CYBERCRIMES E A POSSIBILIDADE DE APLICAÇÃO DA LEI MARIA DA PENHA[1]

Marcus Vinicius Santos do Carmo

Marcus Vinicius Feltrim Aquoti

Resumo: Este artigo tem como objetivo por explicar de forma aprofundada oque são os “Ciber Crimes”, sua real importância na sociedade atual, formas de combate ao mesmo, como também sua inserção no contexto histórico dos tempos modernos, também será feita uma análise mais aprofundada na possível aplicação da Lei Maria da Penha em crimes de cyberstalking.

Palavras chave: Ciber crimes. Maria da Penha. Cyberstalking.

ABSTRACT: This article aims to explain in depth what are the "Cyber Crimes", their real importance in the current society, ways to combat it, as well as their insertion in the historical context of modern times, further consideration will also be given to the possible application of the Maria da Penha Law in cyberstalking crimes.

Keywords: Cyber Crimes. Maria da Penha Law. Cyberstalking.

[1] Discente do curso de Direito do Centro Universitário “Antônio Eufrásio de Toledo” de Presidente Prudente/SP. Endereço eletrônico: marcusvinicarmo@gmail.com

2 Docente do curso de Direito do Centro Universitário “Antônio Eufrásio de Toledo” de Presidente Prudente/SP.

1. INTRODUÇÃO

Os Ciber Crimes, ou crimes cibernéticos, ou crimes virtuais, ou crimes informáticos, qualquer que seja sua nomenclatura, são nada mais nada menos que crimes em que o autor se utiliza de meios tecnológicos, de forma predominante, para ferir, constranger ou lesar a vítima de qualquer maneira que seja, mais especificamente através da gigantesca rede mundial de computares e internet. Tal temática, apesar de bastante palpitante, não recebeu a devida atenção na legislação de nosso pais. A falta da compreensão e entendimento aprofundado no assunto fez com que o atual ordenamento brasileiro ainda não tenha feito nenhum tipo de contato com um sistema adequado para tipificar condutas amalgamadas com o uso de tecnologias, sendo assim deficiente na identificação e repressão desses tipos penais. Por se tratar de uma ação advinda diretamente da vontade do homem, os cibe crimes aumentaram ou se pode dizer que surgiram com a recente explosão tecnológica que o mundo presenciou, advinda também da chamada globalização econômica, das comunicações, da cultura e do indivíduo que foram também acompanhadas pelo aumento da criminalidade, ou seja, caso não houvesse tal avanço tecnológico por parte dos homens, sua incidência seria mínima no mundo atual.

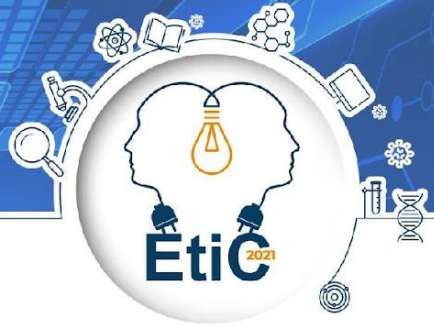
Para uma boa e clara compreensão do assunto, será demonstrado as modalidades e diversificações desse tipo penal, tais como as diversas formas de combate, atuais e antigas, novas medidas que poderiam ser tomadas para prevenir o abuso das tecnologias na incidência de crimes. Tendo também como um ponto a ser problematizado no artigo a questão a da real finalidade de aplicação da lei maria da penha como medida protetiva em casos de crimes de perseguição virtual, ou “cyberstalking”, cometido contra as mulheres.

1.1 CONCEITOS E CARACTERISTICAS

Os chamados crimes cibernéticos são aqueles que se consolidam através de um computador ou dispositivo, onde esse dispositivo pode ser o agente, um mero facilitador ou até a vítima do crime. Questão difícil também é tentar encontrar uma nomenclatura que inclua os delitos cometidos através de uma rede de dados ou um dispositivo tecnológico, por conta dessa dificuldade diversos termos são utilizados erroneamente, dificuldade essa que não é encontrada apenas em território brasileiro, mesmo em países com um entendimento mais avançado do assunto, também se depararam com dificuldades em dar nomes a esses tipos penais, um grande exemplo seria os Estados Unidos da América.

Segundo o doutrinador americano Jonathan Clough, em uma de suas obras sobre cibercrimes o mesmo diz que nenhum dos termos usados atualmente é perfeito, pois não alcançam a totalidade do sentido buscado pelo crime que se quer conceituar, além de Clough, outros estudiosos ainda asseveram sobre o assunto, pois ao que possa parecer, a busca de uma nomenclatura não se trata apenas de mero tecnicismo ou de uma simples discussão terminológica, a ausência de um padrão para nomear esses tipos penais, impede um melhor levantamento estatístico e dificulta a implementação de ações de combate a esse. Do ponto de vista de especialistas e estudiosos, existem dois tipos de cibe crimes, que são separados e tipo I e tipo II, cada qual com suas características próprias e diferenças. Os de tipo I em sua grande maioria tratam de crimes de “pishing”, roubo, manipulação de dados ou serviços, através de vírus ou pirataria, como também roubo de dados ou fraude no setor bancário.

Já os crimes de tipo II incluem, mas não se limitam a atividades como assédio e molestamento na Internet, violência contra crianças, extorsão, chantagem, manipulação do mercado de valores, espionagem empresarial complexa e planejamento ou execução de atividades terroristas, entre outros. Além desse extenso rol de crimes, possui também características próprias que os diferenciam do tipo I, nesse segundo tipo os autores não se utilizam de programas ilegais como no primeiro, e nessa classe também é comum a repetição continua de atos que constrangem, lesam ou agridem a vítima de alguma forma



No que tange a conceituação, além de opiniões próprias é necessário buscar conceitos trazidos por entes renomados, assim preceitua a INTERPOL, 2015:

> É a atividade criminosa ligada diretamente a qualquer ação ou prática ilícita na internet.
>
> (ROSA, 2002, p.53-57). Esse crime consiste em fraudar a segurança de computadores, sistema de comunicações e redes corporativas. Assim o crime na internet, ou cibercrime, nada mais é do que uma conduta ilegal realizada por meio do uso do computador e da internet.

2.3. Surgimento

Não se sabe ao certo a real data de nascimento dos tipos penais conhecidos como cibe crimes, porem tal alcunha surgiu em meados de 1990 com o início da internet, onde a definição apenas fazia menção a um conjunto de atos e problemas causados pela potência da rede computadores e internet, assim como também sendo um fator bastante influenciador, o baixo custo de acesso as redes de telecomunicações e o acesso livre a rede de internet.

Por conta da grande expansão tecnológica que vivenciamos, é evidente que isso traria a sociedade atual grandes benefícios como também carregaria consigo malefícios. Como forma de combater esses malefícios e os evitar, em meados de 2001 foi criada a Convenção de Budapeste, firmado no âmbito do Conselho da Europa, também conhecida como Convenção sobre Cibercrime, sendo essa convenção o único tratado internacional com normas de direito penal e direito processual penal, que versa sobre crimes cibernéticos, tendo como principal objetivo a elaboração de estratégia e plano conjuntos entre os países participantes para o enfrentamento e tipificação de crimes praticados na internet. Atualmente o governo brasileiro não faz parte dessa convenção formada por 60 países, porem já foram tomadas algumas

medidas para que o Brasil ingressa nesse tratado, mesmo que ainda não tenha ocorrido tal junção.

Em meio a uma entrevista, o advogado e especialista Daniel Allan Burg, diz que com a internet o crime se renovou, novas maneiras de se cometer velhos crimes surgiram, assim como com a internet facilita também a impunidade desse tipo de criminosos, onde acabam tornando a investigação mais dificultosa, o advogado também cita alguma das dificuldades que se pode encontrar nessas investigações:

> “A fronteira acaba motivando também, de certa forma, a impunidade, E aqui infelizmente, não tem muito o que fazer. Porque não tem como criar uma lei obrigando o cidadão da Estônia a vir para o Brasil no prazo”

Apesar das dificuldades, o especialista acredita que se houver algum tipo de investimento ou mesmo motivação, tanto em pessoal quanto em treinamento, as investigações podem tomar um rumo mais ágil e fácil para a captura desses tipos de criminosos.

3. MEDIDAS PREVENTIVAS E REPREESSIVAS

3.1 Legislação

No âmbito penal, a legislação brasileira está consideravelmente atrasada e defasada em relação ao combate direto aos crimes cibernéticos, desde a grande explosão tecnológica que o pais conheceu, a legislação vem tratando esses tipos como contravenções penais e crimes comuns. De acordo com os dados de um estudo realizado pela Global Security Map, projeto da organização independente CyberDefcon, o brasil aparece na posição de nº 33, em uma lista de 219 países, em quesito de segurança cibernética. Na opinião de especialistas da área penal e alguns legisladores o atual governo brasileiro não possui um contingente qualificado que consiga tratar de tais problemas, sendo assim um sistema defasado. Para se ter uma

base, o governo americano conseguiu sua primeira aprovação de um projeto de lei a mais de 30 anos atrás, o Brasil teve sua primeira lei aprovada em 2012, que seria a Lei Carolina Dickman. Ou seja, o Brasil está atrasado no implemento de políticas e estratégias de combate aos crimes cibernéticos.

Neste tópico, será abordado o tratamento que é dado aos crimes cibernéticos sob a luz da legislação penal vigente no Brasil, junto ao projeto de lei 236/2012 do senado federal que tem como objetivo instituir o novo código penal brasileiro, como também será realizada uma breve comparação entre os tratamentos dados aos crimes cometidos na internet em diversos países do mundo.

Como já dito anteriormente, o sistema de leis brasileiro é consideravelmente defasado no quesito combate aos crimes cibernéticos, tanto em relação ao cenário internacional quando em relação aos acontecimentos internos, o Brasil está passando ainda pelo processo de informação sobre essa situação, não possuindo medidas muito eficazes para o combate de tais tipos penais, assim como o apoio constitucional só veio a ocorrer recentemente, com a criação de leis, sendo a primeira delas criada apenas em 2012, a chamada lei Carolina Dieckman.

Para contornar a situação ou até mesmo resolve-la, vários estudiosos e especialistas apresentam diariamente hipóteses ou ideias de combate a esses crimes, algumas dessas serão expostas neste artigo.

A discussão sobre o assunto está em pauta a mais de 20 anos no cenário legislativo brasileiro, porem apenas com a lei 12.737 de 2012, sancionada em 2013, apelidada de lei Carolina Dickman, é que se criou o primeiro dispositivo que trata penalmente sobre tais questões, que teve como fato impulsionador o crime de expor na rede de internet fotos intimas da atriz Carolina Dickman e consequentemente impulsionou também a questão sobre os demais crimes cibernéticos.

Com a entrada em vigor da Lei acima mencionada, o atual código penal brasileiro passou então a tipificar o crime de Invasão de Dispositivo Informático, previsto no art. 154 – A do mesmo código, da seguinte maneira:

> 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.

Uma vez que o tema ganhou mais destaque desde a criação da Lei Carolina Dickman de 2012, passando também pelo Marco Civil da Internet, Lei 12.965/2014, ambos os dispositivos serão tratados mais detalhadamente a seguir.

A Lei 12.737/2012, diz expressamente em seu texto:

> “Invadir dispositivo informáticos alheio, conectado ou não a 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. ”

Apesar de ter sido considerada um grande avanço para o sistema penal brasileiro, ainda existem muitas críticas não só ao sistema em geral, mas também em especifico a essa lei também. Sendo assim, por mais que tenha sido um grande impulso para a tipificação desses tipos penais a legislação continua a ser algo defasado e ineficiente nesse quesito.

Um ponto bastante criticado dessa lei, é a condição posta sobre o crime de apenas ser tipificado como fato típico se houver a presença de uma barreira de segurança, onde o indevido acesso por si só não seria punido, apenas se houvesse a violação de uma barreira de segurança.

Quanto á essas críticas entre outros empecilhos que a legislação encontra, tramita sob o Congresso Nacional o projeto de lei nº 236/2012, que visa instituir um novo Código Penal brasileiro, por consequência das grandes mudanças ocorridas desde a época em que foi instaurada a legislação vigente no Brasil.

Esse novo projeto de lei, além de idealizar um novo código penal, também trouxe consigo mudanças nos artigos que versam sobre os cibe crimes, com o objetivo de corrigir falhas e lacunas apresentadas anteriormente, como as já mencionadas na Lei Carolina Dickman, alterando o texto na parte em que dizia especificamente que o sistema informático deveria apresentar alguma barreira de segurança para configurar uma invasão.

Outro ponto que merece um certo destaque, está diretamente relacionado ao caso da atriz, diz respeito a obtenção de dados privados e sua divulgação, e por questões ainda indefinidas tal conduta não foi tipificada pela lei.

A lei 12.965/2014, aprovada no Congresso Nacional em 2014, também chamada de Marco Civil da Internet, foi uma lei que veio a apresentar de forma sistematizada exatamente dez princípios, que preveem o que se pode ou não fazer no âmbito civil, antes de se criminalizar condutas praticadas na internet. De forma controversa, a MCI possuía um caráter antagônico aos projetos de crimes na internet, acarretando assim a criação da Lei 12.737/2012.

Os princípios ou mandamentos presentes na Lei do MCI, são considerados um alicerce responsável por garantir a liberdade de expressão, como também a privacidade e os direitos humanos no âmbito digital, porém sem que seja impossibilitado o controle necessário a segurança de dados e sistemas pessoais entre outros. Mandamentos esses presentes no art. 3º de seu texto, assim:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I – garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
>
> II - proteção da privacidade;
>
> III - proteção dos dados pessoais, na forma da lei;
>
> IV - preservação e garantia da neutralidade de rede;
>
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
>
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
>
> VII - preservação da natureza participativa da rede;
>
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
>
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

A disciplina desses mandamentos tem por objetivo a promoção de um acesso à internet seguro a todos, acesso a informação, e um adesão a uma nova sociedade tecnológica benéfica para todos.

3.1.1 Lei Maria da Penha

No ano de 1983, uma mulher chamada Maria da Penha foi vítima de dupla tentativa de feminicidio, por parte de Marco Antônio Heredia Viveros, que na época costumava ser seu companheiro e marido. O agressor desferiu contra a vítima um tiro nas costas enquanto a mesma dormia, resultando em lesões irreversíveis na vertebra e medula e medula, e consequentemente Maria da Penha veio a fica paraplégica.

Após ocorrido o fato, o agressor declarou a polícia, que o incidente veio a ser consequência de uma tentativa de assalto, o que posteriormente desmentido pela perícia. As agressões continuaram após a vítima retornar de seu tratamento, agressões do tipo cárcere privado e tortura por eletricidade.

Compreendendo a situação e presenciando a inércia das autoridades, a família e amigos conseguiram dar apoio jurídico a ela e assim movimentando sua saída de casa sem que configurasse abandono do lar, e consequentemente não perdendo a guarda de suas filhas.

Não bastando tal humilhação, em meados de 1991 aconteceu o primeiro julgamento de Marco Antônio, oito anos após o crime. Sendo o autor sentenciado a 15 de anos de prisão, porem devido a recursos impostos pelos seus advogados de defesa, o mesmo saiu do fórum ainda em liberdade. Mesmo humilhada e fragilizada, Maria da Penha insistiu em sua justa causa, relatando até sua história em um livro publicado em 1994.

O segundo julgado do agressor, só veio a acontecer em 1996, onde o mesmo dessa vez foi condenado a 10 anos e 6 meses de prisão, porem novamente, sob alegação de irregularidades processuais, não teve sua sentença cumprida. Em

1998, Maria da Penha sofreu outra derrota, o caso havia ganho uma dimensão internacional, sendo levado como denuncia até a Comissão Interamericana de Direitos Humanos da Organização dos Estados Americanos (CIDH/OEA), onde foi trazido como uma questão grave de violação de direitos humanos e deveres protegidos por documentos que o próprio estado assinou, no entanto, o Estado brasileiro permaneceu omisso, não se pronunciando no decorrer do processo até seu fim.

Por conta de sua omissão, em 2001, o Estado foi responsabilizado por sua negligencia e irresponsabilidade em relação a clara violação de direitos humanos de uma pessoa, e uma certa tolerância em relação à violência doméstica praticada contra as mulheres brasileiras.

Diante da falta de medidas legais e ações efetivas por parte do estado responsável, em 2002 foi realizado um Consórcio de ONGs feminista, com o intuito de criar uma lei de combate à violência doméstica e familiar contra as mulheres.

Após diversos debates e discussões entre os três poderes, o projeto de Lei n. 4.559/2004 da Câmara dos Deputados alcançou o Senado Federal, e por seguinte sendo aprovado por unanimidade em todas as Casas. E logo após isso, exatamente em 7 de agosto de 2006, o Presidente Luiz Inácio Lula Da Silva, sancionou a Lei n. 11.340, também comumente conhecida como Lei Maria da Penha. Além de que, por recomendações do CIDH, a lei foi batizada com o nome da vítima do caso mais simbólico, além de ser indenizada tanto material quanto simbolicamente, como forma de reconhecimento de sua luta.

Com a Lei Maria da Penha, a violência doméstica passou a ser tipificada como uma das formas de violação aos direitos humanos, entendida também como problema de saúde pública pela Organização Mundial de Saúde (OMS).

3.1.2 Relação De Crime De Cyberstalking E A Lei Maria Da Penha

O crime de Cyberstalking, é o mesmo que o crime de perseguição, porem neste o autor se utiliza de meios tecnológicos e rede de internet para o fazer, sendo assim uma perseguição virtual.

A Lei 11.340 sancionada em 7 de agosto de 2006, comumente conhecida como Lei Maria da Penha, com 46 artigos distribuídos em 7 capítulos, tem como objetivo criar mecanismos para coibir a violência contra a mulher no âmbito doméstico e familiar, em conformidade com a constituição federal.

Para se traçar a linha que relaciona o crime de cyberstalking e a lei maria da penha, através de um estudo minucioso e analises de casos concretos, pois por se tratar de um tipo penal recente no nosso ordenamento, pouco se sabe ou se tem histórico nesses tipos de condenações, principalmente, nessa questão da Lei Maria da Penha em especifico.

O ano de 2020 pode ser considerado um marco importante para essas questões, pois nesse mesmo ano uma juíza do estado de São Paulo deferiu liminar, a pedido da defensoria, para que se adotassem medidas protetivas a uma mulher vítima de stalking.

O caso teve uma repercussão considerável, onde desde 2016, data em que a vítima conheceu o réu, ao passar do tempo o réu se mostrou tão insistente que a jovem moça teve que bloquear os contatos eletrônicos que possui com o criminoso, criando também vários perfis “fakes” para entrar em contato com a mesma, também com a intenção de difama-la. A Defensora Pública Mariana Chahib ainda afirma:

> “Apesar de aparentemente não se tratar de violência no âmbito domésticos, trata-se de situação sui generis, que permite a aplicação da Lei Maria da Penha”... “Tendo em mente que o objetivo primário da lei é a proteção da mulher em decorrência de seu gênero, deve-se levar em consideração que o requerido, por toda a narrativa trazida, acredita veementemente que viveu, vive ou viverá em um relacionamento amoroso com a requerente”.

A magistrada proibiu o acusado de se aproximar ou fazer qualquer tipo de contato com a vítima e seus familiares, sendo também adotadas as medidas

protetivas para garantir a segurança e integridade da mulher. Por se tratar de um julgado recente, ainda não é possível vislumbrar uma solução clara para essa problematização, porém é um grande avanço e pode ser um marco de avanço para a questão, e consequentemente podendo influenciar e auxiliar em decisões de casos futuros semelhantes a esse.

3.2. Investigação e Tipos penais

Os crimes cibernéticos, como a maioria dos crimes comuns não possuem um padrão de pessoas que os cometem, podendo ser de qualquer tipo, gênero e etc., e por conta de ter como meio de execução dispositivos eletrônicos e a rede de internet, quem menos se espera, é quem pode estar cometendo um ilícito a qualquer momento que seja, sem que nenhuma pessoa a sua volta perceba. Ou seja, qualquer pessoa que tenha acesso a um dispositivo ou meio de telecomunicação, pode estar cometendo um crime, assim não existindo um tipo principal de autor para os crimes cibernéticos.

Porem um dos principais desafios é realmente identificar o autor do crime, por conta de usarem meios de mascarar suas atividades e se tornarem a qualquer tipo de rastreamento, especialistas explicam que um dos maiores obstáculos é a falta de obrigação que os servidores têm de guardar as informações de seus usuários, portanto mesmo que o autor não utilize artimanhas para se tornar invisível, os servidores não possuem obrigação nenhuma de registrar seus dados e atividades.

Mesmo que não haja em vigor uma lei que exija uma identidade digital obrigatória, existe na Constituição Federal Brasileiro um dispositivo que proíbe o anonimato, entrando assim em uma certa contradição onde o próprio autor do crime é protegido pela falta de um dispositivo processual que exija a identificação digital, porem já houveram diversos casos em que lan houses foram responsabilizas por conta da não obrigatoriedade de uma identidade digital obrigatória, pois ocorria de no ambiente público os autores se utilizavam da rede pública do estabelecimento para cometerem seus crimes e não precisando se identificar, assim se tornando de certa forma invisíveis a qualquer rastreio.

Porém, por opiniões diversas, como de juristas e profissões de direito, entendem que as atuais decisões tomadas na justiça já mostram que os servidores devem fornecer essas informações, para que não sejam responsabilizados pelos atos de outros, os servidores deveriam armazenar e fornecerem informações importantes para rastreio, como por exemplo endereço de IP.

O meio digital por incrível que pareça, deixa muito mais pistas do que se pode imaginar, podendo até ser mais fácil o rastreio em comparação aos crimes físicos, são as chamadas pegadas tecnológicas. Por conta de os endereços de IP, por exemplo, levarem as autoridades até um ponto de acesso e não ao autor do crime, as pegadas tecnológicas encontram dificuldades nessa parte, por isso a maioria dos criminosos cibernéticos vão a lan houses ou cyber cafés para cometerem tais atos.

Na maioria dos casos, quando se tem a notícia da pratica de algum crime desse tipo, muito comumente as pessoas já assimilam ao termo “hacker”, porem ocorre que, tal termo tem sido usado sem o devido entendimento do mesmo. O termo hacker se refere a um usuário experiente, que por ser um exímio programador, utiliza de suas habilidades para invadir sistema, porém sem danifica-los, nem obter dados ou sequer destruí-los. Já o cracker, outro termo um pouco menos usado e pouco conhecido, se refere ao indivíduo que invade sistemas, precisamente com a finalidade de roubar informações e causar danos as vítimas, também podendo ser uma denominação associada a aqueles que destroem proteções de softwares e decifram códigos, geralmente em prol da pirataria.

Por conta de se tratarem de crimes que tiveram seu surgimento recentemente, vindo juntamente com a modernização global e tecnológica, as principais vítimas dos crimes cibernéticos são aquelas que tem pouca afinidade ao uso dessas ferramentas, sendo elas em sua grande maioria idosos. Não é descartado também que jovens e as demais pessoas não podem ser vítimas, como por exemplo nos crimes de cyberstalking, onde pode acontecer com pessoas de qualquer idade, tendo afinidade ou não com tecnologia, sendo até mais frequente que ocorram entre os jovens. Porem pessoas idosas, com pouca informação e contato com dispositivos tecnológicos, são comumente vítimas de fraudes entre outros crimes do tipo, pois por

não possuírem informação suficiente e nenhum tipo de acompanhamento acabam por fornecer suas informações aos criminosos, tal situação não é rara atualmente.

Já nos crimes de tipo II, como já dito anteriormente, não existe um padrão para suas vítimas, como os de tipo I. Tanto os autores quanto as vítimas, podem ser de qualquer tipo, idade ou gênero, mas também sendo mais comum que as vítimas sejam jovens.

4 A INCIDÊNCIA DO CRIME DE PERSEGUIÇÃO DIGITAL E O POSSÍVEL CONCURSO COM OUTROS CRIMES

4.1 Concurso Entre Ciber Crimes

Como já é dito no atual código penal brasileiro, tanto na parte especial quanto na parte comum do código, existe a possibilidade de ocorrer o concurso entre dois ou mais crimes, sejam eles da parte especial ou da parte geral, e neste tópico terá enfoque nos crimes cibernéticos e o concurso entre eles.

Primeiramente se deve ter uma noção do que é o concurso de crimes, é a nomenclatura dada à pratica de mais um crime por parte do agente ou agentes, se subdividindo em concurso material, concurso formal e crime continuado. O concurso material tem sua base em texto de lei.

> Art. 69 – Quando o agente, mediante mais de uma ação ou omissão, pratica dois ou mais crimes, idênticos ou não, aplicam-se cumulativamente as penas privativas de liberdade em que haja incorrido. No caso de aplicação cumulativa de penas de reclusão e de detenção, executa-se primeiro aquela.

Assim, é possível, portanto que incorra em concurso material também em crimes cibernéticos, como por exemplo, no ato de invadir um computador alheio sem a permissão do dono, já configurando um crime, roubar informações e divulga-las, mais de uma ação para mais de um crime, sendo assim as penas aplicadas

cumulativamente. Também se subdividindo em homogêneo e heterogêneo, tais classificações estão presentes no artigo 69 do Código Penal.

Já o concurso formal, tendo seu texto no artigo 70 do mesmo código, ocorre quando o autor do ato, mediante uma única conduta ou omissão, pratica dois ou mais delitos, sendo eles iguais ou não. No caso de ciber crimes, pode ser por exemplo, o autor realiza apenas a conduta de difamar ou cometer o ato de injuria em chats online, ao mesmo tempo em que divulga sem autorização devida informações da vítima.

> Art. 70 – Quando o agente, mediante uma só ação ou omissão, pratica dois ou mais crimes, idênticos ou não, aplicasse-lhe a mais grave das penas cabíveis ou, se iguais, somente uma delas, mas aumentada, em qualquer caso, de um sexto até metade. As penas aplicam-se, entretanto, cumulativamente, se a ação ou omissão é dolosa e os crimes concorrentes resultam de desígnios autônomos, consoante o disposto no artigo anterior.

4.1 POSSIBILIDADE DE CONCURSO ENTRE CRIMES COMUNS E CRIMES CIBERNÉTICOS

Como já dito no tópico anterior, tanto na parte geral quanto na especial do código penal, é possível que exista o concurso de qualquer tipo de crime, não sendo uma exceção o concurso entre crimes cibernéticos e crimes comuns. É possível que incorra também tanto em concurso formal quanto material, duas condutas e um crimes, ou dois crimes para uma conduta, desde que um deles seja tipificado como crime cibernético e o outro crime comum é possível. Como por exemplo, o crime em que o agente se utiliza da sua função para invadir computador da empresa e roubar dados, resultando em uma conduta para dois crimes.

5. CONCLUSÃO

Diante do que foi exposto neste artigo acadêmico, é possível alcançar a conclusão de que o tema de Cyberstalking e a possível aplicação da lei maria da penha possui um grande nível de complexidade, e para entender o estudo em sua

integridade é necessário que se alcance também o entendimento de outras áreas do código penal, como a legislação em seu inteiro teor. Com base em opiniões de especialistas e estudiosos do direito, tem-se também o conhecimento sobre o quão defasada nosso ordenamento atual é em relação aos ciber crimes, quais os obstáculos que as autoridades encontram nesse meio digital, como também casos detalhados que vivenciamos nos tempos modernos, é necessário fazer uma análise de todos esses pontos, como também de várias investigações para que seja possível se aprofundar de forma satisfatória no tema.

Além de ser necessário um estudo critico que faça o levantamento de todas as conjecturas acerca do respectivo tema, ainda assim se é com o objetivo de que presenciemos mudanças na atual legislação brasileira é preciso fazer mudanças não só no campo penal, mas também no social, e assim alcançar uma forma harmoniosa, positiva e segura para a sociedade no âmbito digital e tecnológico, trazendo assim uma série de benefícios.

6. REFERENCIAS BIBLIOGRAFICAS

BARRETO, Alesandro Gonçalves, BRASIL, Beatriz Silveira. Manual de Investigação Cibernética à luz do Marco Civil da Internet. 1 Ed., São Paulo: Brasport, 2016.

BARRETO, Alesandro Gonçalves, DOS SANTOS, Hericson. Deep Web: Investigação no Submundo da Internet. 1 Ed., São Paulo: Brasport, 2019.

BARRETO, Erick Teixeira. Crimes Cibernéticos sob a égide da Lei 12.737/2012. Revista Âmbito Jurídico.

BITENCOURT, Cezar Roberto. Tratado de Direito Penal - Parte Geral. 21ª edição, volume 1, São Paulo: Saraiva, 2015

BRASIL, Código penal – Promulgado em 07 de dezembro de 1940. São Paulo: Saraiva, 2019.

GOMES, Luiz Flavio, Bianchini, Alice. Crimes Informáticos e suas Vítimas. 2 Ed., São Paulo Saraiva, 2015.

JESUS, Damásio, Milagre, José Antonio. Manual de Crimes Informáticos. 1 Ed., São Paulo: Saraiva, 2017.

MARCACINI, Augusto Tavares Rosa. Aspectos Fundamentais do Marco Civil da Internet: Lei nº12.965/2014. São Paulo: Edição do autor, 2016.
MATTOS, Alexandre. Crimes na Internet. 1 Ed., Rio de Janeiro: Espaço Jurídico, 2012.

MIRABETE, Julio Fabbrini. Manual de Direito Penal - Parte Geral. 23ª ed., v. I, São Paulo: Editora Atlas, 2006.

Oliveira, William César Pinto de. Lei Carolina Dieckamnn. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 18, n. 3506, 5 fev. 2013. Disponivel em: https://jus.com.br/artigos/23655.