FACULDADE CAMBURY
ESCOLA DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

CRIMES VIRTUAIS E SUA DIFICULDADE PUNITIVA

ORIENTANDO: GABRIEL MARIANO BORGES DA SILVA
ORIENTADORA: PROFA ESP. SARA CRISTINA ROCHA DOS SANTOS

GOIÂNIA
2016

ORIENTANDO: GABRIEL MARIANO BORGES DA SILVA

CRIMES VIRTUAIS E SUA DIFICULDADE PUNITIVA

Artigo Científico apresentado à disciplina Trabalho de Curso III, curso de Direito da Faculdade Cambury, sob a orientação da Profa. Esp. Sara Cristina Rocha dos Santos.

GOIÂNIA

2016

ORIENTANDO: GABRIEL MARIANO BORGES DA SILVA

CRIMES VIRTUAIS E SUA DIFICULDADE PUNITIVA

Data da Defesa: _____ de _____ de 2016.

BANCA EXAMINADORA

Orientadora: Profa. Esp. Sara Cristina Rocha dos Santos nota

Examinador Convidado: Prof. nota

DEDICATÓRIA

Dedico este trabalho os meus pais, Maria José de Fátima Borges e Antônio Fernando Borges da Silva, pela motivação que me trouxe até aqui.

AGRADECIMENTOS

Primeiramente agradeço a todos que me apoiaram até a chegada deste dia.

À todos os professores e colegas que de alguma forma transmitiram suas experiências contribuindo de uma forma ou de outra para o acadêmico que sou hoje.

À todos aqueles que em algum momento do percurso me apoiaram quando foi preciso.

SUMÁRIO

RESUMO **6**
INTRODUÇÃO **6**

1 ERA DIGITAL **6**
1.1 A origem da Era Digital e Seus Benefícios **7**

2 A ILICITUDE NO ÂMBITO VIRTUAL **9**
2.1 Dos Crimes Virtuais **9**
2.2 Meios utilizados na prática de crime virtual **11**

3 DO USO DA ANALOGIA E ATUALIDADE LEGISLATIVA **12**
3.1 Do crime de dano **13**
3.2 Do Marco da Legislação do Meio Virtual **14**

CONCLUSÃO **16**
REFERÊNCIA **17**

CRIMES VIRTUAIS E SUA DIFICULDADE PUNITIVA

Gabriel Mariano Borges da Silva

RESUMO: O presente estudo pretendeu examinar como o desenvolvimento tecnológico abre vertentes para novas práticas de delituosas e consequentemente lacunas na legislação brasileira. Como foco de análise, optou por estudo de autores conceituados nas áreas abrangidas. Dentro dessa perspectiva de análise, procurou obter dados envolvendo as o inicio e as interações do meio virtual no meio físico. Com esses resultados, foi possível observar que as inovações tecnológicas envolvendo a interação do meio físico com o meio virtual necessitam de legislações específicas para que não haja lacunas no ordenamento, garantindo a segurança da sociedade e punibilidade para aqueles que praticam tais delitos. A metodologia utilizada envolveu o método dedutivo e a pesquisa teórica.

Palavras-chave: Crimes virtuais. Punição ao crime virtual. Era digital.

INTRODUÇÃO

O presente trabalho aborda a necessidade do ser humano de inovar para facilitar sua vida, inovação do qual pode ser citada a criação do que futuramente seria denominada internet, nas décadas 60,70 e 80 e como foi a transação de um equipamento para uso militar até os dias de hoje.

Todos esses avanços que possibilitaram uma maior aproximação das relações pessoais, uma melhor forma de comunicar, de transmitir e receber informações de maneira mais cômoda. Isso tudo devido ao encurtamento de fronteiras que esta inovação trouxa.

Inovação da qual foi utilizada para inúmeras atividades com o objetivo de melhorar o mundo de alguma maneira, facilitando as já mencionadas relações pessoais práticas, maior comodidade em atividades como pesquisa, trabalho e diversas outras. Mas com a disseminação dessa inovação, criminosos também começaram fazer uso para meios ruinosos.

Com a ocorrência dessas atividades delituosas tomando cada vez mais espaço e afetando cada vez mais a sociedade, os legisladores se viram obrigados a agir com os meios possíveis para controlar a situação, enquadrando a legislação já vigente quando possível e criando novas para a proteção de todos.

1 ERA DIGITAL

A era dos aparelhos eletrônicos trouxe diversas ferramentas e informações que facilitou a vida das pessoas em inúmeras maneiras. Mudanças do modo como vivemos hoje evolui bastante em termos de qualidade, praticidade e celeridade. Mas esta evolução não chegou de uma hora para outra, houve etapas que se acarretaram, acelerando o desenvolvimento desta fase evolutiva onde foi possível chagar aos dias de hoje.

1.1 A origem da era digital e seus benefícios

O ser humano sendo o animal racional que é, sempre procurou facilitar suas atividades, sejam elas no meio da caça, da moradia ou da locomoção. E até hoje essa característica humana nunca desapareceu, sempre procurando o melhor meio de exercer determinada atividade da melhor maneira possível.

Se segundo Paiva (2012), "Desde os primórdios até os dias atuais, o homem vem buscando desenvolver novas máquinas e ferramentas que lhe torne as atividades do dia a dia mais fáceis e de certa forma mais prazerosas."

Com o passar do tempo o número de invenções criadas foram só aumentando, cada vez mais tornando a vida mais prática e confortável. Destas aquisições podemos citar telefones, rádios, televisores e inúmeras outras. Invenções das quais foram transformando a forma em que vivemos hoje, com maior qualidade nos desempenhos de nossas atividades. Praticidade, também, que na peculiaridade de cada uma das invenções contribuía para o próximo aparato tecnológico.

Por sua vez, Kannan (*apud* PECK, 2011, p. 55):

> A informática nasceu da ideia de beneficiar e auxiliar o homem nos trabalhos do cotidiano e naqueles feitos repetitivamente. Tem-se por definição mais comum que a informática é a ciência que estuda o tratamento automático e racional de informação. Entre as funções da informática há o desenvolvimento de novas máquinas, a criação de novos métodos de trabalho, a construção de aplicações automáticas e a melhoria dos métodos e aplicações existentes.

Com essa área descoberta também foi aberta novas portas para a utilização desta tecnologia. Algo que não poderia ser diferente visto que uma ferramenta relativamente pequena agora concentrava e transformavam informações de maneiras mais práticas.

Segundo Peck (2011, p.58) é possível entender esse acarretamento evolutivo e o que isso levou:

> Esses fatos são reflexos de um caminho rumo à chamada sociedade de convergente que se vem desenvolvendo rapidamente desde a criação do telefone, considerada a

> primeira ferramenta de comunicação simultânea a revolucionar os comportamentos sociais. Na outra ponta deste movimento evolutivo, a Internet veio possibilitar não apenas o encurtamento das distancias com maior eficiência de custos, mas, sobretudo, a multicomunicação, ou seja, transmissão de texto, voz e imagem. A multicomunicação, associada à capacidade de respostas cada vez mais ágeis, permite que a Internet se torne o mais novo veículo de comunicação a desafiar e transformar o modo como nos relacionamos.

A Internet trouxe uma enorme facilidade para a interação. Além da comunicação entre as pessoas, é possível acessar informações disponíveis na rede de dados. O que hoje em dia com o enorme número de usuários que trocam informações significa que basicamente qualquer um pode ter acesso a qualquer tipo de informação pública. Compartilhamento e troca de informações é algo muito comum nos dias de hoje.

De acordo com Peck (2010, p. 58-59) a origem da Internet foi desenvolvida em meados dos anos 60, no ápice da Guerra Fria como uma ferramenta para fins militares:

> Basicamente, tratava-se de um sistema de interligação de redes dos computadores militares norte-americanos, de forma descentralizada. À época, denominava-se "Arpanet". Esse método revolucionário permitia que, em caso de ataque inimigo a alguma de suas bases militares, as informações lá existentes não se perderiam, uma vez que não existia uma central de informações propriamente dita.

Segundo Piva (2006), antes de se chamar Internet, o projeto que deu inicio à esse avanço se chamava ARPANET, criado pelo governo norte-americano:

> A Internet é uma rede de redes em escala mundial de milhões de computadores que permite o acesso a informações e todo tipo de transferência de dados. O que hoje forma a Internet, começou em 1969 como a ARPANET, criada pela ARPA, uma subdivisão do Departamento de Defesa dos Estados Unidos. Ela foi criada para a guerra, pois com essa rede promissora, os dados valiosos do governo americano estariam espalhados em vários lugares, ao invés de centralizados em apenas um servidor. Isso evitaria a perda desses dados no caso de, por exemplo, uma bomba explodisse no campus.

Ainda segundo Piva (2010), posteriormente essa ferramenta passou a ser usada para civis. Inicialmente os primeiros usuários do meio civil foram os universitários e professores de universidades norte-americanas, visto que, a transmissão de dados além de ser um avanço tecnológico onde os estudiosos se interessavam, era prático. E nesse ambiente menos controlado foi possível avançar para os moldes que conhecemos hoje.

De acordo com Piva (2006), a transição da ARPANET para o que nós conhecemos hoje em dia como Internet ocorreu em meados dos anos 80. E juntamente com essa transição também foram incorporados novas nomenclaturas que passaram a ser usadas a partir desse gatilho tecnológico. Como por exemplo *hacker* e ciberespaço.

Piva (2006) ainda diz que o padrão IP/TCP, utilizado na rede para a transferência de dados, foi estabelecido em 1982 e logo em seguida em 1983 se tornou obrigatório. E a partir desse momento a Internet pode ser conceituada como um conjunto de redes interligadas.

Segundo Piva (2006):

> Em 1994 surgiram serviços de entrega pela rede (Pizza Hut), o primeiro banco online, os primeiros shoppings virtuais e, em 1995, a Internet foi privatizada, com o estabelecimento de provedores independentes. No Brasil, a Embratel deixou de ter o monopólio das transmissões.

Piva (2006) ainda comenta que a facilidade de acesso à Internet atualmente. Podendo acessá-la por microcomputadores, celulares, vídeo-games e até geladeiras. A transmissão passou a poder ser feita por linhas telefônicas fixas, móveis, por cabo, por satélite e infra-vermelho.

2 A ILICITUDE NO ÂMBITO VIRTUAL

As chances de que alguém consiga se defender do ataque de algum crime virtual, primeiramente é preciso entender o que é um crime virtual. E para que possamos compreender a definição de crime virtual é bom também entender o significado mais puro de crime, como nos é explicado no ordenamento brasileiro.

2.1 Dos crimes virtuais

Segundo a Lei de Introdução ao Código Penal (BRASIL, 1941), no seu artigo 1º:

> Considera-se crime a infração penal a que a lei comina pena de reclusão ou de detenção, quer isoladamente, que alternativa ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente.

E para uma complementação, no Código Penal (BRASIL, 1984) diz em seu artigo 1º que “Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal”.

Onde com esses dois trechos da legislação onde um apóia o outro podemos constatar que ocorre crime quando esta está definida em lei vigente onde também será informado a penalidade pela prática. Penalidades das quais estão expressas no 1º artigo da Lei de Introdução ao Código Penal, como vimos anteriormente.

Para Capez (2003, p. 105) “Crime pode ser definido como todo fato humano que propositada ou descuidadamente lesa ou expõem a perigo bens jurídicos considerados fundamentais para a existência da coletividade e da paz social”.

Com os crimes feitos virtualmente não é diferente, ainda é crime, e a intenção de quem o pratica também é expor em perigo os vens jurídicos de outrem e assim perturbando a paz social. A diferença é apenas novos meios de serem praticados, mas o resultado, se efetuados com êxitos, são os mesmos que os crimes considerados tradicionais.

Segundo Gustavo e Gabriela (2011):

> Os crimes virtuais utilizam a mesma metodologia de crimes utilizados em crimes já conhecidos. A técnica empregada que difere um pouco dos delitos presentes em nosso ordenamento jurídico penal, mas o fim que se pretende é o mesmo da conduta já tipificada. A intenção do criminoso pode ser de ludibriar uma pessoa para obter uma vantagem financeira ou pessoal, enganar suas vítimas ou mesmo furtar informações particulares com o intuito de utilizá-las em proveito próprio.

Gustavo e Gabriela (2011), ainda cita alguns casos bem comuns onde ocorre o crime virtual:

> Ultimamente uma modalidade de crime que vem se tornando muito comum na internet é o envio de e-mail simulando ser de algum órgão estatal conhecido, como é o caso da Receita Federal, TSE (Tribunal Superior Eleitoral), Polícia Federal e Serasa. A metodologia empregada é enganar o proprietário do e-mail, com uma mensagem dizendo que existe alguma pendência com o órgão e que este deve clicar em algum link para solucionar tal situação ou até mesmo para saber mais detalhes sobre o fato. Ao clicar em tal link, o usuário é redirecionado para uma página em que o intuito é instalar um programa conhecido como sanguessuga no computador da vítima, e a partir desse momento, o criminoso começa a receber dados sigilosos.

Aos olhos de quem não está ciente da existência dessas práticas não está preocupado quando manuseia o e-mail. E ainda pela aparência e com o nome de órgãos respeitados pelo cidadão estampados no e-mail já provocam preocupação da vítima acreditando na informação contida na mensagem e seguindo os passos criados pelo verdadeiro remetente.

Outro caso comum também ocorre com o uso do e-mail, como citado acima, quando no e-mail recebido pela vítima contem informações que lhe induzem a pensar que é um e-mail de seu banco. Com a preocupação econômica da sociedade e com a seriedade destas instituições a vítima começa pensar que está tudo de acordo e começa os preparativos para solucionar o suposto problema. Nesse e-mail pode conter links que encaminharão o usuário para uma falsa página onde é necessário inserir dados de senha, momento do qual o

remetente do e-mail malicioso obtém informações pessoais da vítima. Nesta prática exige um pouco de conhecimento pessoal da vítima para saber por exemplo, no caso citado, qual o banco da mesma. Mas que também mesmo sem essa informação, enviando para pessoas aleatórias podem atingir um número significativo ainda, pelo fato de o número de bancos existentes não ser tão grande.

Fonseca (2002) assim como, comenta outra forma que o crime virtual é praticado para que o remetente possa se apropriar de informações da vítima que envolva entidades bancárias:

> Dentre os delitos perpetrados por estes, podemos citar as constantes investidas as contas bancárias alheias, desviando seus valores para contas fantasmas de amigos ou próprias e, nessa mesma linha de delitos um dos mais usuais delitos dessa natureza que é a "invasão" de computadores particulares com o intuito de ler os chamados e-mails.

2.2 Meios utilizados na prática de crime virtual

Algumas pessoas não sabem mas na maioria das vezes o atacante deste crime só consegue se infiltrar nos nossos computadores e aparelhos similares porquê a titular do aparelho permite isso, mas não necessariamente que tenha a intenção de permitir tal coisa.

De acordo Oliveira (2014) alguns dos meios utilizados para nos ludibriar, sendo uns dos mais utilizados, o e-mail, programas de mensagens instantâneas, sites falsos e programas de compartilhamento de arquivos.

Segundo Oliveira (2014, ebook):

> Atualmente, o e-mail tornou-se um meio de comunicação indispensável, mas, por outro lado, ainda é um dos meios mais eficazes para que um atacante invada um computador. Spam, vírus, golpes de roubo de identidade e e-mails fraudulentos são apenas algumas das ameaças. O usuário recebe um e-mail fazendo despertar sua curiosidade e acaba clicando em um link, permitindo assim que o atacante alcance o seu objetivo.

Como foi citado anteriormente, as máscaras usadas no e-mail para ludibriar a vítima podem ser das mais variadas, com a finalidade de abaixar a guarda e instigar a sua curiosidade para cometer algum ato indevido no e-mail malicioso, como por exemplo, clicar no link enviado.

Outro meio de comunicação pelo computador e aparelhos similares que também pode ser um dos meios utilizados para esta prática são programas de mensagens instantâneas. Difundida pela sua praticidade e, como o nome já diz, instantaneidade de interação. A

diversidade destes programas é enorme e a cada dia que passa mais são criados para atender a necessidade dos usuários.

Oliveira (2014, ebook) explica que Alguns destes programas mais conhecidos são o Skype, Google Talk, Yahoo Messenger, dentre outros. E quando essa prática é utilizada por meio destes programas de mensagens instantâneas é comum o atacante enviar um link através de uma pessoa conhecida. Assim quando o usuário clicar a ameaça enviada fará com que o atacante tenha algum acesso ao computador da vítima.

Outra maneira de enganar a vítima para que ela compartilhe informações sigilosas é o uso de sites falsos.

Segundo Oliveira (2014, ebook):

> Usam técnicas de redirecionamento em que eventualmente o usuário pode ser direcionado para um site falso, idêntico ao original, que lhe solicitará senha. Caso o usuário não desconfie, além do site lhe roubar alguma senha, poderá instalar algum tipo de programa malicioso.

Existe também sistemas de compartilhamento de arquivos, nestes programas é possível achar ou compartilhar arquivos com uma maior facilidade e praticidade.

Cassanti comenta que esses programas servem para compartilhar e localizar arquivos. Com eles você pode encontrar e fazer download de músicas MP3, vídeos AVI e outros tipos de arquivos, inclusive programas. Também é citado os mais utilizados, sendo eles o Ares, LimeWire e eMule. Estes programas disponibilizam milhares de arquivos, mas nem todos são confiáveis.

3 DO USO DA ANALOGIA E ATUALIDADE LEGISLATIVA

Pela internet se tratar de relações entre indivíduos, pode-se também dizer que o Direito Penal Brasileiro por sua vez está igualmente ou pelo menos deveria estar disciplinando certas ações, já que o objetivo do Direito brasileiro é regulamentar e organizar medidas que tenham por objeto a proteção civil e jurídica que além de policiar a sociedade física também policie a “sociedade digital”.

De acordo com as palavras de Crespo (2011, p. 48):

> Com o atual Código Penal já é possível uma punição eficiente para as ilicitudes praticadas com o uso da tecnologia. Existem também aquelas onde o agente afeta bens jurídicos relativos à Sociedade da Informação, como dados de sistemas, por exemplo. Neste caso, passando a exigir uma intervenção legislativa para elaboração de novos instrumentos normativos de punição.

Como falado por Crespo existem algumas tipificações constantes no ordenamento jurídico que já são citadas como ilegais. E com isso sendo legitimamente consideradas crime pelo princípio de só ser considerado crime ação constante em lei e que haja cominação de pena, como é dito no artigo. 1º da Lei de Introdução ao Código Penal e no artigo 1º do Código Penal.

Lima (2014) assim mostra um resumo de alguma destas:

> Art. 153, § 1° - A do Código Penal – Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública. Pena – detenção de 1 a 4 anos, e multa. Art. 313 – A do Código Penal – Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano. Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa. Art. 313 – B do Código Penal – Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente. Pena – detenção de 3 (três) meses a 2 (dois) anos, e multa. Art. 325, § 1°, incisos I e II - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação: Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave. § 1o Nas mesmas penas deste artigo incorre quem: I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública; II – se utiliza, indevidamente, do acesso restrito.

3.1 Do crime de dano

O uso da analogia em teoria poderia ser aplicado no que envolver crimes relacionados ao meio virtual e digital, já que estes crimes nada mais são do que, os mesmos crimes já descritos no Código Penal que são praticados no âmbito físico mas com uma roupagem diferente. Mas na prática há divergência sobre seu uso.

De acordo com Gatto (2011):

> O crime de dano é uma das matérias mais divergentes dentro do âmbito dos crimes de informática julgados por analogia, aplicando o artigo 163 do Código Penal, para os casos mais corriqueiros da internet que é a destruição ou a inutilização de arquivos de dados, possa ser aplicado analogamente aos crimes em que vírus destroem ou danificam substancialmente dados de terceiros.

O artigo 163 do Código Penal (BRASIL, 1984) diz que:

> Art. 163 - Destruir, inutilizar ou deteriorar coisa alheia:
> Pena - detenção, de um a seis meses, ou multa.
> Dano qualificado

> Parágrafo único - Se o crime é cometido:
> I - com violência à pessoa ou grave ameaça;
> II - com emprego de substância inflamável ou explosiva, se o fato não constitui crime mais grave.
> III - contra o patrimônio da União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista;
> IV - por motivo egoístico ou com prejuízo considerável para a vítima:
> Pena - detenção, de seis meses a três anos, e multa, além da pena correspondente à violência.

Mas não se pode fazer o uso da analogia no artigo em destaque, pois estaria contrariando os já mencionados artigos 1º da Lei de Introdução do Código Penal, artigo 1º do Código Penal e o artigo 5º, XXXIX da Constituição Federal, onde basicamente dizem que não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Além do fato de que o objetivo do legislador neste artigo foi a proteção do patrimônio. Assim formando uma brecha, onde se o dano causado for,por exemplo, em algum arquivo digital, onde não haja importância relacionada ao patrimônio, como fotos e emails de amigos, não poderá ser punido pelo artigo 163 do Código Penal. Pois se não houver algum tipo de prejuízo material não poderá ser classificado como crime contra o patrimônio.

Nas palavras de Mirabetti (2010, p. 240), há três condutas, das quais para ser configurado um crime de dano é preciso que pelo menos haja uma delas:

> Destruir inutilizar ou deteriorar. Destruir é eliminar, desfazer, desmanchar, demolir (quebrar um vidro, matar um animal, derrubar um muro etc.). Inutilizar significa tornar inútil, imprestável, inservível a coisa (quebrar peças de uma maquina tirar ponteiros de um relógio etc.). Deteriorar, estragar, arruinar, adulterar (mutilar um animal, misturar um liquido no vinho etc.).

Tornando-se claro que não é sustentado o enquadramento do crime de dano relacionado aos crimes virtuais. Assim precisando que haja uma legislação especifica de tal prática para a proteção da sociedade no uso da internet.

3.2 Do Marco da Legislação do Meio Virtual

Pela preocupação sobre a escassez de legislações comparado com a amplitude do tema, problemas e preocupações advindos do uso da internet vem sendo debatidos há muito tempo.

De acordo com Bastos e Tavares (2000, p. 698):

> A utilização da Internet tem implicações diretas com o tão sacramentado direito de liberdade, mais precisamente a de manifestação. A questão está conectada igualmente ao problema da informação, e de o correspondente direito a ela poder-se

> ascender. Daí surge outro aspecto, que é o referente à divulgação maciça de informação falsa, como que a tornando, de certa maneira uma verdade, pela sua reiterada repetição sem manifestação de impugnações na mesma escala. (...) Por outro lado, a invasão de sistemas informáticos particulares tem sido uma constante preocupação, principalmente por parte dos governos, com relação aos seus dados. Também dentro do contexto de proteger a privacidade de informações, é preciso estabelecer regras o tanto quanto possível precisas de veiculação de dados pessoais por meio da Internet, haja vista que seu acesso é franqueado a todo mundo, e, invariavelmente, seu autor não é descoberto.

Com as necessidades aumentando e com isso a segurança jurídica ficando cada vez mais vulnerável foi preciso a criação de legislações específicas para atuar em atividades relacionadas com o meio eletrônico e virtual. Sendo uma das mais importantes o Marco Civil da Internet, criado como PL 2.126/2011 e posteriormente se tornando a Lei nº 12.965/2014. E a Lei Carolina Dieckmann que surgiu como PL 2.793/2011 e posteriormente veio a se tornar a Lei 12.737/2012.

Talvez o Marco Civil da Internet seja o documento mais significativo no âmbito do direito civil em relação a este tema. Ele estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, como diz em seu primeiro artigo: "Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria".

No Âmbito penal, talvez a legislação em maior destaque seja a Lei 12/737/2012, a famosa Lei Carolina Dickemann, que adiciona os artigos 154-A,154-B, §1º e §2º do 266 e 298 parágrafo único. Mas talvez a mais importante seja o artigo 154-A:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

De acordo com Bezerra (2013):

> O tipo visa tutelar a liberdade individual, mais especificamente o sigilo de dados armazenados em dispositivos informáticos. O delito pode ser classificado como "comum", o que significa que o sujeito passivo pode ser qualquer pessoa, não se exigindo uma qualidade especifica do agente. Assim como o sujeito ativo, o passivo pode ser qualquer pessoa, em especial o proprietário ou possuidor do dispositivo informático, e inclusive terceiros que eventualmente podem ser atingidos pela conduta delituosa.

Legislação que estritamente específica, não fugindo de nenhuma forma após cometido e comprovado. Diferente do crime de dano como visto anteriormente. Além de ser um delito que em relação a maioria das pessoas não é difícil de sofrer tal ato.

Um fato interessante que podemos notar é como a preocupação da sociedade pode interferir em determinados interesses jurídicos. É possível notar a celeridade da transformação de Projeto de Lei para Lei em relação ao Marco Civil da Internet e a Lei Carolina Dieckmann. A transação de PL para Lei do Marco Civil da Internet durou de 24/08/2011 à 23/04/2014 (2 anos, 7 meses, e 28 dias) e transação da PL para Lei Carolina Dieckmann durou de 29/11/2011 à 30/12/2012 (1 anos, 3 meses, e 1 dias).

Podemos considerar que o catalisador desta celeridade tenha sido a divulgação na sociedade de uma ameaça que poderia espreitar qualquer cidadão de bem, Como foi o caso da atriz Carolina Dieckmann da qual inclusive teve o seu nome incorporado na legislação. Proposto este nome em referência na situação que a atriz passou, que, supostamente, teria sido copiado diversas fotos em situação íntima e posteriormente acabaram divulgadas na internet.

E que no Brasil só há proteção para sociedade quando a legislação abrange estritamente determinados delitos. Como demonstrado com legislações como a Lei Carolina Dieckmann, faz-se necessário a criação de legislações sobre áreas onde inevitavelmente pelos avanços tecnológicos deixará algumas lacunas por onde florescer, como ocorre com o meio virtual até hoje.

CONCLUSÃO

O presente estudo partiu de uma análise do tema acerca dos crimes virtuais e suas dificuldades punitivas.

Pretendeu-se com este trabalho conhecer as questões relacionadas com as interações do meio virtual com o meio físico. Especificamente se tratando de crimes dos quais a sociedade em geral está facilmente exposta, pela ilusão de que o praticante do crime não corre o risco de ser descoberto já que a prática do crime não ocorre no ambiente físico, com o praticante inclusive de o praticante podendo estar na comodidade de sua residência afetando terceiros em qualquer parte do mundo. E com o perigo eminente a necessidade de normas que possam cercar as lacunas legislativas que foram aparecendo conforme a tecnologia aprimorava as relações sociais.

Quanto a questão da analogia foi possível verificar que há uma enorme dificuldade para que seja aplicada nas questões relacionadas ao ambiente virtual, já que mais de uma norma, inclusive uma sendo da carta máxima da legislação brasileira, a Constituição Federal, corrobora o princípio da legalidade, onde descaracteriza punições efetuadas a prática de atos que não estejam expressamente contidos em norma reguladora.

Com premissas lançadas ao longo deste trabalho é possível afirmar que há legislações relacionadas com o ambiente virtual no Brasil, mas que ainda se tratando do ambiente virtual é imprescindível a criação de legislações cada vez mais precisas para que as lacunas sejam preenchidas plenamente.

REFERÊNCIA

BEZERRA, Márcia Fernandes. **Apontamentos Sobre o Marco Civil da Internet**. Disponível em: <http://www.santacruz.br/ojs/index.php/JICEX/article/view/76/347>. Acesso em nov. 2016.

BRASIL. **Decreto-lei Nº 3.914, de 9 de dezembro de 1941**. Lei de Introdução do Código Penal.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012.

BRASIL. Lei n 12.965, de 23 de abril de 2014.

BRASIL. Decreto-lei Nº 2.848 de 7 de dezembro de 1940. Código Penal.

CAPEZ, Fernando. **Curso de Direito Penal**: Parte Geral 6. ed. São Paulo: Saraiva, 2003.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais.** São Paulo: Saraiva, 2011.

FONSECA, Cecílio Vieira. **O problema na tipificação penal dos crimes virtuais**. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/13024-13025-1-PB.pdf>. Acesso em: 24 abr.2016.

GATTO, Victor Henrique Gouveia. **Tipicidade penal dos crimes cometidos na internet**. Disponível em: <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=10065&revista_caderno=17>. Acesso em: 12 out. 2016.

GUSTAVO, Luiz de Oliveira Caratti; SILVA, Marília Gabriela. **Os crimes virtuais e a impunidade real**. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=9963&revista_caderno=17>. Acesso em: 06 dez. 2015.

LIMA, Antonio Henrique Maia. **Crimes de internet**: da competência e da dificuldade de obtenção de provas no meio eletrônico. Disponível em: <http://ambito-

juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=14253>. Acesso em: 15 out. 2016.

MIRABETTI. Juliofabrinni. **Manual do direito penal**. 27.ed. São Paulo. Atlas, 2010. V. 2 parte especial.

OLIVEIRA, Moisés Cassanti. **Crimes virtuais, vítimas reais**. Brasport, 2014.

PAIVA, Rafael Rosa Nunes Vieira. **Crimes virtuais**. Disponível em: <http://www.conteudojuridico.com.br/monografia-tcc-tese,crimes-virtuais,37145.html>. Acesso em: 12 out.2015.

PECK, Pratrícia Pinheiro. **Direito digital**. 4 ed. São Paulo: Saraiva, 2010.

PIVA, Emeline Pinheiro. **Crimes virtuais**: uma análise da criminalidade informática e da resposta estatal. Disponível em: <http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2006_1/emeline.pdf> Acesso em: 12 out.2015.

TAVARES, André Ramos; BASTOS, Celso Ribeiro. **As tendências do direito público no limiar de um novo milênio**. São Paulo: Saraiva, 2000.