ISSN 21-76-8498

O DIREITO PENAL BRASILEIRO NO CONTEXTO DOS CRIMES CIBERNÉTICOS

Rafael Silva PADOVEZ[1]
Florestan Rodrigo do PRADO

RESUMO: Na era digital, o domínio da internet atinge não apenas meros cidadãos em busca de entretenimento, mas empresas e até mesmo países, tomando um papel de protagonismo no funcionamento do mundo e se tornando essencial a vida. Nessa dominação virtual, o homem vil, por meio de artifícios, busca vantagens de forma ilícita, surgindo assim os cibercrimes. Uma grande variedade de condutas criminosas passa a surgir, por meio de grandes elaborações, ou até na mais simples conduta de propagar o ódio. Um relatório emitido pela Conferência das Nações Unidas sobre Comércio e Desenvolvimento colocou o Brasil como quarto lugar no ranking mundial de usuários de Internet, tendo 59% de usuários conectados em sua população. Nesse contexto, o Código Penal brasileiro vem se atualizando com o passar dos anos, se aprimorando com fatos recorrentes que vêm a surgir, até mesmo de forma recente, no ano de 2018, mas, ainda assim, a falta de legislação específica se torna um empecilho na busca da segurança digital, bem como a falta de meios e tecnologia para combater e identificar esses criminosos, ameaçando os mais básicos direitos, e muitas vezes dando a sensação de insegurança a seus usuários.

Palavras-chave: Direito digital. Crimes Cibernéticos. Direito penal virtual. Crimes na internet. Direito e internet.

1 INTRODUÇÃO

O mundo moderno e toda sua tecnologia trouxe grandes mudanças, sendo uma das mais relevantes o surgimento e expansão da internet, com seu acesso massivo, atingindo o mundo todo. Ainda que a internet tenha tomado seu papel de importância na atual existência humana, nem tudo funciona perfeitamente, pois o homem busca obter uma vantagem, seja lícita ou ilícita, em tudo aquilo que existe.

Então, a busca por vantagens de forma ilícita trouxe para o grande mundo virtual os crimes, seja os clássicos, não sendo possível datar sua primeira

[1] Discente do 3º ano do curso de Direito do Centro Universitário “Antônio Eufrásio de Toledo” de Presidente Prudente. Rafael.padovez@hotmail.com

prática, como os furtos, bem como novas formas, propiciadas pela inovação tecnológica, chamados então de crimes cibernéticos.

E nessa realidade de um mundo predominantemente digital diversos países do mundo buscam seu combate, com destaque para o Estados Unidos e seu pioneirismo em legislações sobre o tema, e a Europa com a Convenção de Budapeste.

Enquanto isso, em nosso ordenamento jurídico, temos um Código Penal antigo, criado em 1940, há mais de 70 anos atrás, que por mais que venha se atualizando com novas normas, ainda assim, os meios para combater essa forma criminosa são insuficientes.

Essa relação de modernidade, que cresce a cada dia, contraposto a um Direito estático, que evolui em ritmo desacelerado, gera uma grande problemática que sai do mundo virtual.

Por isso, o tema Direito e Internet se torna cada vez mais relevante, uma vez que a função primordial do Direito é por meio das normas controlar a sociedade, trazendo a segurança e estabilidade para que essa avance e não fique próxima a um colapso.

Assim, a busca do presente trabalho é dissecar a evolução das sociedades até onde estamos nos dias atuais, analisando nosso código Penal, desde sua formação, sua eficácia e aplicabilidade nos atuais crimes e situações conflituosas que surgem no ambiente virtual, bem como as leis que surgem para combater essas práticas e as formas de combate desses crimes.

2 A FORMAÇÃO DAS SOCIEDADES DIGITAIS E SUA RELAÇÃO COM O DIREITO

O homem, em sua origem, era nômade, estando assim em constante movimento para sobreviver, vivendo de forma isolada ou em pequenos grupos, buscando sua subsistência nos lugares por onde passava, sem possuir nenhuma forma de organização, vivendo tempos onde a força substituía a lei, e a força era a forma de resolver eventuais conflitos entre aqueles que conviviam apenas para sobreviver.

Porém, o homem não ficou preso a suas raízes de solidão, e passou a ser sedentário, assentando em regiões de prosperidade, formando, assim, as primeiras sociedades, ainda desestruturadas.

As sociedades, desde seus primórdios, estão em constante evolução, e com essa evolução dos povos, surge então o Estado, que busca organizar as sociedades. Em sua obra, Marcus Cláudio Acquaviva (2010, p. 14) diz que “o Estado é uma sociedade necessária e condicionante das demais”, e assim ele surge para organizar as sociedades, e proporcionar os elementos necessários para que ela evolua.

E junto ao Estado surge uma expressão, “*ubi societas ibi jus*”, onde houver sociedade haverá direito, uma expressão de Aristóteles. Uma sociedade sem segurança, com abusos e caótica não prospera, deixando de existir de existir, e então surge o Direito, juntamente com as sociedades, primeiro sobre a ótica de costumes, e posteriormente se positivando, emanando, assim, do intelecto do homem, e emanando ordem para as sociedades.

A ordem traz a segurança e o desenvolvimento para a sociedade, essencial para se chegar no mundo que estamos, porém, por mais que a modernidade nos traga grande qualidade de vida, o Direito não evolui conforme o resto do mundo.

As normas não conseguem se adequar na mesma velocidade em que surgem as questões cotidianas do nosso mundo, sendo que a cada dia surgem novas tecnologias. A Constituição Federal de 1988 em sua classificação é tida como analítica, por ser por ser extremamente extensa e detalhista, possuindo mais de 250 artigos, sendo consideravelmente recente, e, ainda, não está preparada para o mundo atual.

No estudo dos Direitos Fundamentais temos as dimensões dos direitos, que surgem gradativamente. Os mais recentes são os direitos de quarta e quinta dimensão, proporcionados apenas pelas relações que surgem com a globalização e avanços tecnológicos em diversas áreas, como a medicina.

Sobre os direitos de quarta dimensão, existe divergência doutrinária. Parte da doutrina acredita se tratar da engenharia genética, a manipulação de patrimônio genético, e surge o chamado Biodireito.

Quanto à quinta geração, também há divergência doutrinária sobre quais são seus direitos, e da mesma forma, parte da doutrina acredita se tratar da

informática e cibernética, com o avanço das tecnologias virtuais, como a própria realidade virtual, ou a internet, cada vez mais importante

Partindo-se da corrente que afirma estar a quinta geração relacionada à informática e cibernética, como poderia o Direito acompanhar tamanhas inovações que surgem a todo momento, novas tecnologias e situações sem respostas.

O Direito em nossa sociedade é extremamente político, ele se faz por meio de normas, sendo essa uma criação do homem para regular a conduta das pessoas, e, principalmente, em nosso país, o processo de criação de normas é de extrema lentidão, estando atrelado a interesses maiores por parte daqueles responsáveis por sua criação, não apenas na busca da ordem.

Proporcionado por esse avanço tecnológico nas comunicações surge uma Aldeia Global Digital, unindo todas pessoas do mundo, ao mesmo tempo, em um mesmo lugar. Isso se tornou um benefício para diversos ramos, como dos Mercados Financeiro e as empresas.

Forma-se então as sociedades digitais, formada por usuários que se comunicam dentro de um mesmo local virtual, mas distantes territorialmente, trocando ideias, se relacionando, utilizando de seu meio para todas as práticas comuns em nosso mundo, trabalho, entretenimento, conhecimento e outros.

E nesse sentido, cria-se o analfabetismo digital, um problema político-social fundado em diversos trabalhadores não preparados para o uso de novas tecnologias, marginalizando certas pessoas por não estarem preparadas para lidar com esse meio.

3. ORIGEM E EVOLUÇÃO DA INTERNET E A GLOBALIZAÇÃO

Os portugueses, outrora um povo explorador, foram em busca de novas terras, sem conhecer o tamanho do mundo que os aguardava, e em uma de suas buscas pelos povos Indianos eles chegaram ao Brasil, terra de grandes riquezas, até então desconhecidas.

No mundo atual, é difícil existir algum pedaço de terra que o homem não conheça, alguma região inexplorada. E isso tudo foi possibilitado pelas

comunicações, pois foi assim que alianças foram formadas e relações puramente econômicas criadas.

Nesse contexto, surge a internet em 1969, um ambiente virtual, criada pelo Estados Unidos, como um mecanismo de comunicação militar, para evitar eventuais ataques nucleares, e interligar projetos de pesquisas, nessa época chamada de *ARPANet*. Com o fim da Guerra Fria, ela passa a interligar centros de pesquisa e laboratórios, estendendo, assim, seu uso com o tempo.

Por possuir diversos dados militares e o mundo estar em um período de guerra, surgem, então, as primeiras práticas de cunho criminal nesse meio, antes mesmo de ser conhecida como é hoje, por meio de espiões que buscavam essas informações que eram trocadas.

A existência da internet pode ser dividida em quatro períodos. O primeiro foi o uso privado dessa rede, em conexões feitas entre computadores grandes, com aplicação apenas para troca de mensagens e transferências de arquivos, não sendo acessível as pessoas. O segundo período foi a abertura dessa rede para as pessoas, pela linha “discada”, o que ainda era muito lento, mas ainda assim de extrema importância, pois a humanidade passa a ter acesso e utilizar para trabalho ou entretenimento.

O terceiro período é das páginas e sítios, surgindo o conceito de navegação, acesso à banda larga, velocidades que aumentam todos os dias e várias outras inovações. O quarto e último período foi com os smartphones, em que a internet deixa de ser uma rede privada a computadores, e se abrangendo a diversos outros dispositivos, até mesmo televisores.

Não se sabe ao certo quando as sociedades passaram a se relacionar entre si, mas as relações entre povos são necessárias nos dias de hoje, pois alguns possuem matéria prima em excesso, enquanto que outros guardam riquezas tecnológicas não acessíveis a todos, e essa relação de dependência entre povos criou a globalização.

A evolução das comunicações principalmente com o surgimento da internet possibilitou a integração de sociedades distantes, e com essa interação entre povos surge a globalização, um processo de extrema integração política, econômica e cultural entre sociedades do mundo, criando, assim, troca de culturas, conhecimentos, tecnologias e recursos.

Então, a internet toma grande importância em todos aspectos da vida, deixando de ser algo para mero entretenimento, e se tornando fonte de informação, trabalho e organização. Os Estados passaram a utilizar a internet como forma de armazenamento de dados, os Bancos passaram a ter o funcionamento de seus sistemas virtualmente, e a polícia passou a atuar aliada à internet.

O mundo passou a ser digital, e se por alguns minutos essa rede fosse desconectada, poderíamos assumir diversas empresas falindo, estados podendo entrar em colapsos, o mundo ficando em completa escuridão, surge uma relação de dependência da internet.

3 O DIREITO PENAL BRASILEIRO NA ERA DIGITAL

O homem, desde sua mais primordial origem, vive em conflito entre si e com o meio em que vive, tornando-se muitas vezes perigoso para seus semelhantes. Sua história de violência começa nos tempos bíblicos, no livro de Génesis, com a morte de Abel por seu Irmão Caim e, da mesma forma, a primeira punição vem no mesmo período, com a expulsão de Adão e Eva do paraíso por desrespeitarem uma ordem.

A partir do momento que o homem se torna um perigo para aqueles que estão em seu redor surge a necessidade de controle, alguma forma de impedir que suas ações coloquem outros em risco e, como resposta, surgem as penas.

A liberdade sempre foi uma característica do homem e, então, as penas vêm como uma forma de punir o indivíduo, retirando sua liberdade. No ordenamento jurídico brasileiro, é adotada a teoria mista para definir a finalidade das penas, uma junção de outras duas teorias, chamadas de teoria da retribuição e teoria finalista.

Por essa teoria, a pena tem finalidade de retribuição, um castigo contra aquele que cometeu um mal, bem como intimidar a sociedade para que não cometa crimes e, caso cometa, também é um meio para retirar o indivíduo da sociedade a fim de protege-la e ele não mais cometer infrações.

O Código Penal, assim, traz uma série de normas abstratas, descrevendo condutas proibidas, com o fim de proteger os bens jurídicos basilares para a sociedade. A sua importância está atrelada à proteção da sociedade, pois são esses bens jurídicos irradiados pelas normas penais que trazem a sensação de segurança dentro do meio em que as pessoas vivem.

Sem o Direito Penal, a força seria a forma de dominação, não existiria ordem e, por conta disso, toda evolução não seria possível, nem mesmo existiriam sociedades, apenas pequenos grupos vivendo em conjunto, em busca de dominação sobre outros para sobreviver.

Em nosso ordenamento jurídico, já tivemos diversos Códigos Penais, sendo que o código que está em vigência foi criado em 1940, responsável, em sua parte geral, por orientar o interprete quando verificar a ocorrência de uma infração penal, e sua parte especial por definir delitos e cominar penas.

Desde sua criação, o Código Penal brasileiro sofreu muitas alterações, conforme evolui a sociedade se altera o pensamento e também surgem práticas que não eram possíveis no passado.

Quando se pensa na evolução da sociedade chegamos à Internet, com um ambiente virtual, até então inexistente, trazendo uma infinidade de funções e aplicações, atingindo grande parte da população mundial, e evidente, da mesma forma, surgem práticas criminosas antes nunca imaginadas.

No Brasil, o acesso Internet se propagou para grande parte da população, possuindo até mesmo pontos de acesso gratuito, e muitos se tornaram dependentes deste, seja para questões de trabalho, com a figura do *homework*, chamado também de teletrabalhador, ou para entretenimento, pelas redes sociais. E essa propagação do ambiente virtual fez com que práticas criminosas se tornassem comuns nesse meio.

Um grande marco registrado no âmbito digital em nosso país se deu em 2014, com a criação da lei 12.965, chamado de “O Marco Civil da Internet”, que estabeleceu princípios, garantias e deveres para o uso da internet no Brasil. Essa lei foi muito importante, pois trouxe em suas diretrizes garantias ligadas a liberdade de expressão e privacidade de seus usuários, bem como a neutralidade de rede, uma forma de democratização na qualidade do acesso à internet, assegurando a mesma qualidade de acesso à rede mundial de computadores para todos usuários, sem discriminação.

Nessa realidade, é relevante uma análise das principais práticas realizadas nesse meio, haja vista o Brasil ser, segundo o relatório da Conferência das Nações Unidas sobre Comércio e Desenvolvimento, o quarto país no ranking mundial com o maior número de usuários do mundo.

4 AS PRINCIPAIS PRÁTICAS CRIMINAIS DENTRO DO AMBIENTE VIRTUAL

Os cibercrimes são crimes comuns, porém praticadas contra ou com a utilização de sistemas de informática. Para Augusto Rossini (2004):

> [...] 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. 110.).

Existe até mesmo uma classificação para esses crimes, segundo o que preceitua Vicente Greco Filho, em sua obra "algumas observações sobre o Direito Penal e a Internet". Ele divide os crimes cibercrimes em próprios, sendo aqueles cometidos contra um sistema informático, ou impróprios, realizados utilizando um sistema informático como meio, visando ferir outros bens jurídicos. Em suas palavras:

> Em material penal, focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da Internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou (GRECO FILHO, Vicente, 2000, pg. 38).

Os sistemas informáticos são instrumentos como outros já comuns para realizar crimes e, com a Internet surgem novas práticas de crimes. Há de se

dizer que a realização de crimes cibernéticos pode ser feita tanto por sujeitos com conhecimento de programação, como os *Crackers*, ou por pessoas sem grande conhecimento, com condutas mais simples.

4.1 Os crimes contra a honra e de falsa identidade

Com a internet surgem as redes sociais, ambientes de interação entre pessoas. Nessa realidade surge uma nova prática, a criação de perfis *fake*s ou perfis falsos, com informações de outras pessoas ou de pessoas inexistentes.

Muitos começaram a utilizar essa prática inconscientemente, independentemente de sua finalidade, sem saber que se trata de uma prática criminosa, descrita no artigo 307 do Código Penal, o crime de falsa identidade, que tem por conduta “atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem”. (BRASIL, 1940).

Por mais que o artigo não fale expressamente sobre essa aplicação no ambiente virtual, esse dispositivo é aplicado nesses casos, que são muito comuns e muitos, sem saber que se trata de um crime, criam contas falsas deliberadamente.

O crime de falsa identidade pode ser um meio para cometer outras condutas criminosas, sendo esses os crimes contra a honra. Nesses crimes temos a calúnia, difamação e injúria.

São crimes parecidos, mas com condutas próprias. A calúnia é a imputação a alguém de um crime sem que esse exista, ou essa pessoa tenha cometido. Nesse sentido, respondem por esse crime todos aqueles que propalam ou divulgam essa informação, quando souber que essa é falsa. Já a difamação se trata de uma atribuição de uma contravenção penal ou um fato falso a alguém. Ambos os crimes protegem a honra objetiva, a imagem que a pessoa frui a vista da sociedade.

Por fim, a injúria se trata do crime que ofende a honra subjetiva do indivíduo, o sentimento em relação a sua própria dignidade e diferente dos outros crimes, não precisa que um terceiro fique sabendo e nem mesmo deve ser uma falsa afirmação, basta que a vítima se sinta intimamente violada.

Por mais que na Lei 12.965 de 2014 garanta a liberdade de expressão dentro da internet, existe uma linha tênue entre opinião e disseminação de ódio e mentiras e, muitas vezes, por existir o anonimato, as pessoas se sentem livre para praticar tais crimes.

Nesse contexto surge algo que se tornou muito recorrente em nosso país, as *fakes news*, sendo essas notícias falsas, que são propagadas por muitas pessoas. O poder de persuasão dessas notícias é enorme, em grande parte proporcionado pela facilidade de propagação de qualquer tipo de informação no ambiente virtual, atingindo as grandes massas.

Porém, foi recentemente aprovado o projeto de Lei 1978/11, que tipifica o crime de denunciação caluniosa com finalidade eleitoral, assim, a divulgação de notícias falsas com intenções eleitorais passa a ser crime, com uma pena de reclusão de dois a oito anos.

4.2 Estelionato e furto virtual

O comércio tomou seu espaço no ambiente virtual, e se tornou muito atrativo, pois traz uma grande quantidade de produtos. Porém, surgem nesse sentido lojas falsas, para enganar eventuais compradores. Da mesma forma não existe uma lei específica para esse crime, existindo apenas o estelionato, previsto no artigo 171 do CP: “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”.

No mesmo sentido, surge outro crime, chamado de *phising*, no qual os criminosos enviam informações falsas ou apresentam dados para atrair um usuário a adentrar, com anúncios falsos, campanhas imperdíveis ou até mesmo entrar em contanto com o internauta se passando por uma empresa ou pessoa diferente, requisitando dados, para, assim, conseguir dados dos usuários

Essa forma de delito pode recair em até três dispositivos diferentes do Código Penal, podendo ser estelionato (art. 171, CP), caso o agente se utilize de meios para enganar a vítima a passar informações por vontade própria, ou em alguns casos, de forma específica, recaindo sobre o artigo 298 do Código Penal, a

falsificação de cartão, que entrou em vigor em 2012, dentro do artigo de falsificação de documento privado, ou até mesmo recaindo no crime de furto mediante fraude (art. 151, CP), quando o agente enganar a vítima para roubar seus dados sem que ela tenha a intenção de os dar.

Há de se dizer que não deve haver invasão de nenhum dispositivo telemático para obtenção desses dados, senão irá recair no crime previsto no artigo 154-A, podendo estar em concurso com alguns dos crimes anteriormente comentados.

Já o furto se trata de uma ação para subtrair coisa pertencente a terceiro, sem violência ou coação. E em sua concepção, e possível a incidência desse crime nos meios virtuais, pois não há complexidade em sua estrutura. Nesse sentido, surgem diversas decisões do STJ sobre essas práticas.

Foi definido pelo STJ a possibilidade de furto mediante fraude na internet, se diferenciando do estelionato, pois no furto mediante fraude você busca desviar a vigilância da vítima para conseguir o bem, enquanto que no estelionato se busca iludir a vítima para entregar o bem de por vontade própria.

Também, a terceira Seção do STJ definiu o entendimento de furto mediante fraude nos casos de transferência bancária fraudulenta via internet, sem o consentimento do correntista, com competência de julgamento do juízo local, onde se consuma o delito de furto, onde o bem for subtraído.

4.3 Pedofilia e pornografia infantil

No ano de 2009 foi criada a lei 12.015, da CPI da pedofilia, que repaginou o capítulo que trata dos crimes sexuais, mas trouxe equívocos e situações incongruentes, corrigidas pela lei 13.718 de 2018. O crime de pedofilia está no artigo no Estatuto da Criança e do Adolescente, previsto nos artigos 240, 241, 241-A e 241-B, que prevê diversas condutas, mas principalmente filmagens, nudez de menores sendo armazenados, divulgados ou vendidos.

A psicologia e psiquiatria entendem a pedofilia como um comportamento que faz uma pessoa ter atração por crianças ou adolescentes. Na Internet, os pedófilos se utilizam de diversos meios para atrair crianças,

estabelecendo, de forma primária, um contato com elas, introduzindo nos menores uma ideia de que possuir uma relação com um adulto é completamente normal e tentar, assim, marcar encontros.

Outro delito previsto no ECA é a pornografia infantil, que surgiu no ano de 2008, pela lei 11.829, trazendo o artigo 241-E do Estatuto da Criança e do Adolescente. A conduta desse crime implica situações envolvendo crianças ou adolescentes em atividades sexuais explicitas, reais ou simuladas, ou a mera exibição de órgãos genitais para fins primordialmente sexuais.

Ambas práticas são facilitadas na internet, por existir diversos sites que proporcionam esses conteúdos e, assim, muitos pedófilos a utilizam para satisfazer sua lascívia, mediante a utilização de imagens de menores ou os atraindo para encontros.

O STJ vem consolidando a aplicação do ECA nos casos dos crimes envolvendo pedofilia e pornografia infantil por meios eletrônicos. A corte até mesmo concluiu que o mero envio de fotos pornográficas de crianças ou adolescentes já configura o crime, haja vista que o ECA define apenas a publicação e não mera divulgação.

4.4 Invasão de dispositivo informático

No ano de 2012 fora criada a lei 12.737, a Lei dos Crimes Cibernéticos, popularmente conhecida como Lei Carolina Dieckmann, depois de um caso envolvendo uma famosa atriz brasileira, que sofreu uma invasão em seu computador por um hacker, que publicaram imagens íntimas da vítima, invadindo sua privacidade.

Foi, então, trazido por essa lei o artigo 154-A, que diferente do senso comum, que acreditam se tratar a lei Carolina Dieckmann da divulgação de fotos ou conteúdos privados de pessoas, na realidade, o artigo prevê uma conduta de invadir dispositivo informático alheio.

> 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.

Essa lei pune apenas a invasão e não a divulgação ou utilização de qualquer dado obtido pela prática do crime. Mas, ainda assim marcou um grande avanço, que, juntamente com o Marco Civil da Internet, buscam proteger a privacidade.

Sua importância é anda maior, pois foi a primeira tipificação específica de Cibercrimes, mostrando uma preocupação do legislador em proteger as pessoas que se utilizam desse meio, uma vez que os mecanismos de proteção dos sistemas de computadores são insuficientes para proteger os usuários virtuais e, assim, é necessário o surgimento de normas proibitivas contra essas condutas.

Porém, a lei por si só é incompleta, pois apenas pune as invasões, deixando em aberto outras situações, como a divulgação de fotos, cenas, ou desses conteúdos, não existindo uma lei específica para punir esses crimes, que apenas foi surgir no final de 2018, com o artigo 218-C.

4.5 Divulgação de cena de estupro, de estupro de vulnerável, cena de sexo, nudez ou pornografia

No segundo semestre do ano de 2018, surge com a lei 13.718 o artigo 218-C no Código Penal. Esse dispositivo é criado em uma realidade de descontrole nas redes sociais, onde pessoas divulgam diariamente imagens e vídeos de nudez, própria ou de terceiros, se tornando uma prática comum, ferindo diretamente a dignidade das vítimas, que têm sua privacidade violada.

> Art. 218-C: Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio – inclusive por meio de comunicação de massa ou sistema de informática ou telemática – fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável.

Esse crime tem um tipo misto alternativo, possuindo diversas condutas, podendo enquadrar o indivíduo ao oferecer, trocar, disponibilizar, transmitir, vender ou expor a venda, distribuir ou publicar ou divulgar, imagens ou vídeos de cunho

sexual ou que tenha nudez, sem que exista autorização, mostrando uma tentativa do legislador de “pegar” o criminosos por várias formas.

Por mais que esse crime se aplique dentro do mundo virtual, essas condutas podem ser realizadas por qualquer meio de divulgação, podendo ser em jornais, televisão, ou até mesmo com papel impresso.

Mas mesmo sendo uma lei muito importante, ela possui problemas. O primeiro deles é a redação feita pelo legislador, que não é clara em alguns pontos. A lei fala expressamente em visual e audiovisual, ou seja, imagens ou vídeos, mas quando for apenas áudio, não possuindo visual, a lei fica omissa.

A lei também não fala quanto a montagens, ou pessoas muito parecidas, deixando em aberto situações que podem acontecer, pois atualmente existe muita tecnologia de edição. E por fim, é uma lei recente, e poucos sabem que essa conduta, antes praticada desenfreadamente, agora é crime. Assim sua eficácia não é alta, não cumprindo sua função social, pois a sociedade não a respeita.

Apesar de tudo, é uma Lei muito importante, punindo uma prática que vinha se reiterando por todos na sociedade, que viola diretamente os direitos a privacidade e honra dos cidadãos afetados.

5 OS PROBLEMAS DO COMBATE AO CIBERCRIME E A TERRITORIALIDADE DO DIREITO DIGITAL

Grande parte dos juristas brasileiros consideram que cerca de 95% dos crimes cometidos em ambiente virtual já estão previstos no Código Penal e o restante, não tendo previsão, se trata de práticas exclusivas do meio virtual. Mas apesar de haver tipificação para várias condutas, ainda existem diversos problemas.

5.1 A falta de leis específicas bem como suas deficiências

Como já dito anteriormente, a maior parte das condutas estão previstas no Código Penal, porém, ainda assim existe a falta de um tratamento específico a esses criminosos, com aplicação de penas específicas. As punições não são suficientes para coibir criminosos, a vítima sempre fica mais afetada do que o agente, pois esses crimes geram danos psicológicos.

E isso acontece até mesmo com os crimes de lei específicas. A pena do artigo 154-A, da lei Carolina Dieckmann, é de três meses a um ano, sendo de médio potencial ofensivo, podendo ser até mesmo ser substituída por pena pecuniária. Dessa forma, a norma não cumpre sua função em nosso ordenamento jurídico, de intimidar e prevenir novas práticas.

Ainda existem situações que nossa lei não prevê, como os vírus, malwares e Ransomware, pois esses surgiram com a internet, e ainda não possuem nenhuma lei os prevendo como práticas criminosas e, dessa forma, são atípicas, não sendo puníveis. Essas são formas muito utilizadas para praticar o “phising”, como já mencionado, essa forma de atividade na internet para roubar dados.

Além disso, as próprias leis específicas possuem lacunas, não estando preparadas. Um exemplo são os DDoS, ou chamados de Ataques Distribuídos de Negação de Serviço. O centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil define:

> Um ataque DDoS não tem o objetivo direto de invadir e nem de coletar informações, mas sim de exaurir recursos e causar indisponibilidade ao alvo. Os usuários desses recursos são diretamente afetados e ficam impossibilitados de acessar ou realizar as operações desejadas, já que o alvo do ataque não consegue diferenciar os acessos legítimos dos maliciosos e fica sobrecarregado ao tentar tratar todas as requisições recebidas. (CERT.BR, 2016)

A Lei Carolina Dieckmann trouxe o artigo 266 do Código Penal, e sem seu §1°, que diz: “Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta o restabelecimento”. Porém, o próprio dispositivo é incompleto, pois ele diz dispositivo telemático, não abrangendo assim ataques a websites, pois esses possuem outra definição.

Se não bastasse, essa Lei também trouxe outra lacuna, no artigo 154-A. O dispositivo fala apenas sobre dispositivos informáticos, não abrangendo o termo eletrônico, para abranger outros dispositivos, como televisores.

5.2 Formas adequadas e profissionais qualificados

Ademais, ainda que o Código consiga prever quase todas situações, a internet é um ambiente complexo. Pouco adianta existir normas proibitivas se não for possível encontrar os agentes desses crimes.

O processo de investigação de cibercrimes se dá com a identificação da origem da comunicação, pela identificação do seu *Internet Protocol*, também chamado de IP. Todos aparelhos eletrônicos que podem se conectar à internet possuem um IP, sendo sua forma de identificação.

Por meio do IP é possível rastrear o agente do crime até uma localidade, bem como provar a materialidade do crime, pois ele mostra todo tráfego de rede feito pelo usuário, um histórico de sua navegação.

Mas a identificação do IP nem sempre é um trabalho fácil, pois existem diversas formas de se mascara-lo, podendo ser feito até por pessoas sem grande conhecimento de internet, dificultando a identificação deste. Quando se trata de criminosos com grandes conhecimentos, a tarefa é ainda mais difícil.

Nesse sentido, é estritamente necessário a formação de profissionais com conhecimento específico desse meio, pois muitos dos criminosos chamados de *Hackers* e *Crackers* são peritos dentro desse meio e deve-se equiparar conhecimento para realmente ser efetivo.

Além disso, não apenas conhecimento, mas também tecnologia, pois essa evolui todos os dias, ficando cada vez mais rápida e com mais artifícios e, assim, deve se investir nessas tecnologias, para estar a frente, ou pelo menos no mesmo nível dos cibercriminosos.

Existe um procedimento de investigação nos casos dos crimes cibernéticos, com uma ordem de identificação do meio empregado, preservação das provas, identificação dos responsáveis pelo serviço, quebra de sigilo de dados telemáticos (IP e usuário) e comprovação da autoria e materialidade, sendo um procedimento complexo, que depende de celeridade, sendo assim essencial profissionais e equipamentos especializados.

Se não bastasse, para requisitar informações privadas é preciso ordem judicial e o provedor de internet não pode fornecer dados dos criminosos sem um pedido judicial, seja IP, nome ou login. Isso se deve a lei 12.956, o “Marco Civil da Internet”, que trouxe esses direitos aos usuários, e princípios norteadores, garantindo a inviolabilidade da intimidade e da vida privada.

Com tudo isso, surge um sentimento de impunidade, tanto por aqueles que buscam navegar, tanto por quem deseja praticar cibercrimes. A falta de leis específicas com penas próprias para esses crimes e tratamento adequados, bem como a dificuldade de identificar aqueles que cometem essas infrações, torna difícil o trabalho dos órgãos persecutórios.

5.3 Princípio da territorialidade e competência dos crimes na internet

Não existem fronteiras na Internet, todas pessoas de todos países estão no mesmo ambiente, e não é possível definir limites territoriais dentro de cada país no ambiente virtual, não há como parcelar a internet

O princípio da territorialidade do Direito penal define que a lei penal tem aplicação no território do Estado que a editou, pouco importando a nacionalidade dos sujeitos e, assim, crimes cometidos no Brasil são punidos pela lei brasileira, e não avança para territórios de outros Estados. Esse princípio está previsto no artigo 5º do CP: “Aplica-se a lei brasileira, sem prejuízo de convenções, tratados, e regras de direito internacional, ao crime cometido no território nacional”.

Entretanto, a sociedade digital rompe essas barreiras territoriais, construindo um território dificilmente demarcável. Existem alguns princípios nessas questões para se verificar qual lei são aplicáveis aos casos, como o princípio do endereço eletrônico, do local em que a conduta se realizou, do domicílio do consumidor, localidade do réu.

Porém, quando surgem condutas praticadas em territórios de Estados diferentes surgem conflitos, seja de leis ou competência. Na iminência desses problemas, surge a necessidade de cooperação internacional, tratados prevendo como reger eventuais situações e crimes.

A competência jurídica para a internet surgiu em 2012, com a Lei 12.965, o “Marco Civil da Internet”, que determinou os juizados especiais como responsáveis pela decisão sobre ilegalidade ou não de conteúdo, se aplicando também aos casos de ofensa a honra ou injúria. Já nos casos de crimes contra a privacidade ou atos que atinjam bens, interesses ou serviços da União ou de suas autarquias ou empresas públicas, a competência é da Justiça Federal.

A competência de julgamento desses crimes será definida de acordo com o artigo 70 do Código de Processo Penal: “A competência será, de regra, determinada, pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução”.

Mas como já dito anteriormente, em muitos casos é difícil se dizer onde o crime se consumará, pois ele pode ser cometido no ambiente virtual, e surge essa questão, que mais uma vez se reitera, é necessário normas específicas para lidar.

5 CONCLUSÃO

Conforme foi apresentado, a Internet é um ambiente que em grande parte é responsável pelo desenvolvimento do mundo como conhecemos, pelas inovações, formas de se comunicar e, com ela, surge uma grande propagação de informação e relações formadas todos os dias.

Contudo, o homem ainda tem muita dificuldade em lidar com seus crimes que, em grande parte, ficam impunes. Essa realidade vem mudando, cada vez mais a Justiça brasileira julga e pune esses criminosos e surgem novas leis que buscam criminalizar essas condutas.

Existe um projeto de lei do Senado, Nº 236/2012, que altera o Código Penal, na qual parte dos crimes cibernéticos corrige falhas da Lei Carolina Dieckmann, alterando o termo dispositivo informático e inserindo o termo dispositivo eletrônico, para abranger outros dispositivos, como televisores. Ele também traz outros dispositivos, com novos artigos, prevendo novas condutas. A aprovação de leis como essas são importantes, para facilitar o combate, e não deixar lacunas para que algumas pessoas possam praticar seus crimes sem punição.

Mas, ainda assim é necessário a elaboração de Termos de cooperação para suprir as lacunas da lei, criar delegacias especializadas com maior capacitação e estrutura, formando também profissionais mais capacitados, nos setores periciais e de núcleos técnicos, para que os criminosos não estejam a frente das autoridades policiais.

O mais importante é prevenir esses crimes, por meio de conscientização da população, educando para que elas tenham conhecimento sobre os males que existem nesse meio, as formas de realizar crime, ensinar como identificar conteúdos suspeitos. O Ministério Público Federal, em São Paulo e Rio de Janeiro, mantém um Termo de Cooperação Técnica na área de prevenção com a ONG SaferNet Brasil, e já promoveu oficinas sobre o uso seguro e responsável da Internet para professores da rede pública e privada de ensino.

Atualmente existe um projeto de realizar a oficina “Segurança, Ética e Cidadania: educando para boas escolhas online”, em 10 capitais de todo país. Mas ainda sim é preciso estender essa conscientização, educando não apenas jovens e seus professores, mas toda população que utiliza a internet, pois muitos não conhecem os crimes que podem acontecer nesse ambiente.

É um combate difícil, que precisa de mudanças, e como base deve-se olhar também legislações de outros países, como o Estados Unidos, que teve sua primeira Lei aprovada ainda em 1980, e tem uma atuação exemplar do FBI, utilizando estratégias inovadoras e atuando em conjunto com outras organizações, e treinado cada vez mais seus agentes, utilizando até mesmo hackers.

Assim, o Brasil está no caminho para ser um exemplo no combate aos crimes cibernéticos, mas deve-se investir ainda em especialização, conscientização e continuar criando leis específicas com tratamento especial para esses crimes.

REFERÊNCIAS BIBLIOGRÁFICAS

ACQUAVIVA, Marcus Cláudio. **Teoria Geral do Estado.** 3. ed. Barueri, Sp: Manole, 2010. 374 p.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal:** Dos crimes contra a pessoa. 12. ed. São Paulo: Saraiva, 2012. 1260 p. (2).

BRASIL. Código Penal. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em:<http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm> Acesso em: 29 set. 2019.

BORTOT, Jessica Fagundes**. Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileiras e internacional**. Virtuajus, Belo Horizonte, v. 2, n. 2, p.338-362, 2017.

CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança No Brasil. Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS). Disponível em: <http://www.cert.br/docs/whitepapers/ddos/>. Acesso em: 29 set. 2019.

GRECO, Rogério. **Curso de Direito Penal, volume 1.** 19. ed. Nitéroi, Rj: Impetus, 2017. 983 p.

GRECO FILHO, Vicente**. Algumas observações sobre o direito penal e a internet**. Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.

PINHEIRO, Patricia Peck. **Direito Digital.** 5. ed. São Paulo: Saraiva, 2013. 323 p.

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

VALENTE, Jonas. **Relatório aponta Brasil como quarto país em número de usuários de internet.** 2017. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2017-10/relatorio-aponta-brasil-como-quarto-pais-em-numero-de-usuarios-de-internet>. Acesso em: 03 out. 2017.