CRIMES VIRTUAIS E A LEGISLAÇÃO PENAL BRASILEIRA

*** Gisele Freitas Pacheco**
Advogada. Graduada em Direito pela Faculdade de Direito de Ipatinga

****Renato Lopes Costa**
Advogado, professor de Processo Penal e Direito Penal na Fadipa.

RESUMO

Esta pesquisa teve por objetivo analisar o tratamento que é dado a alguns dos crimes virtuais pela legislação penal vigente. Provando que ela atende a maior parte dos crimes que é praticado através da internet e que só muda o âmbito em que é realizada a conduta ilícita. E mais, aponta as dificuldades enfrentadas para a punição do cibercriminosos. Sendo essa última o maior problema que deve ser confrontado. A pesquisa utilizada foi bibliográfica, na qual procurou-se explicar um problema a partir de pesquisas na internet, doutrinas e jurisprudências. Quanto à metodologia fez-se pelo método dedutivo, justificando-se a escolha por essa opção porque a metodologia escolhida permite a compreensão de questões pontuais partindo de leis gerais. Conclui-se que a legislação nunca conseguirá acompanhar o avanço tecnológico, porém as leis já vigentes ainda servem como base para punir quem infringi-las no meio eletrônico e que os maiores culpados da ocorrência do crime digital é o próprio usuário, por falta de atenção ou conhecimento.

Palavras-chave: Crimes virtuais. Direito Penal. Avanço Tecnológico. Internet.

1 INTRODUÇÃO

A internet está presente na vida da maior parte da população do mundo, concedendo mais facilidades para as pessoas, como no trabalho, na escola, em sites de relacionamentos, no judiciário ou até mesmo nas transações financeiras.

Assim como o cotidiano das pessoas, o direito também é influenciado por essa nova realidade que fora trazida pela evolução da tecnologia de informação.

Não obstante, assim como no mundo real, o virtual também não é isento de pessoas que agem de má fé para práticas delituosas. Além disso, usuários da rede estão sujeitos a ter seu sistema de informação invadido por cibercriminosos que obtém os dados contidos no notebook, tablet, computador ou smartphone em questões de segundos, consequentemente, causando sérios prejuízos que se estendem por anos ou a vida inteira das vítimas, ferindo os direitos individuais tutelados na Constituição Federal.

A grande onda de crimes praticados pela internet e a dificuldade de repressão tem gerado grandes debates na sociedade brasileira. Tendo em vista que com as mudanças advindas com a internet, os criminosos levaram os crimes do mundo real

para o virtual, gerando insegurança para quem utiliza os recursos oferecidos na web. Pois é muita quantidade de denúncias que são feitas, porém existem poucas delegacias especializadas no âmbito Federal para cuidar desses crimes.

Por todo o exposto, este trabalho se organizará em quatro partes, delineadas da seguinte forma.

Para delimitar a história e evolução da internet, um estudo bibliográfico será realizado, focalizando sinteticamente desde o significado da palavra e conceitos jurídicos dado por doutrinadores, passando pelas primeiras ideias para o seu surgimento, o seu ingresso no campo acadêmico, bem como no campo comercial de países estrangeiros até a sua introdução no comércio brasileiro. Essa síntese histórica estará presente na primeira parte do trabalho.

A segunda parte analisará os aspectos legais dos delitos praticados na internet sobre a ótica do direito penal. Iniciando com o histórico do crime digital e seu conceito, logo após fará uma breve consideração sobre os crimes cibernéticos, através de uma pormenorização do tratamento que a legislação penal brasileira dá a esses crimes. Analisará a competência para processar e julgar os crimes da tecnologia de informação.

Na terceira parte serão apresentados alguns dos crimes típicos praticados na web, demonstrando se existe ou não tipificação legal para eles.

Será falado também, na quarta parte sobre as dificuldades encontradas para apurar o crime cuja sua ocorrência se dá no ambiente virtual.

Por fim, na conclusão serão apresentados os resultados decorrentes das análises realizadas em todo conteúdo do trabalho.

2 HISTÓRIA E EVOLUÇÃO DA INTERNET

A palavra internet provém de inter, “entre”, mais a junção da palavra network, que vem do inglês, que significa teia ou entrelaçamento de fios.

Segundo PINHEIRO (2016, p. 89), “a internet é um meio de comunicação eletrônica, formada não apenas por uma rede mundial de computadores, mas, principalmente, por uma rede mundial de indivíduos”.

Durante a Guerra fria, em 1962, os Estados Unidos temendo um possível ataque da Rússia e com o objetivo de facilitar as estratégias na guerra surgiu a ideia

sobre a internet, como uma forma de interligar muitos computadores, permitindo o intercâmbio e o compartilhamento de dados entre eles.

Tal ideia concretizou-se, inicialmente, em uma rede de computadores denominada ARPANET, cuja característica era não possuir um comando central, de modo que se ocorre destruição de um ou mais computadores, todos os outros equipamentos que estavam ligados ao sistema continuariam operando, ou seja, no lugar de um sistema de controle centralizado, a rede operaria como um conjunto de computadores que seriam autônomos e que se comunicaria entre si.

Joseph Licklider, cientista que trabalhou nesse conceito, criou o curioso nome de “rede galáctica” para o mesmo. O coração dessa rede seria uma fonte de comunicação por “pacotes”, concebida pelo britânico Donald Davies, na qual cada informação seria dividida em blocos de tamanho fixo, que seriam enviados ao destinatário. Este último se encarregaria de remontar a mensagem inicial.

Algum tempo depois, em 29 de outubro 1969, a ARPANET, entrou no campo acadêmico através do estabelecimento de conexão da Universidade da Califórnia e o Instituto de Pesquisa de Stanford, momento histórico onde foi dado o primeiro passo para a intercomunicação entre computadores de diferentes universidades.

No fim do ano de 1972, um estudioso conhecido por Ray To Linson desenvolveu o correio eletrônico, hoje popularmente conhecido como e-mail.

> Correio eletrônico ou ainda e-mail ou correio-e é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação. O termo e-mail é aplicado tanto aos sistemas que utilizam a Internet e são baseados no protocolo SMTP, como aqueles sistemas conhecidos como intranets, que permitem a troca de mensagens dentro de uma empresa ou organização e são, normalmente, baseados em protocolos proprietários.

O correio eletrônico inovou e revolucionou mais uma vez este imenso universo virtual, pois ele permitia que seus usuários não só trocassem mensagens, mas também que pudessem armazená-las para consulta posterior. Os primeiros países a utilizarem este mecanismo foram a Inglaterra e a Noruega, que se interligaram na mesma rede, tornando a comunicação por e-mail um fenômeno global.

Desde seu surgimento, portanto, a Internet não parou de evoluir. Nos dizeres de LINS (2015) existem vários autores que apontam, nesse processo, quatro grandes períodos:

> Período do uso privado das redes (em que as conexões eram predominantemente feitas entre computadores de maior porte); b) o período de abertura da rede ao público (caracterizado pelo uso da rede via linha discada e mediante um provedor de acesso); c) período do acesso em banda larga (caracterizado por velocidades cada vez mais elevadas e pela diversificação de conteúdos); e d) período da diversificação de telas (a Internet deixa de ser uma rede que acessamos para se tornar uma rede que nos envolve, pois todo usuário tem a seu dispor formas distintas de buscar seus dados e relacionar-se: o computador, o tablet, o telefone pessoal, a televisão digital, etc.).(LINS, 2015, p. 39)

A partir da década de 90, a Internet tomou um rumo comercial, passando a ser utilizada em grande escala, por milhares de pessoas em todo o mundo. Foi neste mesmo ano em que Tim Bernes-Lee, professor do Instituto de Tecnologia de Massachusetts, cientista da computação e físico britânico, desenvolveu o *browser*[1], a Word Wide Web ou www[2]. Afetando e revolucionando a maneira como a informação é transmitida, bem como o comportamento das pessoas.

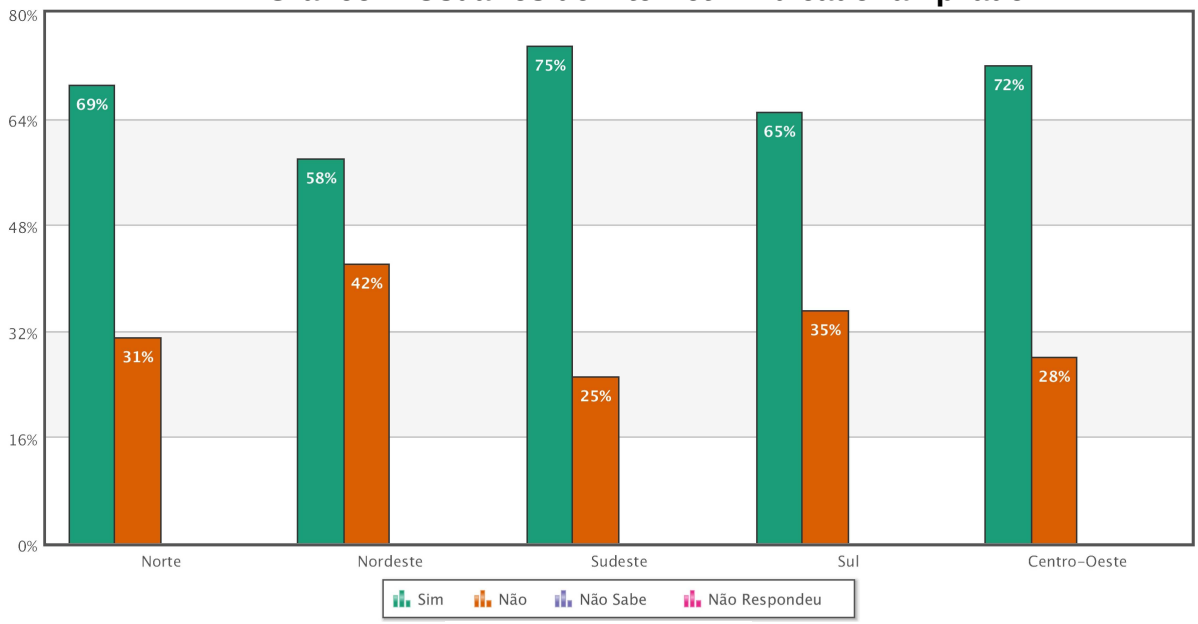
A internet brasileira originou-se com o projeto da RNP, criado em 1989 pelo MCT com apoio de instituições governamentais de vários estados, principalmente a FAPESP. Já a Internet, como rede nacional interconectando diversas redes pelo Brasil, teve início, efetivamente em 1991, com a estruturação da RNP como instituição específica para esse fim e veiculada ao MCT.

Somente em 1995 foi possível, por iniciativa do Ministério das Telecomunicações e do Ministério da Ciência e Tecnologia, a abertura da Internet no setor privado para exploração comercial pela população brasileira. O ambiente virtual no Brasil deixou de ser somente acadêmico e foi disponibilizado para todos, como acontecera em 1994 nos Estados Unidos.

De 95 a 2017 o número de indivíduos conectados à web foi aumentando. Estima-se que no Brasil, 68% da população estão conectados à internet e somente 32% não usufruem da rede, conforme pesquisa divulgada em 05 de setembro deste ano pelo Comitê Gestor de Internet no Brasil (CGI.br) por meio do Centro Regional de Estudos para o Desenvolvimento da Sociedade de Informação (Cetic.br).

[1] *Browser* é um programa utilizado para a navegação na internet.
[2] Word Wide Web em português é conhecida como Rede Mundial de Computadores.

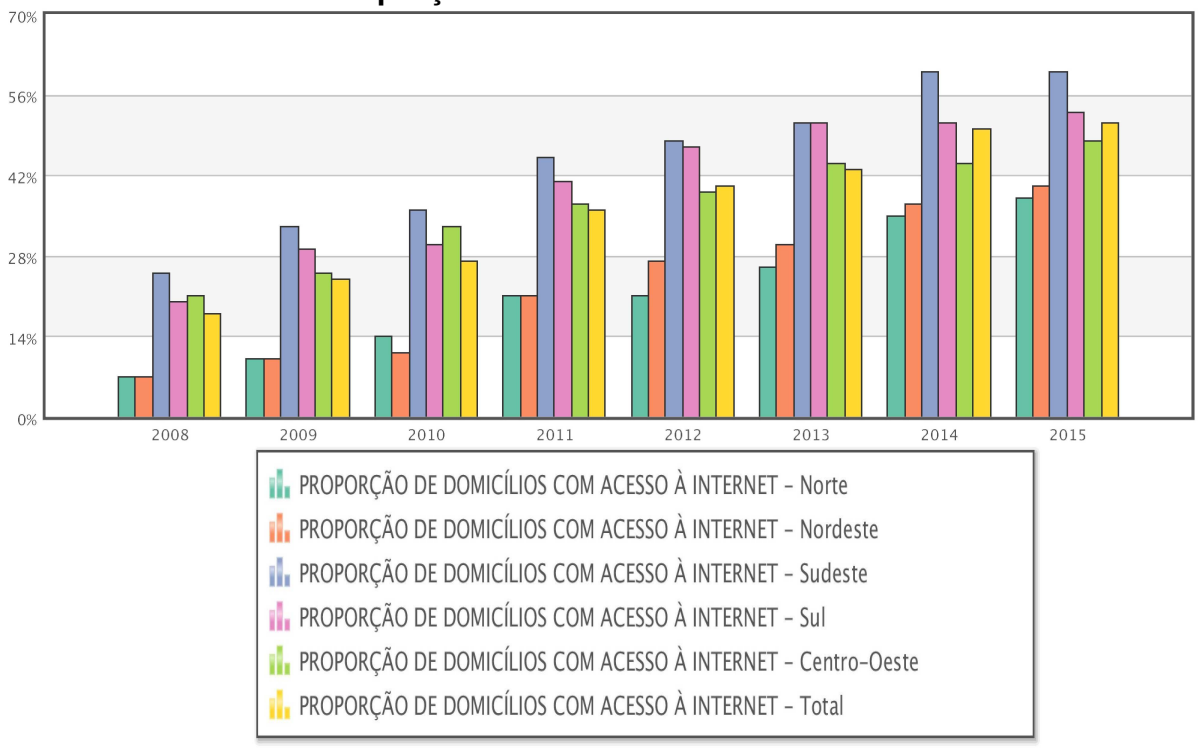
Gráfico 1. Usuários de internet – Indicador ampliado



Fonte: <http://data.cetic.br>

As regiões que mais utilizam desse meio de comunicação, conforme o gráfico acima é a sudeste e a região centro-oeste, ambas com 75% e 72% de usuários respectivamente.

Gráfico 2 - Proporção de domicílios com acesso à internet



Fonte: <http://data.cetic.br>

Além disso, foi publicada outra pesquisa pela CGI no que tange ao crescente número de domicílios com acesso à internet, por região, do ano de 2008 à 2015. Veja o gráfico abaixo:

Os resultados indicam um crescimento deliberado da presença da internet nos domicílios brasileiros. Foram entrevistados mais de 67 bilhões de domicílios pela CGI e o resultado da pesquisa apontou que houve um aumento do quíntuplo de residências com acesso à rede de 2008 a 2015.

Atualmente o Brasil conta com mais de 81.798.000 usuários de internet, conforme dados indicados pela empresa Safer Internet Center do Brasil ou Safernet.

O Brasil ocupa a posição no ranking do 4º país que mais hospeda endereços distintos denunciados. Tal estatística reforça a ideia de que a criminalidade cibernética tende a aumentar em consonância com o avanço da tecnologia de informação.

3 CRIMES VIRTUAIS E O DIREITO PENAL

Nesta parte serão analisados os aspectos legais dos delitos praticados na internet sobre a ótica do direito penal. Iniciando com o histórico do crime digital e seu conceito, logo após fará uma breve consideração sobre os crimes cibernéticos, através de uma pormenorização do tratamento que a legislação penal brasileira dá a esses crimes. Analisará ainda o território e a competência para processar e julgar os crimes da tecnologia de informação.

3.1 Surgimento dos crimes virtuais

A evolução social e tecnologia proporcionou a inovação do crime. A internet nasceu sem ao intuito de se preocupar com o seu uso para a prática de delitos, contudo se tornou o meio utilizado para tanto.

Os primeiros e-crimes surgiram por volta dos anos 60, mas somente começaram a se interessar pela repressão desses delitos nos anos 70. Contudo, somente nos anos 80 a criminalidade cometida na grande rede começou a ser vista como um importante objeto de estudo.

Desde então, começou a ser formada a convicção de que esse aperfeiçoamento de crime não só afetava os setores econômicos e patrimoniais,

mas bem como, outros bens jurídicos tutelados, como a honra e a privacidade. Por força disso, ficou evidente o perigo que a sociedade cibernética poderia trazer às pessoas.

As condutas lesivas naquela época eram mais limitadas, conforme explica PAESANI (2010):

> Inicialmente, as condutas lesivas se limitavam ao acesso abusivo de um computador individual, para retirar dados ou duplicar softwares. Os crimes de computador eram em regra cometidos por empregados de empresas que por sua vez, suportavam as intromissões ilícitas. (PAESANI, 2010, p. 57)

Atualmente os delitos não se limitam apenas na duplicação de dados de softwares[3], mas também em furto de identidade, fraude eletrônica, crimes contra a honra, divulgação de material confidencial, apologia ao crime, estelionato digital, produção ou venda ou posse de pornografia infantil, pedofilia, pirataria, ciberterrorismo, aliciamento e chantagens online, invasão e propagação de vírus e spams[4], disseminação do ódio racial, ameaça, entre vários outros ilícitos penais.

Nesse contexto, o agente criminoso, que pode ser pessoa física ou jurídica, se serve da *Internet* para a prática de novos delitos onde estiver, até mesmo do sofá da sua casa ou de qualquer outro lugar, não medindo esforços algum, bastando que tenha apenas um computador, um conhecimento mediano sobre informática e acesso à web[5], dificulta a identificação do agente delituoso, pois os crimes eletrônicos não respeitam fronteiras.

3.2 Conceito de crimes virtuais

Crimes informáticos podem ser conceituados como a prática de um ilícito no ambiente virtual ou fora dele, por programação ou não, com o objetivo de lesar uma pessoa, sociedade ou seus bens, utilizando-se do ambiente virtual para atingir o fim desejado.

Os crimes cibernéticos dividem-se em puros, mistos e comuns. Porém, ATHENIENSE (2000) trata os cibercrimes como crimes virtuais, fazendo uma diferenciação entre os delitos informáticos, apenas como puros e impuros:

---

[3] É uma série de códigos ou sequência de instruções escritas que serão interpretadas, executadas ou seguidas por um computador a fim que ele execute a tarefa especificada.
[4] O termo Spam é utilizado para designar correio eletrônico não solicitado enviado em massa.
[5] É uma palavra inglesa que significa teia ou rede.

> Entende-se por crimes virtuais qualquer ação em que o computador seja o instrumento ou o objeto do delito, ou então, qualquer delito ligado ao tratamento automático de dados. Distinguem-se os crimes virtuais entre delitos informáticos impuros, aqueles que podem ser cometidos também fora do universo do computador, encontrando já definição no sistema punitivo atual, e os delitos informáticos puros, ou seja, aqueles que só podem ser concebidos em face de um sistema informático, ainda não tipificado na legislação brasileiro.

Contudo FIORILLO (2013) aprofunda mais essa divisão:

> 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. Em contrapartida, podem ser considerados crimes virtuais mistos aqueles em que o uso de meios computacionais é condição necessária para a efetivação da conduta, embora o bem jurídico visado seja diverso do informático. Por fim, o crime virtual comum seria aquele em que se utiliza da Internet apenas como instrumento para a realização do delito já tipificado pela lei penal. (FIORILLO, 2013, p. 167)

Evidencia-se que, a partir desses enfoques, o crime digital impuro ou impróprio é a utilização do ambiente virtual como um meio para executar o delito, ou seja, o alvo não é o meio virtual ou eletrônico em si, mas uma pessoa, retirar dinheiro de uma conta bancária, fraudar dados, entre outros. O que não acontece no crime digital puro ou próprio, neste o criminoso tem o escopo de causar dano à máquina, ambiente virtual ou até mesmo invadir o sistema de uma determinada pessoa, seja ela física ou jurídica, sem autorização deste e não levando nenhum tipo de informação dali.

A expressão crimes virtuais não é adotada de maneira uniforme pela doutrina, podendo ser encontrada como crimes informáticos, crimes da era da informação, crimes mediante computadores, cibercrimes, crimes de computador, crimes eletrônicos, crimes tecnológicos, crimes digitais, crimes high-tech, tecnocrimes, netcrimes, crimes virtuais, crimes da tecnologia da informação e até mesmo e-crimes.

AZEVEDO (2011) conceitua o referido tema como:

> O fato consistente na prática de ilícito contra uma pessoa ou sociedade, mediante o uso da internet, passível de enquadramento nas leis penais brasileiras, para fins de punição efetiva, ou seja, aquele que sai do virtual e entra na realidade de todos. (AZEVEDO, 2011, p. 342)

De uma forma mais aprofundada Rossini acrescenta o conceito de delitos informáticos da seguinte maneira:

> O conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade. (ROSSINI, 2004, p. 67)

3.3 Legislação penal brasileira no tocante aos crimes virtuais

No Brasil, antes de 2012 não havia legislação especifica para a tipificação dos crimes informáticos. Os operadores do direito utilizavam de normas já existentes para suprir as lacunas da lei. Contudo, era necessária uma legislação específica para coibir esses delitos, pois os legisladores de 1940 não imaginavam que os crimes iriam evoluir a esse ponto. Nos dizeres de MASSON (2016):

> É inegável que leis editadas décadas atrás, nas quais sequer se pensava na existência de computadores, levavam a malabarismos adaptativos dos operadores do Direito para enfrentar novos comportamentos, muitas vezes resultando na impunidade dos criminosos. Era preciso adaptar a legislação penal aos novos tempos. (MASSON, 2016, p. 276)

Em 1996 foi posta em vigor a lei que regulamentou o art. 5º, XII, da Constituição Federal, o qual assegura a inviolabilidade das comunicações. De fato, o art. 10 a Lei nº 9.296 significou um grande passo para a cidadania, estabelecendo pena de até 4 anos de reclusão, e multa, no caso de o indivíduo "realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei".

O Deputado Federal Luiz Piauhylino, autor do PL nº 84/99, trabalhou em conjunto com outros Deputados Federais[6], há mais de 10 anos para a aprovação do projeto de Lei que posteriormente se transformou na lei 12.737/2012.

Ocorre que depois de intensos debates a respeito da criação de leis que cuidassem dos crimes cometidos na internet, e o impulso da opinião pública sobre a atividade dos congressistas em maio de 2012, logo após a invasão do computador

[6] Trabalhou inclusive com Eduardo Azeredo, relator no Senado do PLC 89/03 que inicialmente foi o PL nº 84/99.

pessoal da atriz Carolina Dieckmann, onde 36 fotos íntimas da atriz foram subtraídas por cinco homens, posteriormente identificados e responsabilizados pelos crimes de extorsão, difamação e furto, mas não pela invasão do computador, em face da falta de legislação que cuidasse dos crimes cometidos.

Finalmente, os legisladores aprovaram a da Lei 12.737/2012, conhecida como Lei Carolina Dieckmann.

Segundo NUCCI citado por SANCHES (2016), mostra a relevância da criação da figura típica incriminadora através da Lei mencionada:

> Sabe-se, por certo, constituir a comunicação telemática o atual meio mais difundido de transmissão de mensagens de roda a ordem entre pessoas físicas e jurídicas. O e-mail tornou-se uma forma padrão de enviar informes e mensagens profissionais e particulares, seja para fins comerciais, seja para outras finalidades das mais diversas possíveis. *As* redes sociais criaram, também, mecanismos de comunicação, com dispositivos próprios de transmissão de mensagens. Torna-se cada vez mais rara a utilização de cartas e outras bases físicas, suportando escritos, para a comunicação de dados e informes. Diante disso, criou-se novel figura típica incriminadora, buscando punir quem viole não apenas a comunicação telemática, mas também *os* dispositivos informáticos, que mantém dados relevantes do seu proprietário. (SANCHES, 2016, p. 774-775)

Contudo há debates de doutrinadores a respeito da Lei, pois alegam que o tipo penal “violação indevida de mecanismo de segurança” está em aberto. Nesse sentido, explica BITENCOURT (2013):

> Assim, o tipo penal é aberto e exige um juízo de valor para complementar a análise da tipicidade. Aliás, é um tipo semiaberto, ou seja, nem aberto nem fechado, pois ao mesmo tempo que abre com a locução “mediante violação indevida’, fecha com a complementação. “de mecanismo de segurança”, limitando, portanto, o âmbito da violação. Em outros termos, qualquer outra violação que não se refira a “mecanismo de segurança, não tipificará a conduta descrita no caput que ora examinamos. Ou, dito de outra forma, ainda que haja a violação ou invasão “de dispositivo informático alheio, conectado ou não à rede de computadores”, se não houver “mecanismo de segurança” (ou caso haja, não estando acionado) que seja violado, a conduta não se adequará a esta descrição típica. Poderá, eventualmente, adequar-se a outro dispositivo penal, mas não a este, sob pena de violar-se a tipicidade estrita. (BITECOURT, 2013, p. 344)

Nucci *apud* Bitencourt (2016) explica que esta modalidade de conduta não possui nenhum sujeito passivo, portanto o interesse punitivo do estado volta à sociedade sem lhe dar proteção alguma, notoriamente se tratando, portanto, de crime vago. Veja-se:

> Nucci, não sem razão, alerta que esta modalidade de conduta não possui nenhum sujeito passivo determinado. Afinal, consiste na preparação do delito do *caput.* Diante disso o interesse punitivo estatal, nesta hipótese, volta-se à proteção da sociedade, em nítido crime vago. Ora, se o sujeito passivo, na realidade, é a sociedade, este delito poderá não ser autonomamente punido, pois o art. 154-8 seja a ação penal pública condicionada à representação da vítima, salvo se o crime for cometido contra a administração direta ou indireta. (BITECOURT, 2013, p. 346)

Do ponto de vista de SOPRANA (2016), a Constituição não pune o indivíduo que acessa um celular ou uma rede Wi-Fi sem autorização. Ele pune somente quem entra em um sistema alheio com o fim de causar danos, seja ao alterar e destruir dados ou a instalar qualquer tipo de vulnerabilidade. Caso uma pessoa jogue em um computador, abra as pastas, olhe as fotos, mas não modifique nada, ela não será punida pela legislação atual.

Em contrapartida, PINHEIRO (2016, p. 259) ensina que "Legislar sobre a matéria de crimes na era Digital é extremamente difícil e delicado. Isso porque sem a devida redação do novo tipo penal corre-se o risco de se acabar punindo o inocente".

Buscando elucidar questões como princípios, garantia da proteção dos dados pessoais e privacidade dos usuários, direitos e deveres para quem utiliza a internet, bem como traçar diretrizes para a atuação do Estado, foi criado a Lei nº 12.965/14[7].

O projeto do Marco Civil da Internet surgiu no ano de 2007 para regular o uso da internet no Brasil, devendo conceder garantias, deveres, direitos para quem utiliza a internet. Além de dar diretriz para a atuação do Estado e de trazer definições próprias no que tange ao Sistema de Informações.

Em 23 de abril de 2014, sete anos depois, o projeto foi aprovado pelo Senado Federal e logo após pelo presidente da República. Passando a ser conhecido legalmente pela Lei nº 12.965/14.

Além disso, a lei trata de temas como a neutralidade na rede, privacidade, retenção de dados, a função social da internet, liberdade de expressão, responsabilidade civil dos provedores e usuários e transmissão de conhecimento.

O Marco Civil da Internet no Brasil cumpriu um papel fundamental para a legislação brasileira, pois trouxe um grande amadurecimento sobre questões que eram de grande desafio para o judiciário. Trazendo soluções adequadas para a nova realidade enfrentada nos casos concertos. Um exemplo é a previsão de abrangência

[7] A Lei nº 12. 965/14 é conhecida como a Lei do Marco Civil da Internet no Brasil.

para o âmbito internacional, visto que o marco civil alcança empresas não só dentro do Brasil, mas também fora dele.

3.4 Competência para processar e julgar os crimes virtuais

No âmbito do Processo Penal é necessário definir a competência para processar e julgar os delitos informáticos para a aplicação da lei, haja vista que o ambiente virtual interage em diversos países, abrangendo todo o território virtual, não sendo passível de delimitações físicas.

Conforme o entendimento de TÁVORA "a competência passa a ser um critério legal de administração eficiente da atividade dos órgãos jurisdicionais, definindo previamente a margem de atuação de cada um, isto é, externando os limites de poder" (TÁVORA, 2017, p. 387).

No caso em questão os principais aspectos da competência material que devem ser analisados são *ratione materiae*[8] e *ratione loci*[9], conforme o artigo 69 do CPP "determinará a competência jurisdicional: I - o lugar da infração: II - o domicílio ou residência do réu e a III - a natureza da infração.".

A justiça estadual é residual, sendo competente para apreciar, todas as matérias que não sejam da alçada da justiça comum federal ou especializada.

Em contrapartida, os critérios para a fixação da justiça federal têm o domínio mais restrito, pois só poderá haver a deslocação de um processo da justiça estadual para federal nos casos em que envolver grave violação dos direitos humanos, de previsão constitucional e em face de tratados e convenções em que o Brasil subscreveu. É o que diz o artigo 109 da CF/88:

> Aos juízes federais compete processar e julgar: I - as causas em que a União, entidade autárquica ou empresa pública federal forem interessadas na condição de autoras, rés, assistentes ou oponentes, exceto as de falência, as de acidentes de trabalho e as sujeitas à Justiça Eleitoral e à Justiça do Trabalho; II - as causas entre Estado estrangeiro ou organismo internacional e Município ou pessoa domiciliada ou residente no País; III - as causas fundadas em tratado ou contrato da União com Estado estrangeiro ou organismo internacional; IV - os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral; V - os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro,

[8] Visa identificar qual a justiça competente, se a justiça comum ou a justiça especializada.
[9] Visa identificar o juízo territorialmente competente.

> ou reciprocamente; V-A as causas relativas a direitos humanos a que se refere o § 5º deste artigo; VI - os crimes contra a organização do trabalho e, nos casos determinados por lei, contra o sistema financeiro e a ordem econômico-financeira; VII - os habeas corpus, em matéria criminal de sua competência ou quando o constrangimento provier de autoridade cujos atos não estejam diretamente sujeitos a outra jurisdição; VIII - os mandados de segurança e os habeas data contra ato de autoridade federal, excetuados os casos de competência dos tribunais federais; IX - os crimes cometidos a bordo de navios ou aeronaves, ressalvada a competência da Justiça Militar; X - os crimes de ingresso ou permanência irregular de estrangeiro, a execução de carta rogatória, após o "exequatur", e de sentença estrangeira, após a homologação, as causas referentes à nacionalidade, inclusive a respectiva opção, e à naturalização; XI - a disputa sobre direitos indígenas. (...) § 5º Nas hipóteses de grave violação de direitos humanos, o Procurador-Geral da República, com a finalidade de assegurar o cumprimento de obrigações decorrentes de tratados internacionais de direitos humanos dos quais o Brasil seja parte, poderá suscitar, perante o Superior Tribunal de Justiça, em qualquer fase do inquérito ou processo, incidente de deslocamento de competência para a Justiça Federal.

Portanto não é pelo simples fato de um crime ser cometido pela internet que por si só atrairá a competência da justiça federal para processar e julgar tal delito.

O artigo 70, do CPP diz que “a competência será, de regra, determinada pelo lugar em que se consumar[10] a infração, ou, no caso de tentativa[11], pelo lugar e que for praticado o último ato de execução”.

Em decorrência disso, tem-se como juízo territorialmente competente o do local onde operou a consumação do delito, pois o CPP adota a teoria do resultado para definir tal alçada. o renomado doutrinador Nestor Távora explica que a “teoria do resultado ganha relevância nos delitos plurilocais, que são aqueles onde os atos executórios ocorrem em local distinto do resultado, sempre dentro do território nacional.” (TÁVORA, 2017, p. 389)

Ainda segundo TÁVORA (2017, p. 393) o direito brasileiro com o objetivo de adequar as normas processuais penais à moderna criminalidade, o STJ firmou entendimento de que o juízo competente para processar e julgar o crime de furto mediante a fraude na internet, ambiente no qual ocorreu os saques indevidos na conta da vítima, será a autoridade jurisdicional do local onde se situa a conta fraudada, por aplicação do art.70, do CPP.

Em concordância com jurisprudência do STJ, os crimes contra honra, perpetrados por meio eletrônico, seja em chats, sites de relacionamentos, até

---

[10] Crime consumado pode ser entendido como aquele em que há a reunião de todos os elementos de sua definição legal.

[11] Considera-se como tentativa os atos iniciais executórios que não se consumam por circunstâncias alheias à vontade do agente.

mesmo em redes sociais cuja sede seja no exterior, será competente para processar e julgar o juiz de direito da Justiça Estadual. Nesse sentido, a referida decisão, publicado no Diário da Justiça eletrônico, da Terceira Seção do Superior Tribunal de Justiça[12]:

> CONFLITO NEGATIVO DE COMPETÊNCIA. CRIME DE INJÚRIA PRATICADO POR MEIO DA INTERNET, NAS REDES SOCIAIS DENOMINADAS ORKUT E TWITTER. AUSÊNCIA DAS HIPÓTESES DO ART. 109, INCISOS IV E V, DA CF. OFENSAS DE CARÁTER EXCLUSIVAMENTE PESSOAL. COMPETÊNCIA DA JUSTIÇA ESTADUAL. 1 - O simples fato de o suposto delito ter sido cometido por meio da rede mundial de computadores, ainda que em páginas eletrônicas internacionais, tais como as redes sociais "Orkut" e "Twitter", não atrai, por si só, a competência da Justiça Federal. 2 - É preciso que o crime ofenda a bens, serviços ou interesses da União ou esteja previsto em tratado ou convenção internacional em que o Brasil se comprometeu a combater, como por exemplo, mensagens que veiculassem pornografia infantil, racismo, xenofobia, dentre outros, conforme preceitua o art. 109, incisos IV e V, da Constituição Federal. 3 - Verificando-se que as ofensas possuem caráter exclusivamente pessoal, as quais foram praticadas pela ex-namorada da vítima, não se subsumindo, portanto, a ação delituosa a nenhuma das hipóteses do dispositivo constitucional, a competência para processar e julgar o feito será da Justiça Estadual. 4 - Conflito conhecido para declarar a competência do Juízo de Direito do Juizado Especial Cível e Criminal de São Cristóvão/SE, o suscitado. (CC 121.431/SE, Rel. Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA SEÇÃO, julgado em 11/04/2012, DJe 07/05/2012)

Entendeu-se que não houve violação do inciso IV do art. 109 da CF e tampouco do inciso V do mesmo diploma legal, tendo em vista que o crime de injúria não está previsto em tratados ou convenções internacionais que o Brasil se comprometeu a defender.

O órgão brasileiro competente para julgar as infrações praticadas por estrangeiro que reside no Brasil será a capital do estado em que por último residiu, porém ele nunca houver residido no Brasil, será a capital da República, nos termos do artigo 88, do Código de Processo Penal.

Com o crescimento da utilização de computadores e do uso da internet, a criminalidade informática elevou os índices de pessoas vítimas de fraudes, crimes contra a honra, racismo, a propagação da pornografia infantil, dentre outros delitos.

Com essa grande e notória mudança social causada pela globalização da internet que trouxe nova forma de comunicação e modificou as relações sociais em todo o mundo, contudo, junto com tais benefícios surgiram também novos riscos,

[12] STJ – Terceira Seção – CC 121096/PR – Min. Alderita Ramos de Oliveira (des.Convocada) – Dje 8/09/2012.

impondo a necessidade do controle jurídico. A dinâmica e versatilidade, inerentes à internet, tornaram-se foco de preocupação para o poder legislativo que editou as Leis nº 12.735/12 e nº 12.737/12[13] e nº 12.965/14.

Quanto à competência para o processamento dos crimes praticados pela internet, algumas questões devem ser levadas em conta, como o local de transmissão e a existência ou não da transnacionalidade do delito.

O Supremo Tribunal Federal, no julgamento do Recurso Extraordinário nº 628624, decidiu, por maioria de votos, que a competência para processar e julgar o delito de publicação, na internet, de imagens com conteúdo pornográfico envolvendo crianças e/ou adolescentes é da Justiça Federal.

No julgamento, foi aprovada a seguinte tese: "Compete à Justiça Federal processar e julgar os crimes consistentes em disponibilizar ou adquirir material pornográfico envolvendo criança ou adolescente quando praticados por meio da rede mundial de computadores".

4 CRIMES VIRTUAIS

Na sociedade atual tem-se a ideia que na internet tudo pode ser realizado, pois não haverá qualquer espécie de punição, porém é um grande equívoco pensar dessa maneira, pois a maior parte dos crimes que ocorrem no ambiente digital é passível de punição. Independentemente da forma utilizada para praticar o crime.

A legislação penal em vigor sempre possuir meios para combater a maioria dos crimes digitais. O nobre doutrinador Cleber Masson, expressa que "ao contrário das vozes lançadas pela opinião popular, a *internet* nunca foi um território livre, sem lei e sem punição". (MASSON, 2016, p, 276)

Mister se faz ressaltar que os crimes digitais são mais amplos que os eletrônicos, pois no primeiro caso abrange tanto a utilização do ambiente virtual como o meio quanto para o atingir o fim almejado.

É bem verdade que os ataques na internet podem ocorrer com o emprego de técnicas diversificadas, visando alvos diferentes e por inúmeros objetivos. Pois a internet não só cria a oportunidade para o cometimento de novos delitos, mas também, potencializas os crimes já existentes.

[13] A Lei Carolina Dieckman altera os art. 154, 266 e 298 do CP.

As razões que motivam os cibe criminosos a esses ataques, consoante com publicação dada pela CERT.br, varia de uma mera diversão até a concretização de atos criminosos, como será exposto a seguir:

> a) Demonstração de poder: mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente. b) Prestígio: vangloriar-se, perante outros atacantes, por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar *sites* considerados visados ou difíceis de serem atacados; disputar com outros atacantes ou grupos de atacantes para revelar quem consegue realizar o maior número de ataques ou ser o primeiro a conseguir atingir um determinado alvo. c) Motivações financeiras: coletar e utilizar informações confidenciais de usuários para aplicar golpes. d) Motivações ideológicas: tornar inacessível ou invadir *sites* que divulguem conteúdo contrário à opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia. e) Motivações comerciais: tornar inacessível ou invadir *sites* e computadores de empresas concorrentes, para tentar impedir o acesso dos clientes ou comprometer a reputação destas empresas.

Ao passo que, para chegar ao fim almejado, os cibercriminosos usufruem de táticas como, exploração de vulnerabilidade[14], varredura em redes[15], falsificação de e-mail[16], interceptação de tráfego[17], força bruta[18], desfiguração de página[19], negação de serviço[20], dentre outras formas citadas pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.

É sabido que legislar sobre o direito eletrônico é muito delicado, uma vez que se não houver uma devida redação do tipo penal é bem provável que possa punir uma pessoa inocente. Além disso, sabe-se que as testemunhas dos crimes digitais são as próprias máquinas e elas não sabem diferenciar um crime praticado com dolo

---

[14] É definida pelo CERT como uma condição que, quando explorada por um cibercriminoso, pode resultar em uma violação de segurança.

[15] Varredura em redes ou *scan*, conforme o CERT, é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles.

[16] Falsificação de *e-mail*, ou *e-mail spoofing*, é uma técnica que consiste em alterar campos do cabeçalho de um *e-mail*, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra. Definição do CERT.

[17] Um ataque de força bruta, ou *brute force*, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar *sites*, computadores e serviços em nome e com os mesmos privilégios deste usuário. Conforme definição do CERT.

[18] Conforme definição do CERT, um ataque de força bruta, ou *brute force*, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar *sites*, computadores e serviços em nome e com os mesmos privilégios deste usuário.

[19] Desfiguração de página, *defacement* ou pichação, conforme definição do CERT, é uma técnica que consiste em alterar o conteúdo da página *Web* de um *site*

[20] Negação de serviço, ou DoS (*Denial of Service*), é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Conforme definição do CERT.

de um praticado com culpa, em outras palavras, os computadores não sabem informar sobre o contexto da situação. O que acaba levando a punição indevida do agente.

Aliás, é recorrente a quantidade de computadores que são infectados e se tornam máquinas “zumbi”, sendo controlados remotamente por terceiros, no qual enviam e-mail com arquivos maliciosos para outros usuários e infectando suas máquinas.

4.1 Crimes virtuais típicos da era da tecnologia da informação

Através de uma abordagem clara será desenvolvido nos próximos subtópicos, os tipos de crimes digitais mais recorrentes no meio virtual, as suas peculiaridades e a sanção que será definida pela legislação penal, uma vez que a maioria desses crimes não estão previstos no Código Penal, mudando apenas o ambiente onde é realizado o crime.

4.1.1 Ciberbullying

Ciberbulling originou-se da palavra bullying cujo termo é utilizado para descrever atos de violência física ou psicológica intencional e repetida, praticada por um indivíduo ou grupo de indivíduos, causando dor e angústia e sendo executadas dentro de uma relação desigual de poder.

Para SILVA (2010) ciberbullying trata-se da migração para o meio virtual de atitudes de violência psicológica, com o cunho intencional e repetitivo, praticado por um ou mais agressores contra uma ou mais vítimas que se encontram impossibilitadas de se defender.

Os tipos mais recorrentes são as ofensas pessoais por meio do Facebook e a intimidação, humilhação, envio de fotos adulteradas e postadas nas redes sociais e mensagens que abalam o psicológico da vítima, porém nada impede que isso evolua para ameaças contra a vida, disseminação de ódio racial e outros. O que essas atitudes causam é imensurável, podendo levar a vítima a uma depressão profunda e até os casos mais extremos como o suicídio.

Na atual legislação penal brasileira não existe tipificação especifica para essa conduta, de maneira que a sanção é aplicada com a utilização dos artigos de delitos contra a honra e de ameaça.

As principais vítimas estão entre as crianças e adolescentes e normalmente ocorre em ambiente escolar, mas também pode ocorrer fora dele.

Normalmente essas crianças ou adolescentes criam um perfil falso em alguma rede social para praticar o crime, onde eles postam fotos adulteradas, mensagens vexatórias e de intimidação à vítima.

4.1.2 Crimes contra a honra: injúria qualificada e difamação

Os criminosos impulsionados pela possibilidade do uso da internet por anonimato proferem palavras injuriosas ou de cunho difamatório, ofendendo a honra subjetiva e/ou objetiva da vítima.

A injúria qualificada ou racial difere-se do crime de difamação, enquanto uma atinge a honra subjetiva da vítima a outra fere a honra objetiva. Nos dizeres do Ministro Marco Aurélio *apud* MASSON (2016, p.189) “a difamação pressupõe atribuir a outrem fato determinado ofensivo à reputação. Na injúria, tem-se veiculação capaz de, sem especificidade maior, implicar ofensa à dignidade ou ao decoro.”

São várias as ocorrências dos delitos contra a honra reportados na internet. Há exemplo do ilícito da injúria racial, cometido no ambiente eletrônico, é o caso da atriz Thais Araújo, que ocorreu em setembro de 2015. A atriz postou uma foto da sua própria imagem no Facebook e em menos de uma hora um grupo de haters[21] escreveram vários comentários maldosos que criticavam o cabelo da atriz. Veja:

[21] É um termo usado para pessoas que proferem comentários de ódio nas redes sociais.

Figura 1: Comentários racista contra Thais Araújo

Fonte: <extra.globo.com>

Outra famosa que recorrentemente sofre ataques de haters na internet é Titi, filha de Bruno Gagliasso e Gio Ewbank. Um deles ocorreu em 10 de novembro de 2016, onde uma internauta fez um comentário em uma foto que ambos postaram com a filha dizendo que a garota não combina com os pais e que eles deveriam devolvê-la para África, pois o lugar dela seria lá. Além de dizer que deveriam adotar uma criança que “parece” com eles, dos olhos claro e loiro. Observe:

Figura 2: Injúria racial contra filha de Giovanna Ewbak

Fonte: <observatoriodatelevisao.bol.uol.com.br>

A injúria qualificada está prevista no art. 140, §1º do Código Penal, punida com pena de reclusão, de um a três anos, sem qualquer prejuízo de multa. Embora seja uma pena inferior àquela cominada no *caput* do artigo é plenamente constitucional, encontrando seu fundamento de validade na dignidade da pessoa humana.

Vê-se a necessidade de informar que a Lei 9.459/97 modificou o art. 140 do Código Penal, acrescentando-lhe o § 3o, que prevê a injúria qualificada pelos elementos de raça, cor, etnia, religião e origem, dando-lhe a mesma pena do crime do artigo 20, *caput*, da lei especial 7.716/89.

Esse tipo de ilícito reclama que a ofensa seja dirigida à pessoa ou pessoas determinadas e não para algum grupo ou pessoas indeterminadas, como ocorre no racismo.

Dessa forma, para que ocorra a injúria racial é imprescindível, além do quesito pessoal, a atribuição de qualidade negativa à vítima firmada em elementos que remetem a sua raça, cor, etnia, cultura, religião ou origem.

Cabe ressaltar, que o delito explanado é afiançável e prescritível, além se estar previsto no código penal, diferente do racismo que se encontra na legislação especial, qual seja, Lei 7.716/1989.

No que tange à difamação, delito este que tem previsão no artigo 139 do Código Penal, é constituído quando o indivíduo ofende a honra objetiva da vítima imputando-lhe fato ofensivo à sua reputação.

Ademais, não é necessário que seja verdadeira a imputação, tendo em vista que subsiste o crime, desde que o objetivo seja de ofender a vítima. O legislador, buscando elucidar esse tema, ao tipificar o crime de difamação, deixou nítido que as pessoas não podem fazer comentários maldosos sobre a vida alheia, pois não lhe diz respeito.

4.1.3 Racismo

Em um país onde impera uma grande diversidade de raças, pessoas de várias cores e traços, como é no Brasil, não deveria ser “normal” a ocorrência do racismo. O delito está presente no rol dos crimes que mais ocorrem no país atualmente. Tanto com os famosos quanto com os anônimos, pode se ler ou ouvir palavras, cujo conteúdo é racista, sendo proferidas contra certas pessoas.

Como já foi explanado anteriormente, muitos imaginam que ao adentrar na rede, tudo pode ser feito ou dito, pois não haverá consequência alguma para o comportamento adotado. A internet cria no indivíduo uma sensação de impunidade, pensar dessa forma equivocada e agir criminosamente trarão consequências sim, seja na esfera civil ou penal.

Um exemplo que pode ser apontado é o da estudante de direito do estado de São Paulo, Mayara Petruso, que usou a sua conta no Twitter e Facebook, após a derrota do candidato às eleições presidenciais, José Serra, no ano de 2010, para exprimir ofensas aos nordestinos, dizendo que não são pessoas e que deveriam ser mortos por meio de afogamento. Veja:

Figura 3: Tuites com conteúdo racista de Mayara

Fonte: <idgnow.com.br>

Para o renomado doutrinador Cleber Masson o racismo “é a divisão dos seres humanos em raças, superiores ou inferiores, resultante de um processo de conteúdo meramente político-social” (MASSON, 2016, p. 192). Dessa divisão gera a atitude perversa de discriminação e preconceito entre indivíduos de um mesmo país, estado ou cidade.

A CFRB/88 não faz diferenciação entre os seres humanos, pois todos são iguais, sem qualquer distinção. Garantindo a todos os brasileiros ou estrangeiros que residam no país o direito à vida, liberdade, igualdade, segurança entre outros direitos previstos no Título II do diploma legal acima referido.

É possível afirmar que a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, disposto expressamente no artigo 5º, XLII, da Constituição Federal/88. Tendo em vista que todos os seres humanos são iguais, perante a lei e perante a ciência, o que já foi comprovado através do mapeamento do genoma humano[22].

[22] Mapeamento do genoma humano significa a localização dos genes nos cromossomos e o conhecimento das distâncias físicas e genéticas que os separam, bem como o sequenciamento do

Nos dizeres de Masson “não há diferença biológica entre os seres humanos, quer na essência, biológica ou constitucional (art. 5.º, *caput*), são todos iguais.”(MASSON, 2016, p 192)

Ressalta-se que os crimes de racismos estão previstos em Lei especial, qual seja, 7.716/1989, que tipificou o racismo como crime e não mais como contravenção penal, muito embora, na redação original, não tenha inovado nas hipóteses delituosas, penalizando apenas as condutas preconceituosas por raça ou cor. Só em 1997, com a Lei 9.459, foram acrescidas ao texto legal as hipóteses de discriminação ou preconceito por etnia, religião ou procedência nacional, aumentando a pena para 1 a 3 anos. Atualmente existem várias situações às quais podem ser arroladas, tais como manifestações preconceituosas generalizadas, atingindo uma coletividade ou por segregação racial.

Algum tempo depois, o artigo 20 da Lei 7.716/89 foi alterado pela Lei 12.228/10, que incluiu no § 3º a possibilidade de interdição das respectivas mensagens ou páginas de informação na rede mundial de computadores. Passando a vigorar da seguinte forma:

> Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.
> (...)
> § 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza:
> § 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.

Resta observar que o referido artigo é, atualmente, o principal dispositivo para tipificação dos crimes de racismos executados através da internet. Deixando nítido que qualquer crime dessa natureza, se praticado por intermédio dos meios de comunicações sociais, incluindo a internet, ou de publicação de qualquer natureza sofrerá as sanções dos respectivos parágrafos do artigo 20 da Lei que criminaliza o racismo.

DNA de cada cromossomo. Os dois principais tipos de mapas do genoma humano são o genético e o físico.

4.1.4 Pedofilia e pornografia infantil

Nos últimos anos é impossível não associar pedofilia com internet. Existe verossimilhança nas possibilidades novas de obter prazer e saciar os desejos através do mundo virtual. Nessa perspectiva, houve maior divulgação e expansão da prática da pedofilia, pela facilidade de transmissão de informações.

Consoante com Ramalho, a pornografia infantil "atualmente é disseminada de forma rápida e barata através da internet, alcançando diversas pessoas que antes precisariam de meios analógicos para comercialização de vídeos e fotos com crianças praticando atos sexuais"(RAMALHO 2016, p. 28-35).

É de suma importância dizer que, a legislação brasileira só punirá a exteriorização de atos de pedofilia, que atentam contra a dignidade sexual da criança ou adolescente, no entanto, se o pedófilo apenas nutrir desejos sexuais por estes, não poderá sofrer as sanções, uma vez que o Direito Penal não tem o condão de restringir os atos internos, da mente do sujeito, pois a princípio, não configura um fato típico e antijurídico pela lei, sendo, portanto irrelevante para o direito.

De acordo com dados divulgados da Jornada Estadual contra Violência e a Exploração Sexual de Crianças e Adolescentes, constatou que só no Rio Grande do Sul havia uma média, no início de 2013, de 10 casos por dia de menores que sofriam abuso ou exploração sexual.

Outro relato que evidencia uma situação extremamente alarmante, são os dados divulgados pela empresa Safernet, que em 11 anos, a Central de Denúncias de Crimes Cibernéticos recebeu e processou 1.518.617 de denúncias anônimas de pornografia infantil envolvendo 312.037 URLs[23] distintas, das quais 119.623 foram removidas, conectados à internet através de 42.188 números de IPs[24] distintos em todo o mundo.

Somente no Brasil, no ano de 2016, foram reportados mais de 280 casos de pornografia infantil. Em virtude dessas considerações, na internet há uma verdadeira rede organizada, com grupos espalhados em todos os lugares e de pessoas interessadas em obter acesso a imagens obscenas com menores. É bem verdade que a questão da pedofilia na internet é bem mais grave do que se pode

[23] É uma palavra inglesa cujo significado é localizador uniforme de recursos, referente ao endereço de rede onde se encontra um recurso informático.
[24] É a identificação de um dispositivo informático.

imaginar, apesar de haver no Brasil grandes esforços para combater tais crimes, ainda é muito difícil conte-los.

Segundo o Estatuto da Criança e do Adolescente entende-se como criança o indivíduo que tiver de 0 a 12 anos de idade completos; já adolescentes, dos 12 aos 18 anos incompletos.

Os artigos 240 e 241 do ECA passaram a tratar da comercialização e produção de materiais pedófilos e pornográficos desde 2008, com a alteração trazida pela Lei 11.829, que expandiu o seu núcleo, abrangendo conteúdos com imagens que expõem abuso infanto-juvenil

De modo geral, tais artigos criminalizam os indivíduos quem oferecem, trocam, disponibilizam, divulgam, vendem, expõem, produz, reproduz, alicia, assedia, facilita, induz o acesso, adquiri, possui, armazena, simula materiais pornográficos, seja de qualquer espécie e por qualquer meio, envolvendo crianças ou adolescentes.

Após o reconhecimento em Repercussão Geral pelo STF no RE 628624, a conduta de divulgar imagens, vídeos pornográficos de criança na internet atrairá a competência da justiça federal, uma vez que qualquer pessoa de qualquer lugar do mundo poderá ter acesso a essas imagens ou vídeos, ultrapassando as barreiras nacionais. Além de estar em consonância com o artigo 109, inciso V, da CF, sendo um dos crimes que o Brasil se comprometeu a combater em 1990, através da Convenção Internacional sobre Direitos da Criança, adotado pela Assembleia Geral das Nações Unidas, aprovada pelo Decreto legislativo 28/90 e pelo Decreto 99.710/90. Além disso, a competência territorial será da seção judiciária onde ocorreu a publicação das fotos ou vídeos.

4.1.5 Invasão

Invasão é um tipo de ataque bem-sucedido que tem como resultados o acesso, a manipulação, alteração ou destruição de informação de um dispositivo informático.

A conduta de invadir dispositivo informático não era tratada pelo Código Penal, no entanto quando a atriz Carolina Dieckman teve seu computador invadido e 36 fotos íntimas que estavam no seu computador foram subtraídas por cinco homens, posteriormente identificados e responsabilizados pelos crimes de extorsão,

difamação e furto, mas não pela invasão do computador, em face da falta de legislação que cuidasse dos crimes cometidos, os membros do congresso nacional, impulsionados pela mídia, diante do caso ocorrido contra uma figura pública, aprovaram em 2012 a Lei 12.737.

O projeto de lei, antes de ser aprovado que trazia no seu bojo a tipificação de alguns crimes cometidos na grande rede. Ao todo eram 20 artigos, apenas dois foram mantidos, incluindo ao Código Penal Brasileiro o delito de invasão de dispositivo informático ou intrusão informática, que se encontra no artigo 154-A do referido diploma legal.

A tipificação da conduta de invadir dispositivo informático tem como objetivo maior proteger a liberdade individual, no tocante à inviolabilidade dos segredos. HUNGRIA *apud* GRECO (2017) esclarece que o segredo deve ser interpretado como:

> Um fato da vida privada que se tem interesse em ocultar. Pressupõe dois elementos: um *negativo* – ausência de notoriedade, e outro *positivo* – a vontade determinante de sua custódia ou preservação. Secreto é o fato que ainda não é notório (*res arcana*), não se devendo, porém, confundir a notoriedade com a *vaga atoarda*. Não deixa de ser secreto o fato sobre o qual apenas corre um *boato* incerto. (GRECO, 2017, p. 745)

O crime de intrusão informática se consuma no instante em que o agente delituoso invade dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança, com a finalidade de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, instalar vulnerabilidades ou obter vantagem ilícita, não importando se este objetivo vem a ser efetivamente alcançado.

Aquele que contribui mediante produção, oferecimento, distribuição ou difusão de programa de computador para que um terceiro venha a devassar dispositivo informático alheio incorrerá na mesma pena do *caput* do artigo 154-A.

4.1.6 Inutilização de equipamento informático

Neste tópico será elucidado o crime de dano realizado por meio da rede mundial de computadores, que se dá através da inutilização do computador ou outro dispositivo eletrônico ou pela destruição de dados ou informações constantes no sistema de informação.

O delito de dado informático não tem previsão legal, porém os tribunais vêm aplicando o artigo 163, do Código Penal para tratar do crime, tendo em vista que o crime é o mesmo, porém só foi aperfeiçoada a técnica para a sua aplicação, que se dá através ambiente virtual.

Nesse liame, o referido artigo do atual diploma penal explica que aquele que destruir, deteriorar ou inutilizar coisa alheia responderá penalmente pelo crime de dano.

Partindo deste paradigma, ilustra Marco Aurélio Rodrigues da Costa (1997) *apud* Zaniolo (2016):

> A informática concerne danos físicos ao computador na sua forma interna e externa. Se os danos visam à destruição do equipamento é aplicável, exclusivamente, o CP, art.163, porém, se os danos vão além da parte física do equipamento, atingindo 'software' e dados, é de ser apurada a vontade do agente. (ZANIOLO, 2016, p. 255)

No entendimento de MASSON (2016, p. 438) o dano deve ser o seu próprio fim, tendo em vista que ele não é resumido em inutilizar, destruir ou atém mesmo deteriorar coisa de outrem.

Esse tipo de crime pode ser aplicado através da disseminação de vírus, *boots worms*, *trojans*, *rootkits, adwares, ransomwares*, entre outros

O worms é um programa mais completo, uma vez que não necessita de um hospedeiro para se alastrar. A sua principal função é deletar dados de um computador. É conhecido como verme.

Já os boots infectam o disco rígido de um dispositivo informático. O seu poder de destruição é tão alto que pode até impedir que a vítima utilize o seu aparelho eletrônico.

Os rootkits geralmente infectam as tarefas e processos de memória, conseguindo anular o pedido do programa que está com esse software malicioso. Como resultado, o programa pode não encontrar os arquivos necessários para funcionar.

4.1.7 Furto digital mediante fraude

O furto eletrônico qualificado pela fraude e está inserido entre crimes digitais mais comuns devido à sua facilidade, pois não requer conhecimento avançado sobre computadores. Podendo ser aplicado por qualquer um.

Desde muito tempo, pessoas más intencionadas usam métodos fraudulentos para obter vantagem para si ou outrem, fazendo com que a vítima sofra algum tipo de prejuízo. PINHEIRO (2016) diz que:

> Toda fraude, independentemente da sua natureza, tem como pressuposto a utilização de um subterfúgio para ludibriar a vítima, seja por meio da ação ou da omissão do agente, isto é, o fraudador fornece informação errônea a vítima ou ainda omite. (PINHEIRO, 2016, p. 445)

À vista de Antônio Loureiro Gil a fraude eletrônica corresponde a uma "ação intencional e prejudicial a um ativo intangível causada por procedimentos e informações, de propriedade de pessoa física, ou jurídica, com o objetivo de alcançar benefício, ou satisfação psicológica, financeira e material".(GIL, 1999, p 15)

Nessa lógica, o criminoso envia uma mensagem que não foi solicitada, conhecida como phishing scam[25], passando-se por uma instituição financeira, uma empresa ou um banco conhecido, obtendo os dados do cartão de crédito da vítima através de uma página falsa na internet e por fim, passa pelo sistema de vigilância e proteção da instituição financeira sobre os valores mantidos a sua guarda.

A princípio, esse tipo de mensagem convencia o usuário ao acesso às páginas fraudulentas na Internet, imaginando ser da própria instituição. Hodiernamente, o furto por meio da fraude eletrônica refere-se também à mensagem que conduz o usuário à instalação de malware[26], além de mensagem, que apresenta formulário dentro do próprio conteúdo, que induz a pessoa a uma falsa percepção da realidade, no qual elas preenchem e enviam seus dados pessoais e financeiros para o fraudador e esse defrauda todo o sistema de proteção da vítima.

É possível diagnosticar que há divergência na doutrina em relação a que artigo o delito de fraude eletrônica se enquadraria, art. 171 "obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em

[25] É a palavra utilizada para definir um e-mail falso enviado para um indivíduo.

[26] Malware pode ser classificado como qualquer tipo de software malicioso que infecta ou tenta infectar um dispositivo móvel ou um computador. Podendo ser usado para extrair senhas, dados pessoais, dinheiro de contas bancárias e outros.

erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.” ou 155 “subtrair, para si ou para outrem, coisa alheia móvel: § 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime for cometido: I - com abuso de confiança, ou mediante fraude, escalada ou destreza”, ambos do Código Penal.

Contudo, as divergências podem ser esclarecidas com a decisão relatada pela Ministra Laurita Vaz, da Terceira Seção do STJ, no Conflito Negativo de Competência 67343 GO 2006/0166153-0. Veja:

> CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSO PENAL. FRAUDE ELETRÔNICA NA INTERNET. TRANSFERÊNCIA DE NUMERÁRIO DE CONTA DA CAIXA ECONÔMICA FEDERAL. FURTO MEDIANTE FRAUDE QUE NÃO SE CONFUNDE COM ESTELIONATO. CONSUMAÇÃO. SUBTRAÇÃO DO BEM. APLICAÇÃO DO ART. 70 DO CPP. COMPETÊNCIA DA JUSTIÇA FEDERAL PARANAENSE. 1. O furto mediante fraude não se confunde com o estelionato. A distinção se faz primordialmente com a análise do elemento comum da fraude que, no furto, é utilizada pelo agente com o fim de burlar a vigilância da vítima que, desatenta, tem seu bem subtraído, sem que se aperceba; no estelionato, a fraude é usada como meio de obter o consentimento da vítima que, iludida, entrega voluntariamente o bem ao agente. 2. Hipótese em que o agente se valeu de fraude eletrônica para a retirada de mais de dois mil e quinhentos reais de conta bancária, por meio da "Internet Banking" da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima, o Banco. A fraude, de fato, foi usada para burlar o sistema de proteção e de vigilância do Banco sobre os valores mantidos sob sua guarda. Configuração do crime de furto qualificado por fraude, e não estelionato. 3. O dinheiro, bem de expressão máxima da ideia de valor econômico, hodiernamente, como se sabe, circula em boa parte no chamado "mundo virtual" da informática. Esses valores recebidos e transferidos por meio da manipulação de dados digitais não são tangíveis, mas nem por isso deixaram de ser dinheiro. O bem, ainda que de forma virtual, circula como qualquer outra coisa, com valor econômico evidente. De fato, a informação digital e o bem material correspondente estão intrínseca e inseparavelmente ligados, se confundem. Esses registros contidos em banco de dados não possuem existência autônoma, desvinculada do bem que representam, por isso são passíveis de movimentação, com a troca de titularidade. Assim, em consonância com a melhor doutrina, é possível o crime de furto por meio do sistema informático. 4. A consumação do crime de furto ocorre no momento em que o bem é subtraído da vítima, saindo de sua esfera de disponibilidade. No caso em apreço, o desapossamento que gerou o prejuízo, embora tenha se efetivado em sistema digital de dados, ocorreu em conta corrente da Agência Campo Mourão/PR, que se localiza na cidade de mesmo nome. Aplicação do art. 70 do Código de Processo Penal. 5. Conflito conhecido para declarar competente o Juízo Federal de Campo Mourão - SJ/PR.

Observe nas imagens adiante um dos artifícios usados para captar os dados do cartão de crédito da vítima. É interessante lembrar que o método fraudulento que será exposto não pode ser confundido com estelionato, embora parecidos, pois no estelionato o criminoso vislumbra obter o consentimento da vítima para praticar o

ilícito, já no furto a sua qualificadora é utilizada para burlar a esfera de vigilância da vítima, como explicado anteriormente. Veja:

Figura 4 – Furto Internet Banking, parte 1

Fonte: <seumicroseguro.com>

Figura 5 – Furto Internet Banking, parte 2

Fonte: <seumicroseguro.com>

Conforme pesquisa realizada por via chat e e-mail com vários internautas pela Safernet foram registrados 54% de denúncias de fraudes somente na região sudeste e ainda, de acordo com notícia dada pela câmera dos deputados, foi realizada uma operação que ocorreu em setembro de 2013 que investigava no estado de São Paulo, Goiás e no Distrito Federal casos de fraudes bancárias no qual “ mais de 549 contas da Caixa Econômica Federal foram envolvidas, 367 delas usadas para saque e passagem de dinheiro. As fraudes ocorreram de novembro de 2012 a julho de 2013 e envolveram mais de R$ 2 milhões.”

4.1.8 Estelionato Digital

O estelionato digital é um crime previsto no art. 171, do Código Penal e consiste em “obter para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento”.

Esse tipo de crime pressupõem uma vontade viciada da vítima que entrega a coisa por livre e espontânea vontade.

Não há dúvidas que o crime comentado pode ocorrer por meio da internet. Frisa-se que é bastante comum a existência de pessoas sendo vítimas desse tipo de golpe.

Atualmente, existe pacificação nas doutrinas e jurisprudências acerca da aplicação do crime de estelionato digital, pois havia uma extrema necessidade de diferenciá-lo do delito de furto mediante a fraude no ambiente virtual, tendo em vista que ambos são fáceis de serem confundidos.

Essa aclaração jurisprudencial foi dada através do Conflito Negativo de Competência 67343 GO 2006/0166153-0, relatado pela Ministra Laurita Vaz, da Terceira Seção do STJ, o qual abarca a seguinte explicação:

> O furto mediante fraude não se confunde com o estelionato. A distinção se faz primordialmente com a análise do elemento comum da fraude que, no furto, é utilizada pelo agente com o fim de burlar a vigilância da vítima que, desatenta, tem seu bem subtraído, sem que se aperceba; no estelionato, a fraude é usada como meio de obter o consentimento da vítima que, iludida, entrega voluntariamente o bem ao agente.

4.1.9 Extorsão

Por fim, será analisado neste tópico o delito de extorsão no meio digital, mais praticado com a utilização de *ransomware*[27] que ocorre quando os dados com senhas de um determinado indivíduo são criptografados ou compactados, bloqueando o acesso aos mesmos e, em muitos casos, inutilizando o dispositivo infectado, além disso, para que a vítima recupere o controle sobre o seu dispositivo ou arquivos infectados ela deve realizar um pagamento. SAISSE (2016) explica que:

> O *ransomware* é propagado das mais variadas formas, seja por intermédio de acesso aos sites suspeitos que liberam o código malicioso apenas com a visita do usuário ou por arquivos disfarçados (músicas, imagens, etc.), normalmente divulgados em redes sociais ou enviados por e-mail aparentando algo comum, de interesse público, cobranças, causas sociais, etc. Ainda podem ser liberados via instalação de aplicativos vulneráveis em dispositivos móveis ou computadores.

Após a liberação do código no sistema, o *ransomware* opera sem o conhecimento do usuário até que todos os seus componentes para bloqueio de dados sejam instalados na máquina da vítima. Uma vez finalizada a instalação, um mecanismo de exibição de imagens ou mensagens é exibido comunicando o bloqueio dos dados e do resgate a ser pago para liberação. Neste momento, todos os dados do dispositivo se tornam totalmente inacessíveis.

Estas solicitações são normalmente valoradas em *bitcoins*[28], em razão do extremo anonimato sobre as transações realizadas nesse sistema de pagamentos.

Os alvos mais visados para esse tipo de crime são, na maioria das vezes, dispositivos de usuários individuais, redes corporativas e até mesmo do governo também são afetadas.

Se um computador for infectado, por exemplo, as chances de os dados serem perdidos são altas e consequentemente a vítima temorosa paga aos criminosos o valor correspondente para recuperação dos seus dados. Como afirma SAISSE (2016) “isso impulsiona a economia clandestina e como resultado aumentam o número de novos criminosos e o número de ataques.”. Nada impede também que o delito aconteça por outros meios.

---

[27] São softwares do tipo malware criados com o objetivo de infiltrar-se em sistemas sem a percepção de seu titular.

[28] É uma moeda digital do tipo criptomoeda descentralizada ou sistema econômico alternativo.

No que concerne especificamente ao artigo que deve ser aplicado é o 158, do Código Penal. Veja:

> Art. 158 - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa.

Nesse tipo de crime a vítima sabe o que está acontecendo e faz a entrega da coisa contra a sua vontade, em razão de violência ou grave ameaça.

4 DIFICULDADES ENCONTRADAS PARA A REPREENSÃO DOS CIBERCRIMES

Mesmo após a criação de uma legislação específica para os crimes virtuais, onde tipificou crimes que não poderiam ser punidos pelo atual código penal e instituiu a criação de delegacias especializadas em crimes da internet, os criminosos não se sentiram inibidos, tanto é que o Brasil ocupa a 5ª posição dos países em que mais ocorrem cibercrimes no mundo.

Os pontos que mais dificultam a repressão desses delitos são a falta de efetivo na polícia, a facilidade de encobrir as únicas provas existentes, as dificuldades de identificar o autor desses ilícitos, probatória e a lentidão dos procedimentos são alguns dos problemas que surgem.

O número de denúncias de crimes eletrônicos que são feitos é grande e a tendência é aumentar cada dia mais. Já a estrutura que a polícia federal, consoante entrevista de CANUTO, conta com apenas 15 grupos de combate ao crime cibernético em todo o País, mas apenas em São Paulo, Minas Gerais e Rio Grande do Sul há uma estrutura maior de pessoas envolvidas diretamente no trabalho.

O chefe da Unidade de Repressão a Crimes Cibernéticos da Polícia Federal, Carlos Eduardo Sobral, reclamou um efetivo maior e também a qualificação constante. "O volume de investigação vem crescendo, e o efetivo tem que crescer na mesma proporção. Hoje o nosso efetivo acaba sendo menor do que o volume que necessita para que seja dado um rápido andamento às investigações", afirmou.

Se um crime é praticado pela internet e se as provas não forem colhidas rapidamente e salvas em um equipamento de armazenamento de dados externo em que os criminosos não terão acesso, devendo manter tais provas fora do alcance de vírus ou outras pragas virtuais através de um cd[29] ou provas documentadas para

[29] Palavra utilizada para disco ótico digital usado para armazenar dados.

não correr o risco de serem perdida, haverá uma grande probabilidade de não punir, logo mais, os culpados e tampouco, provar a existência do ilícito.

No mesmo entendimento GRECO (2017) explica que:

> A dificuldade em atribuir a autoria do fato vem em grande medida determinada pela dificuldade probatória que rodeia a ilicitude informática. Isso se deve à própria dinâmica do processamento informático, que impede detectar uma determinada atividade ou processo posteriormente à sua realização, e em outras ocasiões, devido a facilidade para fazer desaparecer, de forma fraudulenta, por meio da manipulação de programa e dados, as atividades, operações, cálculos ou processos que foram realizados anteriormente. (GRECO, 2017, p.775)

É notório que os avanços tecnológicos não podem ser acompanhados pelas leis, pois estas últimas demoram anos para sair do papel. Além disso, os procedimentos para combater os delitos informáticos são muito lentos, pois a maioria dos dados que são utilizados para iniciar uma investigação é digitada e com a grande demanda e o pequeno número de efetivo acaba atrasando todo o trabalho.

Uns dos exemplos de lentidão dos procedimentos ocorrem com os crimes de pedofilia, no qual a CPI que cuida dos cibercrimes constatou que a polícia federal, somente no ano de 2014 recebeu mais de 50 mil relatórios sobre casos de pedofilia ou pornografia infantil praticados na grande rede. Enquanto as policias, juntamente com as empresas da internet vão fazendo os relatórios para a investigação vão ocorrem novos crimes e os antigos vão ficando a cada dia mais velhos.

Contudo o maior risco de segurança da informação é comportamental, pois os próprios usuários se expõem aos criminosos. Como é o caso a seguir:

Figura 6: Tuites Carolina

Fonte: <docplayer.com.br>

As pessoas se expõem na internet, divulgando fatos pessoais, sua rotina de trabalho ou pessoal e ficam vulneráveis aos criminosos.

A testemunha de um crime virtual é a máquina e esta não sabe distinguir se o crime foi praticado com dolo ou culpa. Segundo PINHEIRO (2016, p. 326) “a tecnologia ajuda a documentar os atos de má-fé, no entanto não há tecnologia à prova da má-fé”.

Um exemplo é o caso de uma pessoa enviar erroneamente por e-mail contendo um documento sigiloso da empresa em que trabalho ou documentos pessoais de um determinado indivíduo. A máquina nunca saberá distinguir se houve ou não vontade do agente sobre o ato descrito. Levando até a uma punição indevida da pessoa, não fazendo justiça como deve ser feita.

5 CONCLUSÃO

A evolução social e tecnologia proporcionou a inovação do crime, potencializando-os. A internet nasceu sem ao intuito de se preocupar com o seu uso para a prática de delitos, contudo se tornou o meio utilizado para tanto.

Conclui-se que a legislação brasileira não consegue acompanhar os avanços tecnológicos com a mesma agilidade que é oferecida pela internet, porém as leis

existentes ainda se aplicam aos casos discutidos na pesquisa, devendo apenas regulamentar questões especificas, como é o caso do Cyberbullying.

Além disso é possível concluir que a problemática reside não só na dificuldade para localizar e punir os agentes delituosos que usam a web de má fé ou na escassez e até mesmo na salvaguarda de provas encontradas no ambiente virtual, mas também no grande número de ataques virtuais que traz à tona o desconhecimento do uso saudável da internet pelos usuários, uma vez que, o maior risco de segurança da informação é comportamental, pois os próprios usuários se expõem aos criminosos.

É sabido que legislar sobre o direito eletrônico é muito delicado, uma vez que se não houver uma devida redação do tipo penal é bem provável que possa punir uma pessoa inocente. Além disso, sabe-se que as testemunhas dos crimes digitais são as próprias máquinas e elas não sabem diferenciar um crime praticado com dolo de um praticado com culpa, em outras palavras, os computadores não sabem informar sobre o contexto da situação. O que acaba levando a punição indevida do agente.

No que tange a competência processual dos crimes virtuais, seguirá os ditames do artigo 109 da CF. Devendo ir apenas para a esfera dos crimes cuja competência é da Justiça Federal os casos descritos no mencionado artigo, como por exemplo o crime de pornografia infantil e racismo. Já os demais serão da Justiça Estadual, que é residual por natureza.

Conforme visto em toda a pesquisa, constata-se facilmente que é crucial adotar uma postura ética e segura na internet, seja através de leis, políticas, normas e educação, já que, o maior causador de brechas para os crimes descritos é o próprio indivíduo que usam as ferramentas eletrônicas de forma inadequada.

É necessário que as pessoas aprendam a usar a Internet de forma saudável, seguindo um conjunto de dicas de segurança cibernética simples e que podem ajudar a evitar grande parte dos ataques virtuais. Pois, boas práticas adotadas na rede podem melhorar significativamente os ataques virtuais.

Em contrapartida, assim como na vida real ninguém está isento de ser vítima de algum tipo de crime no seu dia-a-dia, tampouco no mudo virtual, pois embora se tenha todo zelo e todas as técnicas de proteção para utilizar caixa eletrônico, realizar compras onlines, utilizar a internet banking, enviar e-mail, logar nas redes sociais, baixar músicas ou livros digitais, ver filmes através da smart TV, acessar o smart

phone e em outras tarefas do cotidiano real/virtual, pode-se ainda sofrer algum tipo de ataque que muitos criminosos espalhados pelo mundo podem praticar.

Tal conclusão reforça a ideia defendida por alguns autores, como Cleber Masson e Patrícia Peck Pinheiro que não existe necessidade de criação de mais leis, pois as vigentes se aplicam aos crimes virtuais.

REFERÊNCIAS

ADOLESCENTES. Jornada estadual contra a violência e a exploração sexual de criança e. **Seis livros sobre abuso e exploração de crianças.** Disponível em: <http://wp.clicrbs.com.br/jornadasestaduais/2014/05/28/6-livros-sobre-abuso-e-exploracao-da-crianca/>. Acesso em 27 dez. 2017

ATHENIENSE, Alexandre. **Crimes virtuais:** soluções vigentes e projetos de lei. Disponível em: <http://www.dnt.adv.br/noticias/crimes-virtuais-solucoes-vigentes-e-projetos-de-lei>. Pulicado em set. 2000. Acesso em: 25 out. 2016.

BITENCOURT, Cezar Roberto. **Tratado de direito penal 2:** parte especial: dos crimes contra a pessoa. 13. Ed. São Paulo: Saraiva, 2013.

BRASIL. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no. **Cartilha de Segurança para Internet**. Disponível em: <https://cartilha.cert.br/ataques/>. Acesso em: 05 abr. 2017.

BRASIL, **Código Penal**: Decreto-lei nº 2.848, de 07 de dezembro de 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737 .htm>>. Acesso em: 05 nov. 2016.

BRASIL, **Constituição Federal**: Lei nº 9.296, 24 de julho de 1996. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/L9296.htm>>. Acesso em: 26 nov. 2016.

BRASIL. Safer Internet Center do: **Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos**. Disponível em: <http://indicadores.safernet.org.br/index.html>>. Acesso em: 03 nov. 2017.

CANUTO, Luiz Claudio. **CPI constata dificuldades em rastrear e punir crimes de internet**. Disponível em: <http://www2.camara.leg.br/camaranoticias/noticias/SEGURANCA/494363-CPI-CONSTATA-DIFICULDADE-EM-RASTREAR-E-PUNIR-CRI ME -DE- INTERNET.html>>. Acesso em: 02 jan. 2018.

CUNHA, Rogério Sanches, **Manual de direito Penal:** parte especial, Salvador. JusPODIVM, 2016.

DEPUTADOS, Câmara dos. **Projetos de Lei e Outras Proposições.** Disponível em: <http://www.camara.leg.br/buscaProposicoesWeb/?wicket:interface=:2:paginacaoBusca:nav:2:pageLink:1:ILinkListener: >. Acesso em: 25 out. 2017.

DEPUTADOS, Câmara dos. **CPI constata dificuldades em rastrear e punir crimes de internet**. Disponível em< http://www2.camara.leg.br/camaranoticias/noticias/SEGURANCA/494363-CPI-CONSTATA-DIFICULDADE-EM-RASTREAR-E-PUNIR-CRIMES-DE-INTERNET.html>. Acesso em: 02 jan. 2018.

DICIONÁRIO, Priberam. **Significado da palavra logar**. Disponível em: <https://www.priberam.pt/dlpo/logar>. Acesso em 12 jan. 2018.

EXTRA. Jornal. **Comentário racista contra Thais Araújo.** Disponível em: <https://extra.globo.com/casos-de-policia/policia-prende-responsaveis-por-ataques-racistas-contra-tais-araujo-1888626 7.html>. Acesso 10 nov. 2017.

FILHO, Adilson Paulo Prudente do Amaral (2011). **Crimes cibernéticos:** e o grupo de combate da procuradoria da República no estado de São Paulo. REVISTA JURÍDICA CONSULEX, nº 343, p. 37-38, maio 2011.

FIORILLO, Celso Antônio Pacheco. **Crimes no meio ambiente digital**. 1 Ed. São Paulo: Saraiva, 2013.

GIL, Antônio Loureiro. **Fraudes informatizadas**. 2 Ed. São Paulo: Atlas, 1999, p. 15.

GRECO, Rogério. **Código Penal comentado**. 11 Ed. Rio de Janeiro, 2017.

INFORMAÇÃO. Centro Regional de Estudos para o Desenvolvimento da Sociedade da. **Portal de Dados:** domicílios com acesso à internet. Disponível em: <http://data.cetic.br/cetic/explore?idPesquisa=TIC_Dom>. Acesso em: 30 out. 2017.
INFORMAÇÃO. Centro Regional de Estudos para o Desenvolvimento da Sociedade da. **Portal de Dados:** usuários de internet indicador ampliado. Disponível em: <http://data.cetic.br/cetic/explore?idPesquisa=TIC_DOM&idUidadeAnalise=Usuarios&anolnicio=2008&anoFim=2015>. Acesso em: 30 out. 2017.

JUSTIÇA. Superior Tribunal. **Diário da justiça Eletrônico:** conflito de competência crimes contra honra. Disponível em: <https://www.jusbrasil.com.br/diarios/51029781/stj-20-02-2013-pg-585>. Acesso 20 dez. 2017

LINS, Bernardo Felipe Estelita. **A evolução da internet:** uma perspectiva histórica. In cadernos ASLEGIS, nº 48. Brasília: ASLEGIS, 2015.

MAIA. Eleidi Alice Chautard Freire. **Mapeamento do genoma humano e algumas implicações éticas**. Disponível em <http://revistas.ufpr.br/educar/article/view/35129>. Acesso 23 dez. 2017.

MASSON, Cleber. **Direito penal esquematizado:** parte especial. 6. Ed. São Paulo: Método, 2016.

NOW, IDG. **Tuites com conteúdo racista de Mayara**. Disponível em: < http://idgnow.com.br/internet/2011/12/12/ministerio-publico-aceita-denuncia-e-mayara-petruso-respondera-por-racismo/>. Acesso em: 10 nov. 2017

NUCCI, Guilherme de Souza, **Código Penal Comentado**, 16. Ed. Rio de Janeiro: Forense, 2016.

PINHEIRO, Patrícia Peck. **Direito Digital**, 6. Ed. São Paulo: Saraiva, 2016. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502635647/ci/395!/4/4@0:0.00>. Acesso em: 03 nov. 2017

PAESANI, Liliana Minardi. O papel do direito contra o crime cibernético. In: **Âmbito Jurídico**, Rio Grande, XIII, n. 79, ago. 2010. Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=7972>. Acesso em: 15 nov. 2016.

PLAYER. Doc. **Tuites Carolina**. Disponível em: <http://docplayer.com.br/2276902-Direito-digital-unicamp-instrutora-dra-patricia-peck-pinheiro-twitter-patriciapeckadv.html>. Acesso 2 jan. 2018

SAISSE, Renan Cabral. **Ransomware: "sequestro" de dados e extorsão digital**. Disponível em: <http://direitoeti.com.br/artigos/ransomware-sequestro-de-dados-e-extorsao-digital/#_edn4>. Acesso 11 jan. 2018

RAMALHO, José Ricardo (2016). **Pedofilia e a rede do mal:** os aspectos legais e punitivos relacionados ao uso da internet para a prática de crimes sexuais contra crianças e adolescentes. REVISTA VISÃO JURÍDICA, nº 343, p. 28-35, 12 dez. 2016

RODRIGUES, Guilherme. **Injúria racial contra filha de Gio Ewbank**. Disponível em: <https://observatoriodatelevisao.bol.uol.com.br/famosos/2016/11/de pois-de-ofender-gaby-amarantos-internauta-ataca-filha-de-bruno-gagliasso-parece-uma-macaquinha>. Acesso em: 10 nov. 2017

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. 1. Ed. São Paulo: Memória Jurídica, 2004.

SANTOS, Coriolano Aurélio de Almeida Camargo; FRAGA, Ewelyn Schots. **As Múltiplas Faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e Seus Reflexos no Universo Jurídico**. São Paulo: OAB SP, 2010.

SEGURO, Seu micro. **Furto internet banking**. Disponível em:< https://seumicroseguro.com/2014/04/07/site-da-caixa-possibilitou-ataques-de-phishing/ >. Acesso 5 jan. 2018

SILVA, Ana Beatriz Barbosa. **Bullying:** mentes perigosas nas escolas. Rio de Janeiro: Objetiva, 2010.

SOPRANA, Paula. **A CPI dos crimes cibernéticos mutila o marco civil da internet**. Disponível em <http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/04/cpi-de-crimes-ciberneticos-quer-alterar-marco-civil-da-internet-no-brasil.html >. Acesso: 26 nov. 2016

TÁVORA, Nestor. ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**. 12. Ed. Bahia: JusPodivm, 2017, pág. 387.

TEIXEIRA, Cenivalda Miranda de Sousa Ulrich Schiel (1997). **A internet e seu impacto nos processos de recuperação da informação**. Disponível em: <http://www.scielo.br/scielo.php?pid=S0_100196519970001000 09&script=sci_arttext&tlng=e>. Acesso em: 21 out. 2016

BRASIL. Superior Tribunal de Justiça. Conflito de Competência: CC 67343/GO 2006/0166153-0. Relatora: Laurita Vaz - Terceira Seção. **Diário da Justiça Eletrônico**, Brasília, 06 fev. 2008. Disponível em: < https://stj.jusbrasil.com.br/jurisprUdencia/8787855/conflito-de-competencia-cc-67343-go-2006-0166153-0>. Acesso 31 dez. 2017

VIANNA, Túlio Lima. **Fundamentos de direito penal informático.** Monografia apresentada ao Curso de Direito da Faculdade UFMG. Universidade Federal de Minas Gerais. Belo Horizonte, 2001.

WIKIPÉDIA. A enciclopédia livre. **E-mail**. Disponível em: <http://pt.wikipedia.org/wiki/E-mail>. Acessado em: 29 out. 2016>.

ZANIOLO, Pedro Augusto. **Crimes Modernos:** p impacto da tecnologia no Direito**.** 3 Ed. 2016. Curitiba. Juruá Editora.