa de troca de informações iria originar a “rede das redes” de computadores e, nos meados de 1960, seria denominada *Internet*.

O governo norte americano criou a primeira rede de comunicação de pacote de dados (Defense Advanced Research Projects Agency Network – ARPANET), que seria a primeira forma de comunicação da Internet. (CERF et al., 2000; GREENSTEIN, 2010). Posteriormente, os estudos aprimoraram essa rede criando então o Internet Protocol (IP) que mudou os paradigmas da telecomunicação e Informática.

A partir dos anos 80, desenvolveu-se a *internet* como é conhecida hoje e a popularização dos microcomputadores tornou possível um acesso economicamente viável.

No Brasil, a iniciação da *internet* começou por forte incentivo e comando do Poder Público nas telecomunicações, quando, em abril de 1975, a Embratel recebeu a missão de instalar e explorar uma rede de dados com finalidade um pouco mais universalizada, tendo em vista que os poucos bancos de dados existentes se restringiam às instituições do governo, somente podendo ser acessados por público interno. (BENAKOUCHE, 1997, p. 127)

Na década de 80, a Embratel, então monopolizadora dos serviços, lançou o projeto Ciranda restrito aos funcionários da empresa, interligando os computadores e constituindo, assim, a primeira comunidade tele informatizada do pais. Após tal fato, lançou-se também uma rede pública de transmissão de dados, RENPAC (Rede Nacional de Comunicação de dados por comutação de pacotes), a qual teve pouca aceitação, sendo sanada com outro projeto, denominado Cirandão, destinado a ofertar o serviço ao público em geral (DE CARVALHO, 2006. p. 64-65).

Também nessa década, o monopólio estatal sobre os serviços de comunicação de dados passou a ser quebrado, o que permitiu que outras empresas pudessem concorrer, o que de fato somente foi implementado na década de 90 em razão da necessidade de capacidade e infraestrutura.

A partir de uma intenção de disseminar a *internet* no Brasil, logo o setor acadêmico despertou interesse, com foco na troca de teses e estudos, tanto no âmbito interno da instituição de ensino, como internacionalmente.

Em 1992, começaram a ser criados os primeiros Servidores (Computadores de realizam a operação e distribuição da Internet) de grande porte denominados Backbones, que seriam os descentralizadores da Internet.

Em 1995, através de uma portaria interministerial foi definido o Comitê Gestor da Internet no Brasil(CGI.br) com representantes da Academia, empresas e usuários, debatendo diretrizes para desenvolvimento, segurança e inovações da internet, momento em que se começou a difundir a concepção de que a Internet era um serviço de valor adicionado sobre o qual não haveria nenhum monopólio.

A partir de então, a *internet* passa a ser uma realidade para os brasileiros, primeiro ligada ao próprio setor de comunicações, depois espalhada para o campo educacional, quando, então, se desenvolveu para o acesso de milhares de pessoas que, hoje, podem se conectar com um simples toque no celular.

3- O DESENVOLVIMENTO TECNOLÓGICO E AS MUDANÇAS SOCIAIS E COMPORTAMENTAIS

Já tendo sido delineada a origem e a evolução da *internet* no Brasil convém relacionar o seu uso para as mais diversas finalidades, sejam elas positivas ou negativas. O desenvolvimento tecnológico, em especial, com a disseminação da *internet* e suas ferramentas, mostrou-se instrumento de relevante valor para o

crescimento das relações pessoais, econômicas, informacionais, e porque não se dizer, também, criminosas.

Inseridos que estamos na chamada era informacional, com uso de diversos aplicativos e sempre conectados à rede, tanto para vivências sociais ou vinculadas ao trabalho, somos expostos a uma enormidade de situações e atividades que são desenvolvidas de forma mais célere através da internet.

Não soa estranho acompanhar em tempo real as principais notícias do mundo, realizar compras em sites, pagar contas, trabalhar nos domicílios (homeoffice), pedir refeições por meio de aplicativos, conversar e interagir com pessoas localizadas em territórios longínquos, tudo isso podendo ser feito de maneira prática, barata e célere, através da internet.

O uso do ciberespaço vem permitindo a criação de novas ideias, profissões, atividades e transações, ultrapassando o limite do imaginável, pois a cada ano vivenciamos novas possibilidades e ultrapassagem de barreiras, levando os indivíduos a uma verdadeira dependência desse importante mecanismo de interação social/profissional.

Ocorre que, nem só aspectos positivos ressoam do ciberespaço, já que, diante desse novo cenário de múltiplas funções e atividades realizadas, muitos dados e informações ficam desprotegidos, vulnerando os usuários, que, despreparados tecnicamente, figuram como vitimas de crimes praticados na internet.

Na contemporaneidade, a criminalidade digital é fator crescente, somando-se, dentre alguns outros fatores, o aumento do número de usuários da rede, as falhas de segurança desta, bem como a frequente inabilidade ou negligência em seu uso, expandindo-se o cometimento por diversas vias, tais como e-mails, redes sociais digitais e demais páginas que propiciam o compartilhamento de mensagens, fotos, vídeos etc (CERQUEIRA, 2013, p. 145/146).

Na linha do apresentado, citam-se as anotações sobre o assunto de Simone dos Santos Lemos Fernandes e Valéria Caldi (2017):

> A internet e redes assemelhadas, além de proporcionarem uma absurda evolução no campo das comunicações, mostrarem ser, ao mesmo tempo, instrumentos poderosos para a prática de delitos, funcionando como um incrível combustível para a prática de condutas ilícitas, cobertas pelo manto do anonimato ou, no mínimo, da dificuldade de identificação da autoria. As atividades ilícitas não estão mais restritas por limites físicos relacionados à presença, transporte, distribuição e vigilância. A noção de imunidade, num pais como o Brasil, onde já muito forte, ficou ainda muito mais fortalecida. (p. 104).

Focando no aspecto criminal, ciente de que o Direito Penal possui como objetivo primordial a proteção dos bens jurídicos considerados relevantes à sociedade, analisar o avanço da referida ciência diante dessa nova realidade mostra-se de suma importância, já que são experimentadas práticas cada vez mais expansivas e lesivas, exigindo do estado uma resposta efetiva.

Ademais, o Direito deve acompanhar a evolução e os anseios sociais, não se podendo desvincular da sociedade, já que fora criado para essa finalidade: regular a vida em comunidade.

O Direito Penal é uma ciência revestida de uma principiologia peculiar, ligada, essencialmente, ao chamado principio da reserva legal ou legalidade, que significa que não haverá crime, nem pena sem anterior previsão legal, traduzindo no brocardo latino *"nullum crimen, nulla poena sine lege"* e inserido na Constituição Federal, no artigo 5º, inciso XXXIX.

Além disso, destacam-se os princípios da fragmentariedade e intervenção mínima, revelando-se a ocupação desse ramo do Direito somente para as condutas mais lesivas do ponto de vista da proteção do bem jurídico.

O direito penal seleciona as condutas mais gravosas para fins de sancionar, sendo este o caráter fragmentário do mesmo, posto que nem todos os comportamentos violam bens jurídicos capazes de atrair a tutela criminal (BITENCOURT, 2014, p. 55).

Relacionando-se os princípios acima com os crimes digitais ou crimes praticados na *internet*, o direito penal volta-se a essa vertente, analisando-se quais os bens jurídicos violados, bem como em quais situações exige-se a atuação desse ramo excepcional do Direito.

Sobre os citados bens jurídicos, convém destacar que a evolução social dita a seleção e proteção de alguns pelo direito penal, surgindo, em razão da intensificação e popularização da *internet*, incremento na ocorrência de atos ilícitos, o que demanda a analise de um outro bem jurídico a ser protegido.

Não se nega que muitos crimes só tiveram uma adaptação na sua forma de execução, agora utilizando a internet, em nada alterando a seleção previamente estabelecida pelo direito penal em relação às normas já tipificadas, citando-se como exemplos comuns, extorsões, crimes contra dignidade, subtração de bens e ameaças realizadas no ambiente virtual, dentre outros. (Brito, 2013, p. 41)

Mesmo havendo a citada proteção e o respeito à legalidade, não se pode ignorar que há bens ainda não protegidos, em especial quando se pensa em condutas como invasões de sistemas informáticos, capazes de causar danos de grande dimensão de ordem social, patrimonial e pessoal, emergindo, dessa nova ordem de ideias, a necessária proteção da segurança informática, abarcando a integridade, confidencialidade e disponibilidade das informações no ciberespaço.

4- CRIMES CIBERNÉTICOS

O aparecimento dos crimes virtuais ou cibernéticos liga-se ao fenômeno mundial conhecido como globalização, responsável por operar mudanças nas searas policias, econômicas e sociais, e desta forma, estabelecer novas formas de comportamento, ensejando a atuação do Direito como forma de regulação normativa.

Após a Segunda Guerra Mundial, iniciou-se a quarta fase da globalização (de ALMEIDA DUARTE, 2009, p. 82), trazendo um novo estágio do capitalismo com tendências multinacionais, refletindo no estabelecimento de uma linguagem comum e universal, crescente disparidade e desigualdade entre os países, surgimento de sociedade de consumo, aparecimento da *internet* e de novas formas de criminalidade.

A Globalização não é, portanto, um fenômeno que repercute somente na política e na economia, mas também na sociedade, comunicação e informação e, nesse ponto, apresenta-se como fenômeno positivo e negativo simultaneamente, abrindo espaço para uma nova criminalidade, mais organizada e de difícil persecução. (PINHEIRO, 2006, p. 3-4)

Até então, os bens jurídicos protegidos pelo direito penal eram essencialmente ligados à pessoa e seus bens, sendo individuais. Com o desenvolvimento do capitalismo e globalização, surgem os bens jurídicos coletivos ou supra individuais, como a ordem pública, econômica, meio ambiente e outros.

Nessa dinâmica, dispõe Evandro Lins e Silva (2003)

> (...) É evidente que a existência um mercado global, sem fronteiras geográficas, com regras próprias, e que não se submete ao controle dos Estados- nações, tende a criar novas formas de criminalidade que se caracterizam por ser uma criminalidade supranacional, por ser uma criminalidade que possui uma estrutura hierarquizada, por ser uma

> criminalidade que dificulta sobremaneira detectar o lugar de sua ocorrência e por ser uma criminalidade na qual os limites entre atividades criminosas e atividades lícitas tornam-se frouxos, evanescentes (p. 178-179).

Com destaque, as palavras de Ulrich Sieber (2008):

> O processo de globalização proporciona novas oportunidades de execução de crimes que ultrapassam fronteiras, levando o direito penal a seus limites territoriais e exigindo novos modelos de um direito penal transnacional eficaz. O desenvolvimento da sociedade de informação e da sociedade de risco gera novos riscos e uma criminalidade complexa, que também leva o direito penal- principalmente no contexto de uma crescente política criminal global- a seus limites funcionais na proteção da sociedade e da liberdade do individuo e o coloca ante novos desafios categoriais. (p. 270)

Nessa toada, aparecem os crimes informáticos, os quais remontam a década de 60, quando apareceram os primeiros casos de utilização do computador para prática de crimes como sabotagem, espionagem, entre outros, evoluindo, a partir de então, para piratarias de computador, abusos nas telecomunicações, manipulações de caixas bancárias, condutas envolvendo pornografia infantil etc. (NETO, 2003, p. 68).

Teriam esses crimes como “alvo os computadores em si, em geral, a partir de ataque a integridade de dados, confidencialidade e privacidade dos usuários, como fonte de armazenamento de arquivos pornográficos ou softwares pirateados, ou como ferramentas auxiliares para a prática de outros crimes” (BRITTO, 2017, p. 7).

Antes de adentrar à conceituação e classificação desses crimes cometidos na internet, deve-se ressaltar a dificuldade do direito penal em lidar com esse avanço tecnológico especialmente colocado pela *internet*, já que seria este um ambiente livre e sem fronteiras, aproveitando-se os agentes da possibilidade do anonimato e da ausência de regras na rede mundial de computadores.

Mas, então, o que seriam os crimes virtuais? Em uma simples resposta chega-se à conclusão de que seriam quaisquer ações típicas, antijurídicas e culpáveis cometidas contra ou pela utilização de processamento automático de dados ou sua transmissão em que a *internet* seja o principal objeto ou instrumento do crime.

Do conceito acima exposto, advém a importante classificação dos crimes digitais ou *cibercrimes*. Isso porque a informática permite tanto o cometimento de novas modalidades criminosas, como serve de meio para a prática de já conhecidos

tipos penais, citando-se como exemplos, o furto, estelionato, pornografia infantil, injúria etc.

Haveria, assim, crimes cometidos com o computador, sendo este o meio, e crimes cometidos contra o computador, ou seja, contra as informações e programas nele contidos, sendo aquele o objeto do crime.

Compartilhando de tal ideia, porém, utilizando-se de classificação diversa, apareceriam os crimes virtuais puros, mistos e comuns, destacando-se as lições de Mário Furlaneto Neto e José Augusto Chaves (2003).

> O crime virtual puro seria toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, pelo atentado físico ou técnico ao equipamento e seus componentes, inclusive dados e sistemas. Crime virtual misto seria aquele em que o uso da internet é condição *sine qua non* para a efetivação da conduta, embora o bem jurídico visado seja diverso do informático, como, por exemplo, as transferências ilícitas de valores em uma homebanking ou no chamado salamislacing, onde o cracker retira de milhares de contas correntes, diariamente, pequenas quantias que correspondem a centavos e as transfere para uma única conta. Por derradeiro, crime virtual comum seria utilizar a internet apenas como instrumento para a realização de um delito já tipificado pela lei penal. Assim, a Rede Mundial de Computadores acaba por ser apenas mais um meio para a realização de uma conduta delituosa. Se antes, por exemplo, o crime como o de pornografia infantil (art. 241 do ECA) era instrumentalizado por meio de vídeos ou revistas, atualmente, dá-se por salas de bate-papo, ICQ, como também pela troca de fotos por e-mail entre pedófilos e divulgação em sites.(p.69)

Seguindo classificação similar, Augusto Eduardo de Souza Rossini (2002):

> Há os Delitos Informáticos Puros, aqueles em que o sujeito visa especificamente ao sistema de informática em todas as suas formas, sendo que a informática é composta principalmente do software, do hardware (computador e periféricos), dos dados e sistemas e dos meios de armazenamento. A conduta (ou ausência dela) visa exclusivamente ao sistema informático do sujeito passivo. São exemplos, atos de vandalismo contra a integridade física do sistema em razão de acesso desautorizado – as condutas dos hackers e crackers – ainda não tipificadas no Brasil, além de algumas já previstas, como as hipóteses preconizadas na Lei n 9.609/98 (Lei de Proteção de Software). E há os Delitos Informáticos Mistos, em que o computador é mera ferramenta para a ofensa a outros bens jurídicos que não exclusivamente os do sistema informático. Alguns de seus exemplos são o estelionato, a ameaça e os crimes contra a honra, podendo imaginar-se, inclusive, homicídio por meio da internet (mudança à distância de rotas de aviões, alterações à distância de medicamentos com o desautorizado uso do sistema informático de um hospital.(p. 138-139)

Exemplificando a classificação acima disposta, Vladimir Aras (2008):

> Cada dia veem em maior número as notícias sobre *cibercrimes*, dos quais são espécies os delitos informáticos próprios (crimes praticados contra sistemas informáticos) e os delitos informáticos impróprios (crimes praticados por meio de sistemas informáticos). Na espécie "própria" ou "pura", reúnem-se práticas como o *hacking,* a difusão de *softwares* daninhos

> (*malware)* e os ataques de negação de serviço (*denial of service attacks*). Entre os delitos impróprios, estão os crimes de violação de direitos de autor, ciberpedofilia, ciberdiscriminação e estelionato informático. (p.2)

A par das diversas conceituações, classificações e nomenclaturas, o que é certo é que, existem, com o advento da informática e *internet*, crimes que se distinguem pelo bem jurídico violado, eis que atentariam contra o sistema de informática e contra outros valores sociais ou outros bens jurídicos, cometidos através de um sistema de informática, que compreenderiam todas as espécies de infrações previstas em lei penal.

Combinando-se com a necessidade de o direito penal proteger bens jurídicos caros à sociedade, revela-se imperioso a proteção da segurança informática, o que se faz através da criação de alguns tipos penais informáticos puros, o que será abordado no tópico da legislação nacional.

No plano internacional, conscientes dessa nova realidade de criminalidade, em especial após o atentado terrorista de 11 de setembro de 2001, resultou-se a edição da Convenção de Budapeste, com o objetivo de escolher uma legislação comum que tivesse como objetivo a cooperação entre os estados na luta contra a criminalidade no ambiente virtual (BRITO, 2013, p. 47).

Dessa convenção, houve a tipificação das seguintes condutas, destacadas por David Augusto Fernandes (2013):

> (...)1) Infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos: a) acesso doloso e ilegal a um sistema de informática; b) interceptação ilegal de dados ou comunicações telemáticas; c) atentado à integridade dos dados (conduta própria de um subgrupo hacker, conhecido como cracket10); d) atentado à integridade de um sistema; e) produção, comercialização, obtenção ou posse de aplicativos ou códigos de acesso que permitam a prática dos crimes acima indicados. 2) Infrações informáticas: a) falsificação de dados; b) estelionatos eletrônicos (v.g., os phishing scams11). 3) Infrações relativas ao conteúdo: a) pornografia infantil (produção, oferta, procura, transmissão e posse de fotografias ou imagens realistas de menores ou de pessoas que aparecem como menores, em comportamento sexual explícito); b) racismo e xenofobia (difusão de imagens, ideias ou teorias que preconizem ou incentivem o ódio, a discriminação ou a violência contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica; injúria e ameaças qualificadas pela motivação racista ou xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade); 4) Atentado à propriedade intelectual e aos direitos que lhe são conexos. (p. 145-146)

Além da Convenção de Budapeste, destaca-se a Convenção Universal sobre o Direito do Autor, a Convenção de Berna para a Proteção das Obras Literárias e

Artísticas, o Acordo sobre os aspectos dos direitos de propriedade intelectual relacionadas ao comércio e o Tratado da Organização Mundial da Propriedade Intelectual sobre o direito do autor, destacando-se a importância da primeira Convenção acima abordada, a qual contribuiu significativamente para a elaboração da Lei 12965/14- Marco Civil da Internet. (CERQUEIRA, 2013, p. 142).

Ademais, nessa linha, o governo norte americano, em razão do ataque terrorista de 11 de setembro, estabeleceu o chamado *Patriot Act*, fortalecendo o serviço de inteligência com mecanismos de obtenção de dados na *internet*, estabelecendo sanções aos responsáveis por invasões ou danificações não autorizadas aos sistemas de computadores governamentais (BRITTO, 2017, p. 11/12).

5- A NECESSÁRIA RELEITURA DO DIREITO PENAL E PROCESSUAL PENAL À LUZ DESSA NOVA FORMA DE CRIMINALIDADE

Como já mencionado, a rede mundial permitiu uma mudança social, de hábitos e costumes, tornando-se, além de importante meio de obtenção de informação, motivo de inquietude em razão das mais variadas práticas ilícitas, gerando um tipo de criminalidade que contém uma série de dificuldades no seu deslinde e aplicação das sanções estatais, isto porque caracterizada pela dificuldade de investigação, alteração dos conceitos e espaço e tempo, proteção do anonimato, obtenção de provas e caráter transnacional dos delitos, o que pode servir para gerar conflitos de competência.

Sobre a questão territorial e de fronteiras do ciberespaço, bem pontua Emeline Piva Pinheiro (2016):

> Com o ciberespaço, a geografia como a conhecemos (física) desaparece, surge uma nova geografia, algo que não é material, mas ainda assim é real. O ciberespaço é um não lugar, ou um lugar imaginário, que só temos acesso pelo computador, mesmo assim ele está ligado à realidade pelo uso que temos feito dele nos dias atuais, transformando-o em um espaço intermediário entre duas realidades. Como já dissemos, o lugar de situação da internet é o ciberespaço, o espaço virtual, logo, ela não existe espaço físico, mas nem por isso ela deixa de ser real. Como o direito deve lidar com esta falta de lugar, de espaço físico da internet é uma das grandes questões da atualidade (p.10).

O caráter transnacional dos delitos, alterando os conceitos físicos de espaço, conforme acima exposto, são uma marca desses crimes virtuais, ensejando,

conflitos entre os estados soberanos em razão das diversas espécies normativas internas e formas de investigações próprias de cada pais.

Como, muitas das vezes, são crimes que ultrapassam as fronteiras internas do país, surgem impasses quanto à territorialidade e soberania, trazendo questionamentos e busca de soluções sobre a forma de lidar com essa nova criminalidade, a ponto de não agredir a soberania interna e ao mesmo tempo ser eficiente no combate de tão expansivos e danosos eventos criminosos.

A característica marcante desses crimes tem gerado reflexões no sentido de se criar uma rede de integração global entre as nações, facilitando a investigação e coleta de provas, justamente diante da possibilidade de serem objeto de execução a distância, envolvendo diversos países e ultrapassando as fronteiras nacionais em questão de segundos. Além disso, vislumbra-se a necessidade de melhor equipar os profissionais vinculados à atividade persecutória criminal, provendo-os de equipamentos e treinamentos capazes de analisar esses novos crimes, agindo de forma preventiva e repressiva (PINHEIRO, 2016, p. 26).

Nessa linha, cresce a exposição de ideias no sentido de consolidar formas de integração e cooperação internacional, facilitando a aplicação do direito penal, como se percebe da transcrição de Ulrich Sieber (2008).

> Para o resultante desenvolvimento de um direito penal com eficácia transnacional, há duas abordagens distintas na esfera da atividade legislativa penal, entres os quais se encontram, ainda, numerosas formas mistas. Por um lado, são desenvolvidos modelos de cooperação estatal em assuntos penais, pelos quais são validadas as decisões de um sistema de direito penal nacional em um outro sistema de direito penal. Uma abordagem cooperativa como esta fundamenta tanto a clássica colaboração administrativa e judiciaria como o novo princípio- há alguns anos proferido na União Europeia- de reconhecimento reciproco de decisões judiciais. (...) por outro lado, desenvolvem-se um direito penal supranacional, com o qual o ordenamento jurídico penal abrange um campo de aplicação territorial maior desde o inicio. Esse modelo é encontrado esporadicamente no direito sancionador da Comunidade Europeia (por exemplo, na formação de carteis e na proteção dos interesses financeiros da comunidade europeia) e também- com uma abrangência mundial- no direito penal internacional. Entre esses dois modelos existem numerosas formas mistas de uniões federativas e supranacionais, caracterizadas pela coexistência de ordenamentos jurídicos, centralizados e descentralizados ou pela diferenciada divisão das atividades legislativa, judicial e executiva entre instituições centralizadas e descentralizadas. Exemplos de modificações dos modelos-base supracitados são o modelo suíço de competências federais e dos cantões ou o direito penal internacional, dependente do trabalho conjunto com Estados Nacionais. (p. 273-274)

Além do fator da fronteira e da soberania, encontram-se problemas com elucidação dos crimes e identificação da autoria em razão da dificuldade de

identificação dos IPs, os quais podem ser burlados com recursos de mascaramento, bem como em razão da confidencialidade de alguns conteúdos, os quais utilizam a criptografia, impedindo a realização do trabalho da polícia investigativa.

Ademais, diante do despreparo de muitos usuários em detrimento do notório conhecimento de outros, crescem os novos criminosos do mundo moderno: os hackers e crackers. Estes utilizam toda a expertise para o cometimento de crimes cada vez mais complexos e que, sendo praticados na *internet*, ganham uma rápida disseminação ao mesmo tempo em que garantem um anonimato em conjunto com o rápido perecimento dos meios probatórios, diluindo-se na mesma velocidade de sua consumação.

Os fatores acima fazem crescer a necessidade de especializar e investir numa polícia especializada ao combate de tais crimes, não sendo crível a sustentação da mesma forma de investigação realizada para o combate aos crimes comuns.

À luz do exposto, Sílvio de Castro Cerqueira e Claudionor Rocha lecionam que (2013):

> As instituições responsáveis pelas investigações criminais não podem se dar ao luxo de parar no tempo e esperar que os acontecimentos ditem suas respostas à sociedade. Atendendo aos princípios gerais do Direito Administrativo, elas precisam, sob pena de ingressar na esfera de ineficiência, se adiantar ao crime e construir estruturas que lhes permitam efetivamente cumprir suas missões constitucionais dentro dos preceitos afetos às ações do administrador público. Deixar de buscar a evolução propiciada pelo mundo da tecnologia equivale a negar o emprego de novos e eficientes instrumentos de combate ao crime moderno, que é executado sem aviso, sem violência, sem contato pessoal, onde o criminoso busca refúgio no anonimato do universo cibernético e restará impune se não houver o devido preparo da força repressora. (p. 155)

6- AVANÇOS LEGISLATIVOS

Apesar das dificuldades acima, a nossa legislação vem avançando, destacando-se, principalmente, a Lei do Marco Civil e a Lei Carolina Dieckmann, sendo esta aplicada para fins penais, com criação de tipos e proteção de bens jurídicos relevantes na luta contra a criminalidade digital.

De acordo com Patrícia Peck (2016):

> Do ponto de vista do amadurecimento do Ordenamento Jurídico, há três estágios evolutivos para que um país dê tratamento adequado às novas questões criminais, em especial no tocante á segurança digital: 1º estágio:

> ter lei penal que trate os novos delitos e condutas ilícitas que ocorrem em ambiente da web-alcançado pelo Brasil em 2012 mesmo que de modo inicial (poucos artigos foram aprovados); 2º Estágio- garantir a capacidade de guarda de prova de autoria para a penalização do infrator- o Brasil conseguiu um pequeno avanço com a promulgação da Lei Marco Civil da Internet, mas ainda falta muito a fazer, principalmente para afastar a oportunidade de anonimato em meios digitais, que acaba, por sua vez, alimentando ainda mais a impunidade e a insegurança; 3º Estágio- criar um modelo próprio de cárcere digital para colocar o criminoso versão 2.0, evitando que haja apenas cárcere físico e ele continue, mesmo que preso, a agir por meio da web, bem como investir em sua reintegração na sociedade no combate ao próprio crime digital- isso o brasil nem iniciou, pois exigiria a revisão de todo o modelo de execuções penais e penitenciário, como outros países já estão fazendo, em especial EUA e Comunidade Europeia (p. 386 e 387)

Sobre a Lei do Marco Civil da Internet (lei 12.965/14), trouxe-se a garantia da liberdade de expressão, privacidade e neutralidade da rede, intimidade dos usuários, inviolabilidade das comunicações, vedação da divulgação de dados pessoais, obrigatoriedade de guarda de registros de conexão e obrigação de retirada dos conteúdos infringentes.

Já com relação à Lei 12.737 de 2012 (Carolina Dieckmann), que incluiu a figura típica previsto no Código Penal no artigo 154- A, prevê como comportamento criminoso a conduta de 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, com pena prevista de detenção, de 3 (três) meses a 1 (um) ano, e multa.

Juntamente com esse novo delito, podem ser citados os artigos e crimes abaixo enumerados, os quais revelam o esforço e atenção do legislador para a prevenção e repressão dos crimes passíveis de serem cometidos pela internet.

- Artigo 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.
- Artigo 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.

- Artigo 266, do Código Penal- Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa. § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento
- Artigo 241- A, ECA- Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: pena: reclusão de três a seis anos e multa. Nas mesmas penas incorre quem: I- assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo; II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo; § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.
- Artigo 241-B, ECA- Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
- Art. 2º da Lei 8137/91- Constitui crime da mesma natureza: (...)V - 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. Pena - detenção, de 6 (seis) meses a 2 (dois) anos, e multa.
- Artigo 10 da Lei 9296/96- Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa.
- Artigo 72, da Lei 9504/97. 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; II -

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; III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.

- Artigo 12 da Lei 9609/98- Violar direitos de autor de programa de computador: Pena - Detenção de seis meses a dois anos ou multa. § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: Pena - Reclusão de um a quatro anos e multa. § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

Além das previsões normativas acima sedimentadas, o legislador, antenado à necessidade de melhor estruturar a forma e a celeridade das investigações, previu mecanismos mais eficientes de combate aos crimes praticados em âmbito virtual, destacando as previsões normativas abaixo colacionadas.

A primeira refere-se à lei 7716/89, acrescentando o legislador, por meio das leis 12.735/2012 e 12.288/12 as seguintes medidas: cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio e interdição das respectivas mensagens ou páginas de informação na rede mundial de computadores. Com a alteração legislativa, o juiz poderá determinar a imediata remoção da publicação ofensiva e discriminatória, com estabelecimento de penalidade referente ao crime de desobediência. (BRITO, 2013, p. 73)

> Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. Pena: reclusão de um a três anos e multa. § 1º Fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos ou propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo. Pena: reclusão de dois a cinco anos e multa. § 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza: Pena: reclusão de dois a cinco anos e multa § 3º No caso do parágrafo anterior, o juiz poderá determinar, ouvido o Ministério Público ou a pedido deste, ainda antes do inquérito policial, sob pena de desobediência: I - o recolhimento imediato ou a busca e apreensão dos exemplares do material respectivo; II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da

> publicação por qualquer meio; III - a interdição das respectivas mensagens ou páginas de informação na rede mundial de computadores.

Também as leis 12.894/13 e 13.642/18 incluíram na Lei 10.446/2002, que versa sobre crimes de repercussão internacional e interestadual, atribuição da Polícia Federal para apuração de crimes de falsificação, corrupção e adulteração de medicamentos, assim como sua venda, inclusive pela internet, bem como quaisquer crimes praticados pela rede mundial de computadores que propaguem o ódio ou aversão às mulheres.

> Art. 1º Na forma do inciso I do § 1º do art. 144 da Constituição, quando houver repercussão interestadual ou internacional que exija repressão uniforme, poderá o Departamento de Polícia Federal do Ministério da Justiça, sem prejuízo da responsabilidade dos órgãos de segurança pública arrolados no art. 144 da Constituição Federal, em especial das Polícias Militares e Civis dos Estados, proceder à investigação, dentre outras, das seguintes infrações penais: (...) V - falsificação, corrupção, adulteração ou alteração de produto destinado a fins terapêuticos ou medicinais e venda, inclusive pela internet, depósito ou distribuição do produto falsificado, corrompido, adulterado ou alterado. (...) VII – quaisquer crimes praticados por meio da rede mundial de computadores que difundam conteúdo misógino, definidos como aqueles que propagam o ódio ou a aversão às mulheres."

Já no âmbito dos crimes cometidos contra criança e adolescente, importante evolução adveio com a previsão da infiltração dos agentes de polícia para a investigação dos crimes contra a dignidade sexual das crianças, previstos no estatuto da Criança e Adolescente, culminando no acréscimo dos artigos 190-A a 190- pela Lei 13.441/ 2017.

> Art. 190-A. A infiltração de agentes de polícia na internet com o fim de investigar os crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos arts. 154-A, 217-A, 218, 218-A e 218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), obedecerá às seguintes regras: I – será precedida de autorização judicial devidamente circunstanciada e fundamentada, que estabelecerá os limites da infiltração para obtenção de prova, ouvido o Ministério Público; II – dar-se-á mediante requerimento do Ministério Público ou representação de delegado de polícia e conterá a demonstração de sua necessidade, o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas; III – não poderá exceder o prazo de 90 (noventa) dias, sem prejuízo de eventuais renovações, desde que o total não exceda a 720 (setecentos e vinte) dias e seja demonstrada sua efetiva necessidade, a critério da autoridade judicial. § 1º A autoridade judicial e o Ministério Público poderão requisitar relatórios parciais da operação de infiltração antes do término do prazo de que trata o inciso II do § 1º deste artigo. § 2º Para efeitos do disposto no inciso I do § 1º deste artigo, consideram-se: I – dados de conexão: informações referentes a hora, data, início, término,

> duração, endereço de Protocolo de Internet (IP) utilizado e terminal de origem da conexão; II – dados cadastrais: informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão. § 3º A infiltração de agentes de polícia na internet não será admitida se a prova puder ser obtida por outros meios. Art. 190-B. As informações da operação de infiltração serão encaminhadas diretamente ao juiz responsável pela autorização da medida, que zelará por seu sigilo. Parágrafo único. Antes da conclusão da operação, o acesso aos autos será reservado ao juiz, ao Ministério Público e ao delegado de polícia responsável pela operação, com o objetivo de garantir o sigilo das investigações. Art. 190-C. Não comete crime o policial que oculta a sua identidade para, por meio da internet, colher indícios de autoria e materialidade dos crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos arts. 154-A, 217-A, 218, 218-A e 218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Parágrafo único. O agente policial infiltrado que deixar de observar a estrita finalidade da investigação responderá pelos excessos praticados.

Ciente das várias práticas de crimes contra patrimônio ocorridas por intermédio da internet, citando-se como exemplo rotineiro a cópia das senhas bancárias para obtenção de vantagem patrimonial indevida, o STJ e demais órgãos jurisdicionais passaram a enquadrar na figura típica prevista no artigo 155, parágrafo 4º, II, do Código Penal, o qual consagra o chamado furto qualificado pelo emprego da fraude, muito embora seja tema de divergência eis que passível de inclusão em outra modalidade delitiva, prevista no artigo 171 do mesmo diploma: o estelionato.

Nessa linha, o projeto de lei (PLS) 76/2000, que seguia tramitação em conjunto com os projetos 89 de 2003 e 137 de 2000, pretendia tipificar o furto eletrônico no artigo 155, §4º, inciso V do CP, com pena de reclusão de 2 a 8 anos e multa, bem como o crime de estelionato informático com o nome de “difusão de código malicioso”, numa tentativa de definir e tipificar os delitos informáticos.

No mesmo projeto, havia a previsão de uma outra figura criminosa, cujo bem jurídico tutelado seria a proteção da segurança dos sistemas informatizados (ou informáticos, conforme previsão na Convenção de Budapeste), a ser prevista no artigo 285-A o qual se consumaria quando o agente acessasse a rede de computadores, dispositivo de comunicação ou sistema informático protegido por restrição de acesso.

Além desse, havia a previsão também do artigo 285-B que cuidava da obtenção ou transferência, sem autorização ou em desconformidade com autorização do legitimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação nesses disponível.

Seguindo a mesma sistemática de previsão de normas penais incriminadoras, destacava-se a inserção no artigo 163, do Código Penal da expressão “ou dado eletrônico alheio”, ficando assim constituído o tipo penal:

> Artigo 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio. Além disso, no mesmo projeto, pretendia-se a criação de um novo tipo penal, sedimentado no artigo 163-A, cujo teor seria: Criar, inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado. Pena: reclusão, de um a três anos, e multa. § 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultarão do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado: Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa. § 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Apesar do esforço legislativo acima evidenciado, o projeto teve sua tramitação encerrada, conforme se observa no site do Senado, no endereço eletrônico disposto: https://www25.senado.leg.br/web/atividade/materias/-/materia/43555,

> (Matéria incluída na Ordem do Dia, extra pauta, conforme acordo entre as lideranças partidárias). Discussão encerrada, sem debates. Aprovada a Emenda nº 4-CCT/CCJ (Substitutivo), ficando prejudicados o Projeto de Lei da Câmara nº 89, de 2003, os Projetos de Lei do Senado n.º 76 e 137, de 2000, que tramitam em conjunto e, ainda, as demais emendas e subemendas. (...) Os Projetos de Lei do Senado n.º 76 e 137, de 2000, prejudicados, vão ao Arquivo. À SGM, com destino ao Arquivo.

7 – CONSIDERAÇÕES FINAIS

As mudanças sociais e comportamentais operadas, muito em razão do desenvolvimento da tecnologia e da internet, refletem em uma nova forma de cometimento de delitos, aproveitando-se os criminosos do anonimato e da dificuldade de elucidação dos crimes.

A rapidez do trâmite das informações, a possibilidade de escamotear a identidade e também ocultar os elementos da materialidade fazem com que os crimes cometidos na internet sejam, hoje, a forma mais eficaz de sucesso na empreitada delitiva.

Para acompanhar essa nova modalidade criminosa, é preciso modificar as antigas formas de prevenção e repressão, preparando os agentes para uma rápida e eficaz persecução penal, devendo, para tanto, investir em trabalhos de inteligência

informática e investigativa, contando, outrossim, com a participação e cooperação de órgãos de repressão internacional.

Além disso, o direito penal, como importante ramo da ciência jurídica, capaz de selecionar os bens jurídicos mais caros ao individuo, deve voltar-se a essa nova realidade, readaptando seus tipos penais ou mesmo criando outros capazes de atender aos anseios da crescente criminalidade na internet.

REFERÊNCIAS:

BENAKOUCHE, Tamara. Redes técnicas/redes sociais: pré-história da Internet no Brasil**.** *Revista USP*, 1997, 35: 124-133.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, D.F: Senado Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 05 jun.2018.

BRASIL. Código Penal. Decreto- Lei nº 2848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 07 jun. 2018.

BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 07 jun. 2018

BRASIL. Lei 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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 08 jun. 2018.

BRASIL. Lei 8137, de 27 de dezembro de 1990. Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8137.htm. Acesso em: 08 jun. 2018.

BRASIL. Lei 8069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8069Compilado.htm. Acesso em: 08 jun. 2018.

BRASIL. Lei 9296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do artigo 5º da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/l9296.htm. Acesso em: 07 jun. 2018

BRASIL. Lei 9504, de 30 de setembro de 1997. Estabelece normas para as eleições. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/l9504.htm. Acesso em: 07 jun. 2018

BRASIL. Lei 9609, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no pais, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 07 jun. 2018

BRASIL. Lei 7716, de 5 de janeiro de 1989. Define os crimes resultantes de preconceito de raça ou de cor. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L7716.htm. Acesso em: 08 jun. 2018.

BRASIL. Lei 10.446, de 8 de maio de 2002. Dispõe sobre infrações penais de repercussão interestadual ou internacional que exigem repressão uniforme, para os fins do disposto no inciso I do parágrafo primeiro do art. 144 da Constituição. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/2002/L10446.htm. Acesso em: 08 jun. 2018.

BITENCOURT, Cezar Roberto. Tratado de Direito Penal: parte geral**.** 20.ed. ver., ampl. E atual.- São Paulo: Saraiva, 2014

BRITO, Auriney. Direito Penal Informático. São Paulo: Saraiva, 2013.

BRITTO, Gladstone Avelino; FREITAS, Maristella Barros. Ciberataques em massa e os limites do poder punitivo na tipificação de crimes informáticos. *Revista de Direito Penal, Processo Penal e Constituição*, 2017, 3.2: 1-16.

CARVALHO, M. S. R. M. A trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança. *Unpublished Estudos de Ciência e Tecnologia no Brasil, Universidade Federal do Rio de Janeiro, Rio de Janeiro*, 2006

CERQUEIRA, Sílvio Castro; ROCHA, Claudinor. Crimes cibernéticos: desafios da

investigação**.** Cadernos Aslegis, p. 131-161, 2013. Disponível em: file:///C:/Users/Usuario/Downloads/crimes_ciberneticos_cerqueira_rocha%20(2).pdf. Acesso em: 10 mar. 2018.

DE ALMEIDA DUARTE, Maria Carolina. Globalização e a Nova Criminalidade**.** Territórios e Fronteiras, v. 2, n. 1, p. 81-98, 2009. Disponível em: http://www.ppghis.com/territorios&fronteiras/index.php/v03n02/article/view/32. Acessoem: 10 mar. 2018.

FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. Revista da Faculdade de Direito da UFMG, v. 2013, n. 62, p. 139-178, 2013. Disponível em: https://www.direito.ufmg.br/revista/index.php/revista/article/view/P.0304-2340.2013v62p139. Acesso em: 15 abr.2018

FERNANDES, Simone dos Santos Lemos; CALDI, Valeria. Do reflexo do desenvolvimento de novas tecnologias de informação na prática de crimes contra crianças e adolescentes. Crimes cibernéticos. Organizador: Ângelo Roberto Ilha da Silva. Livraria do Advogado. Porto Alegre, 2017

FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. Crimes na internet: elementos para uma reflexão sobre a ética informacional. **Revista CEJ**, v. 7, n. 20, p. 67-73, 2003. Disponível em:

http://www.egov.ufsc.br/portal/conteudo/crimes-na-internet-elementos-para-uma-reflex%C3%A3o-sobre-%C3%A9tica-informacional. Acesso em: 17 mai. 2018.

GREENSTEIN, S. The emergence of the Internet: collective invention and wild ducks. Industrial and Corporate Change, Oxford, v. 19, n. 5, p. 1521-1562, Oct. 2010.

MOWERY, D. C.; SIMCOE, T. Is the Internet a US invention?: an economic and technological history of computer networking. Research Policy, Amsterdam, v. 31, n. 8-9, p. 1369-1387, Dec. 2002.

PECK PINHEIRO, Patrícia. Direito digital. Editora Saraiva, São Paulo 6.ed, 2016

_____. Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil: TIC Domicílios e TIC Empresas 2010. São Paulo: CGI.br, 2011a. 584 p.

PINHEIRO, Emeline Piva. Crimes Virtuais: uma análise da criminalidade informática e da resposta estatal, p. 1-34, 2016. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/emeline.pdf. Acesso em 15 jun.2018.

ROSSINI, Augusto Eduardo de Souza. Brevíssimas considerações sobre delitos informáticos. Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, São Paulo, v. 1, p. 131-142, 2002. http://www.mpsp.mp.br/portal/page/portal/Escola_Superior/Biblioteca/Cadernos_Tematicos/direito_e_internet.pdf. Acesso em: 20 mai.2018.

SIEBER, Ulrich. Limites do direito penal e desafios do novo programa de pesquisa em direito penal no Instituto Max- Planck de Direito Penal Estrangeiro e Internacional. Revista Direito GV**.** São Paulo, p. 269-330, 2008. Disponível em: http://www.scielo.br/pdf/rdgv/v4n1/a12v4n1.pdf. Acesso em: 13 jun. 2018.

SILVA, Evandro Lins e. A globalização e seus meandros. In: ESCRITOS em homenagem a Alberto Silva Franco. São Paulo**:** Revista dos Tribunais, 2003.