KAMYLLA CAROLINE OLIVEIRA DIAS

INFILTRAÇÃO POLICIAL EM CRIMES CIBERNÉTICOS Á LUZ DO ORDENAMENTO JURÍDICO BRASILEIRO

CURSO DE DIREITO – UniEVANGÉLICA

2020

KAMYLLA CAROLINE OLIVEIRA DIAS

INFILTRAÇÃO POLICIAL EM CRIMES CIBERNÉTICOS Á LUZ DO ORDENAMENTO JURÍDICO BRASILEIRO

Monografia apresentada ao Núcleo de Trabalho de Curso da UniEVANGÉLICA, como exigência parcial para a obtenção do grau de bacharel em Direito, sob a orientação da Professora M.e Karla de Souza Oliveira.

ANÁPOLIS - 2020

KAMYLLA CAROLINE OLIVEIRA DIAS

INFILTRAÇÃO POLICIAL EM CRIMES CIBERNÉTICOS Á LUZ DO ORDENAMENTO JURÍDICO BRASILEIRO

Anápolis, _____ de Novembro de 2020.

Banca Examinadora

_____

_____

AGRADECIMENTOS

Primeiramente a Deus, que me concedeu com sabedoria e guiou-me na laboração do presente trabalho.

Aos meus familiares e amigos pelo apoio.

A minha professora e orientadora Karla, por seguir avante comigo nesta caminhada acadêmica, cooperando sempre com o seu conhecimento, carinho e dedicação.

E aquelas pessoas que de perto ou de longe contribuíram para meu sucesso.

Muito obrigada.

“A justiça não consiste em ser neutro entre o certo e o errado, mas em descobrir o certo e sustentá-lo, onde quer que ele se encontre, contra o errado”

Theodore Roosevelt

RESUMO

A pesquisa tem por base elucidar e desenvolver discussões sobre a investigação do *cibercrime*, dimensionando sua importância diante da problemática de peculiaridades que os delitos informáticos abrangem. O foco do estudo está centralizado na infiltração de agentes policiais como um instrumento de prevenção e repressão, usado para combater e obstaculizar ações praticadas na maioria das vezes por organizações criminosas, apontada pelos autores como um dos fatores de incidências de ilícitos penais no ambiente virtual. O objetivo do estudo é identificar as mudanças que foram empreendidas no cenário atual com o surgimento da *internet* e do déficit de conteúdo jurisdicional acerca do tema debatido. Com intento de demonstrar como está a preparação do Estado diante da inovação no qual toda a sociedade foi integrada. O estudo se realizou a partir dos pressupostos teóricos e jurídicos de autores que pesquisam sobre o delito informático, no campo que esgrimem os propósitos da prática do *cibercrime*. Contestam-se as dinâmicas atuais aplicadas, a partir dos seguintes autores: Greco (2015); Rossini (2002), Costa (1995), Ramalho (2002), Nogueira (2008) e outros autores citados na pesquisa. A metodologia utilizada orientou-se pela pesquisa bibliográfica e exploratória centrada nas contribuições teóricas dos autores que realizaram estudos sobre o crime virtual no contexto jurídico. As reflexões deste estudo realizado sugerem uma mudança que possa agregar na legislação vigente maiores diligências, assim como suprir a carência do Direito Penal Brasileiro. Este novo paradigma exige uma nova postura comprometida efetivamente com o âmbito virtual, por meio dos Tribunais Superiores, a partir de uma postura democrática, transparente e jurídica no processo de investigação.

Palavras-chave: *Cibercrime*; *Internet*; Redes Sociais; Computador.

SUMÁRIO

INTRODUÇÃO

O presente trabalho aborda a temática da infiltração policial em crimes cibernéticos. Ademais, evidencia os prós e contras de sua utilização como ferramenta auxiliar na resolução de crimes executados pela internet.

O propósito da investigação cibernética, é destituir as organizações e associações criminosas. Essa afirmativa de apuração, deve ser encarada como um dos instrumentos presentes dentro ainda do curso do inquérito policial, e integrada quando já estiverem sido esgotados todos os outros recursos disponíveis.

A pesquisa foi desenvolvida em três capítulos e as considerações finais. A parte introdutória apresenta uma visão geral do problema, com fulcro nos crimes virtuais. Dessa forma, busca esclarecer a relevância do tema e definir de forma clara e coesa os objetivos deste estudo.

O primeiro capítulo aborda o tema infiltração policial e sua natureza jurídica, ao demonstrar como foi dado o trajeto de toda *internet* até os dias atuais e abordagens a respeito de sua evolução, seus avanços e retrocessos, apontando-se o cenário jurídico atual.

O segundo capítulo apresenta como é formada uma conduta indevida no *cibercrime*, enfocando-se nas práticas descritas como ilegais. Nesse capítulo a discussão é mais entorno das concepções dos autores a respeito da legalidade discutida dentro do espaço-tempo internet. A forma com que a *internet* impõe como legal e permitido, e um pouco do que é de fato proibido realizar, fazer ou manter com acesso a redes de dados.

O terceiro capítulo busca ressaltar a importância de uma legislação completa como um elemento necessário, para uma construção de segurança maior dentro da própria plataforma. Através das investigações, visa uma nova oportunidade para o Estado implementar mudanças na própria matéria jurisprudencial. Para melhor atender a demanda da população, um novo caminho para a superação de limites jurídicos anteriores precisa ser adotado.

Registra-se que esse estudo pode contribuir com todos aqueles que buscam novos caminhos e reformas competentes na legislação brasileira. No que condiz ao *cibercrime*, a fim de aperfeiçoar sua jurisprudência de forma eficaz. Isto pois, é de extrema relevância que o ordenamento jurídico possa se antecipar quanto a aprovação de projetos de lei, com relação a essa temática, antes que também tornem-se antiquados para as gerações futuras, mas prósperas para geração presente.

CAPÍTULO I - CRIMES CIBERNÉTICOS

Esse capítulo trata acerca do conceito e natureza jurídica de crimes cibernéticos, em seguida, discorre sobre o surgimento *da internet*, e por fim, aborda a respeito da evolução dos crimes cibernéticos.

1.1 Conceito e natureza jurídica

A criminalização tem sido amplamente afetada por meio de plataformas digitais, seja de maneira formal ou informal, ocasionando inquietação no sistema judiciário e de maneira geral no seio da sociedade. Nesse sentido, esse capítulo busca de forma sucinta nos estudos de autores como Greco (2015), Rossini (2002), Costa (1995), Ramalho (2002), Nogueira (2008) e outros autores citados, as diferentes concepções e interpretações diante o posicionamento do ordenamento jurídico, bem como, compreender os propósitos da prática do *cibercrime*, seus avanços e retrocessos.

A princípio, para pontuar o *cibercrime* é preciso conceituar o que é um crime. Segundo Rogério Greco, analiticamente da seguinte maneira: “analisa todos os elementos ou características que integram o conceito de infração penal sem que com isso se queira fragmentá-lo. O crime é, certamente, um todo unitário e indivisível.” Em outras palavras, quando o autor pratica um ato delinquente de modo

transgressivo, a infração realizada deve ser ponderada como um inflexível penal (2015, p. 142).

Denota-se crime cibernético ou delitos informáticos, toda e qualquer infração penal realizada por meio do ciberespaço, seja de maneira formal ou informal, na qual a *internet* é o portal de entrada principal, em que infames ficam livres para cometer quaisquer tipos de delitos ilegais. Em virtude disso, os usuários estão cada vez mais expostos e vulneráveis na utilização de aplicativos comunicativos e redes sociais no seu cotidiano.

Segundo LÉVY, a definição de ciberespaço se denota como:

> O ciberespaço (que também chamarei de rede) é o novo meio de comunicação que surge da interconexão mundial de computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ele abriga, assim como os seres humanos que navegam e alimentam esse universo. Quanto ao neologismo cibercultura, especifica aqui o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem no juntamente com o crescimento do ciberespaço (2000, p.17).

Com a vinda de um novo meio de conversação, o ciberespaço ganhou visibilidade por se tratar de um ambiente onde as pessoas poderiam manifestar suas emoções, compartilhá-las com outros de acordo com suas afinidades, tudo de forma exclusivamente digital, dado que não há a existência desse espaço no modo físico. Na concepção de William Gibson, o ciberespaço é como a mente humana que reserva todas as memórias do homem, ora a encenação de um novo universo paralelo, no qual os humanos decidiram fazer morada (2002, p. 53).

O indivíduo integrante da sociedade e que pratica uma conduta delituosa com o propósito de induzir, propiciar, partilhar, alienar ou facilitar a propagação da imagem, vida particular de outrem, deverá ser enquadrado na conduta de prática ilegal prevista na Constituição Federal, em seu artigo 5º. Infere-se que a aquisição de quaisquer desses elementos sem a anuência do responsável, demonstra a culpabilidade e intenção clara e objetiva do agente infrator.

Por sua vez, Rossini preceitua delito informático como um procedimento ilícito. Ao ser cometido por uma pessoa de imagem particular ou pública, por meio

de ferramentas digitais, seja dentro ou fora dessa esfera, o delito é considerado típico e delituoso. Na ocasião em que provocar direta ou indiretamente ofensas ao sistema tecnológico. Além de tudo, constitui em assegurar e manter o sigilo das informações, a flexibilidade com que as mesmas são transmitidas, assim como certificar-se que o homem não esteja desemparado nesse ambiente (2002, p. 133).

Guilherme Guimarães Feliciano expressa a criminalidade informática como sendo “o recente fenômeno histórico-sócio-cultural caracterizado pela elevada incidência de ilícitos penais (delitos, crimes e contravenções) que têm por objeto material ou meio de execução o objeto tecnológico informático (*hardware, software* e redes)”. Consequentemente é preciso alcançar um dos meios de transmissão para concluir de fato o delito dentro deste local (2000, p. 42).

Em outra oportunidade, Augusto Rossini acrescenta o motivo pelo qual assim denomina esse tipo de delito, “pois dessa forma, não envolvem tão somente aquelas ações praticadas no âmbito da *internet*, mas toda e qualquer conduta em que houver ligação com sistemas informáticos- quer de meio- quer de fim, de forma que essa intitulação englobaria, até mesmo, infrações em que o computador seria um simples apetrecho, sem a vital conexão à rede mundial de computadores” (2002, p. 133).

O que pode ser observado, com o advento da tecnologia, é o constante crescimento de mudanças no comportamento cotidiano, a sociedade moderna precisou se readaptar a novas formas de comunicação. Isto pois, aumentou a proporção de dependentes dessa plataforma virtual, seja no quesito profissional ou individual, trazendo consigo vertentes positivas e negativas.

Na percepção de Costa, o crime de informática poderá ter a seguinte caracterização:

> O crime de informática pelo bem jurídico protegido. É a conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar (1995, p. 4).

Acrescenta Túlio Vianna, que delitos informáticos são: “crimes impróprios, nos quais o computador é utilizado como instrumento para a execução do crime, sem que haja ofensa a inviolabilidade da informação automatizada como no caso dos crimes contra a honra; próprios, nos quais a tutela jurídica protege as informações ou dados, a exemplo da interceptação telemática ilegal” para mais, subentende que existe uma terceira caracterização mista que ampara os patrimônios sob circunstâncias de extravio (2003, p. 170).

Bem lembrado por Ramalho Terceiro, uma hipótese que diferencia o crime virtual dos demais é pelo fato de:

> Os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da *internet* são denominados de crimes virtuais, devido à ausência física de seus autores (2002, p. 58).

O que antes era possível ser praticado apenas de forma física, eventualmente com sua ausência, abriu uma porta de possibilidades que facilitaram a execução de delitos virtuais. Por outro lado, permitiu que alguns dos usuários conseguissem atingir uma ou mais pessoas em tempos diversos ou sincronizados em um mesmo horário, independentemente da presença ou local usado para o crime.

O indivíduo que obtém conhecimento de um sistema operacional ou também descrito como o sujeito ativo do crime informático, é autodenominado *hacker*. O verbo *hack* pode ser traduzido ao pé da letra com sentido de invasão, ou seja, trata-se de um sujeito com habilidades em pirataria eletrônica, que possui como propósito adentrar invasivamente na privacidade alheia. Este sujeito empenha-se em conseguir satisfação para seus desejos financeiros, ou até mesmo ferir a vítima por motivos pessoais, como ocorre nos casos de crimes contra a honra.

O investigante Pekka Himanen, observou que há uma sistematização no processo. Uma vez que os *hackers* fazem o repasse de seus conhecimentos para as pessoas interessadas, entende-se que essa ação aperfeiçoa sua imagem, o faz ganhar prestígio e reconhecimento da sua associação. Além de invadir e exprimir

informações de outrem, eles também são aptos a persuasão de outras pessoas para a sua comunidade. Transmite a eles todo os ensinamentos que adquiriram em sua navegação ou que também foi repassado a eles, por intermédio de outros (2001, p. 18).

Por destacar-se sempre perante aos outros e ser prestigiado por muitos, ressalta Nogueira sobre o perfil desse indivíduo:

> Este em geral domina a informática e é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade de cometer crimes, costumam se desafiar entre si, para ver quem consegue invadir tal sistema ou página na *internet*, isto apenas para mostrar como estamos vulneráveis no mundo virtual (2008, p. 61).

A contribuição no rompimento de tecnologia de ponta, cabe aos *crackers*. Peritos do lado obscuro que praticam fraudes para beneficiar-se de dados bancários, golpes eletrônicos e furto de demais itens que os tragam vantagens, capazes de criar *craks*. Em alternativa, os códigos e sistemas são criados justamente para danificar o processo de proteção e permitir o seu acesso.

Estes infratores, má intencionados, procuram se beneficiar de uma conexão à *internet* para exprimir e desvelar aclaramentos particulares, são reconhecidas como *phreakers*. Desde que a atividade seja realizada sem a expressa concordância e com auxílio de um meio telefônico, seja explanações de um cidadão comum ou de uma renome figura pública, também vangloria-se da circunstância para coagir, chantagear e extorquir as pessoas.

Nesse mesmo sentido, Nogueira versa sobre os pichadores virtuais:

> Estes adoram violar algum site, a maioria do poder público, como do FBI, Supremo Tribunal Federal, INSS e lá deixar sua marca, às vezes acontece algum tipo de protesto político ou religioso com esse tipo de invasão, ou podemos chamar de manifesto, normalmente não causam danos (2008, p. 62).

Em suma, a responsabilização por tais atos é um grande desafio para quem se preocupa em respeitar o princípio da dignidade da pessoa humana. Sendo

assim, o modo de penalidade deve ser uma reflexão consciente na tomada de decisões, no que tange ao processo normativo.

Esse processo, deve acontecer de forma responsável e coletiva, para que em ocasião futura todos possam estar alertas e cientes das incógnitas envolvidas. Com a finalidade de lograr para ambientes que garantam segurança, zelo e conforto legal para ambos navegadores.

1.2 Surgimento da *internet*

Denota Augusto Rossini, que os americanos deram início a um projeto de pesquisa militar. Dessa forma, tinha como pretensão a facilidade na troca de transmissões comunicativas, no compartilhamento de informações, visto que o governo americano receberia assim maior auxílio para lidar com próximos e futuros ataques (2002, p. 133).

Durante a década de setenta, o primeiro meio utilizado para testar a *internet* entre os pesquisadores, foi nomeado como e-mail (*eletronic mail)*. Logo, foi o instrumento inicial que possibilitou a extensão da sua comunicação dentro das universidades, além de demonstrar a rapidez e agilidade nas trocas de mensagens. A tecnologia utilizada na época, para transmissão de dados foi criada com o nome de WAN (*Wide Area Networks*), mas a linguagem utilizada nos computadores ligados em rede era bastante complexa, por isso, na época, o potencial de alastramento da *internet* não podia ser imaginado (MERKLE E RICHARDSON, 2000).

No ano de 1995, a *internet* começou de fato a ser liberada para uso de todo público em geral, ultrapassando o uso exclusivo de computadores e abrangendo também o uso contínuo por aparelhos celulares. Após o acontecimento chamado de bolha.com que o assunto começou a repetir e então todos tomaram conhecimento. No ano de 2000, a novidade repercutiu, o que fez com que a internet ganhasse renome e também novos acessos. (REIDE, 1997).

Nesse sentido, é necessário resguardar que o projeto tinha apenas como meta a colheita de informações úteis. Contudo, o campo cibernético ampliou-se e atualmente é uma área vasta que está sempre perpassando por atualizações e modificações constantemente, para melhor desfrute dos usuários. Ainda que, alguns ambientes sejam desconhecidos no ciberespaço e escassos de regulamentações protetivas.

Marcelo Xavier de Freitas Crespo reitera que:

> A *internet*, além de permitir que a criminalidade se mostrasse de formas ainda não previstas na legislação, através de condutas ainda não tipificadas no ordenamento brasileiro, promoveu a alteração dos bens jurídicos atingidos com essa nova criminalidade. Diferentemente do que ocorria com a criminalidade não informática, que atinge os bens jurídicos individuais, a criminalidade informática, em face da facilidade dos meios, tem o potencial de atingir os chamados bens jurídicos difusos, valores vislumbrados a partir de uma massa não definida (2011, p. 36).

No cenário atual, a rede mundial de computadores garantiu a todos o acesso, pesquisa e compartilhamento de conteúdo de forma livre. Esta liberdade permite a difusão de fotografias, vídeos, opiniões e informações, da forma que melhor convém aos usuários. Em razão dessa expansão, também expandiu a criminalidade, justamente pela amplitude de exposição dos usuários, permitindo, inclusive, que os infratores se escondam no anonimato. Isso se deve, dentre outros motivos, pela carência de normas punitivas para tais atos criminosos.

Logo, fazer a observação dessa abordagem em todos os seus aspectos encontrados, é um problema complexo. Á vista que, a internet é um espaço extenso, o qual faz parte da vida diária de milhões de pessoas, é improvável que todos os usuários compreendam os riscos, ao navegar na busca de seus afazeres.

1.3 Evolução dos crimes cibernéticos

Atualmente a sociedade vive um salto quantitativo em relação às tecnologias. Futuramente, ao equiparar-se ao passado, provavelmente, perceberá

que essa geração foi caracterizada como uma época de aceleração tecnológica de avanço, sem precedentes na maneira de consumir e gerar informação, assim como a evolução do ferro e da eletricidade, que demarcou a sociedade em décadas passadas (MIRANDA, 2002).

Desde a pré-história que a informação e a comunicação são essenciais para a raça humana. A comunicação entre os membros dos grupos de caçadores da Idade da Pedra, era fundamental para garantir o sucesso dos ataques, coordenados a animais de grande porte. O desenvolvimento da linguagem humana, foi uma consequência desta necessidade (BORDENAVE, 1982).

Grandes mudanças passaram a ser reconhecidas, segundo Bastos:

> Toda a grande revolução da humanidade também arrasta esperanças e receios, mas, sobretudo incertezas. Se os meios de comunicações tradicionais se baseavam numa lógica unidirecional cultivando um modelo de cidadão passivo e obediente (espectador), a Sociedade da Informação criou, através da interatividade, cidadãos ativos conectados com a fonte de informação. A soma da dimensão multimídia com interatividade conduziu ao aparecimento do pensamento em rede (1998, p.14).

Os crimes cibernéticos começaram a ficar cada vez mais constantes. Por conseguinte, gerou uma situação desconfortante, resultando em medo e euforia para toda a população. Consequentemente, os aplicativos começaram a reforçar sua rede de proteção. Porém, até o presente, são relatados episódios, em que infratores burlam o sistema.

Levando em consideração o resultado de atividades ilícitas e divulgações desnecessárias, estabelecendo a conclusão direta a gravidade de seu uso se empreendido de forma equivocada. Sem considerar o processo contínuo e desagradável que ocorrem no cotidiano dos usufruidores, que não chegam a conhecimento dos investigadores.

De acordo com Simas:

> “A evolução operada nas novas tecnologias, projetou-se sobre o fenómeno criminal, pois se atendermos às suas duas vertentes, por um lado, a tecnologia poder, ela mesma, objeto de prática de crimes e por outro lado, suscita e potência novas formas criminais ou novas formas de práticas antigos crimes” (2014, p. 14).

Considera-se que a *internet* trouxe benefícios, pois promoveu, inclusive, uma melhoria no sistema educacional e no quesito profissional. Desta maneira, a plataforma trouxe respostas positivas, como por exemplo, em relação ao sistema educacional. Possibilitou que os alunos, usassem a internet para aprofundar assuntos já mencionados em sala de aula. Em alternativa, para o sistema profissional, trouxe ferramentas para auxiliar os servidores, em suas tarefas designadas pela empresa.

Com as novas mudanças, foi disponibilizada para quase toda a população mundial o acesso as redes. Contudo, o acesso está cada vez mais aprimorado, motivo pelo qual passou a ter mais destaque no ambiente, pessoas que de fato dominam o espaço virtual. Bem como, o sujeito passivo deixa de amparado pela legislação, ao momento em que não consegue expressar devidamente, ou ter um controle de banalização eficiente, contra esses criminosos.

Conforme Lemos André observa:

> No ciberespaço há a transcendência da matéria: Depois da modernidade que controlou, manipulou e organizou o espaço físico, nos vemos diante de um processo de desmaterialização pós-moderna do mundo. O ciberespaço faz parte do processo de desmaterialização do espaço e de instantaneidade temporal contemporâneos, após dois séculos de industrialização moderna que insistiu na dominação física de energia e de matérias, e na compartimentalização do tempo. (1996, p. 12-17).

A sociedade, no presente momento, se molda as adaptações do mundo virtual. Em consequência, os princípios, crenças e padrões antes conservados, foram sucumbidos a nova era. É plausível alegar que a humanidade está submissa as ferramentas digitais, e toda a comunidade vivenciaria um momento drástico com a sua ausência. Posto isso, não se veem mais em um cenário, em que possa se obstar de uma conexão, para corresponder aos seus intentos desejados.

Uma das formas dessa dependência são os jogos virtuais. Transmite a mensagem, aos jogadores, de que tudo pode ser alcançado quando não medirem esforços para que isso aconteça. Isso é demonstrado - através de batalhas - fases e metas definidos pelo próprio jogo. Cada jogador, tem o poder de escolha sobre seu personagem - desde suas roupas – espaços - objetos que desejam obter para si. Por outro lado, incentiva e estimula os usuários a cumprir as metas estabelecidas para evoluir o seu próprio personagem e avançar para as próximas etapas.

Classifica-se como um dos jogos de simulação da vida real, a animação de *Second Life*. Dentro do ambiente, é possível realizar compras, investindo com dinheiro real para personalizar a casa e vida dos personagens. Embora tenha diretrizes firmadas no próprio site quanto ao comportamento, são apresentados diariamente diversos casos judiciais relacionados a violação do direito do consumidor e possíveis fraudes.

Nesse seguimento aponta Podestá:

> É fato incontestável que no mundo atual, por mais que se queira rejeitar os avanços tecnológicos, nossa vida encontra-se submetida a toda base instituída para a caracterização de exposição potencial da nossa intimidade e vida privada a todos aqueles que, sem razão plausível ou direcionados a necessidade pública, dela queiram conhecer (2001, p. 159).

Á luz dos parâmetros constitucionais, Sílvio de Castro Cerqueira e Claudionor Rocha lecionam que:

> As instituições responsáveis pelas investigações criminais não podem se dar ao luxo de parar no tempo e esperar que os acontecimentos ditem suas respostas à sociedade. Atendendo aos princípios gerais do Direito Administrativo, elas precisam, sob pena de ingressar na esfera de ineficiência, se adiantar ao crime e construir estruturas que lhes permitam efetivamente cumprir suas missões constitucionais dentro dos preceitos afetos às ações do administrador público. Deixar de buscar a evolução propiciada pelo mundo da tecnologia equivale a negar o emprego de novos e eficientes instrumentos de combate ao crime moderno, que é executado sem aviso, sem violência, sem contato pessoal, onde o criminoso busca refúgio no anonimato do universo cibernético e restará impune se não houver o devido preparo da força repressora (2003, p. 155).

A questão colocada, é a falta de responsabilização com relação as atividades ilícitas e ilegítimas praticadas no ambiente virtual. Nesse processo, é notório a falta de novos embasamentos jurídicos, que discorram a prática do *cibercrime*. Portanto, é indispensável que sejam apresentadas novas propostas, sem exclusão á parte burocrática, o acréscimo aos elementos que não foram pontuados, e a introdução de métodos normativos, para melhor corresponder ao delito virtual.

Em outros termos, os magistrados precisam ultrapassar a visão distorcida em relação ao modo investigativo adotado anteriormente, acompanhando e se envolvendo nas mudanças que versam sobre o auge da era informática, como todos seus aspectos. Deve abandonar a velha legislação, passando a integrar novos recursos para enfrentar com prontidão e efetividade, a nova realidade em que se situa o agrupamento de toda a nação.

Cabe então aos mediadores judiciários, entender e compreender profundamente esta nova forma de comunicações. Para inovar o modo de persecução investigativa, deve ser levado em consideração, a tomada de decisões de forma consciente. Tais ações, contribuirá para o molde da civilização atual, e para novos modos de inspeção eficazes, em busca da identificação dos delituosos.

CAPÍTULO II- CONDUTA INDEVIDA NO CYBERCRIME

Esse capítulo busca apresentar como ocorrem os delitos informáticos por meio das práticas virtuais. Exemplifica ações que são permitidas e proibidas no espaço virtual, além de expor a conduta e o modo comportamental. E depois, explana quais condutas recaem em falhas, de acordo com seus limites e destinos.

Fundamentar-se á segundo concepções de Colares (2002), Damásio (2003), Mirabete (2002) e outros autores que discutem sobre o tópico apresentado. Elaborados na tentativa de captar a deontologia e pressupostos jurídicos no contexto normativo e algumas considerações ou reflexões sobre a laboração dessa atividade.

2.1 Práticas maliciosas e ilícitas

Considerando o tema proposto e suas acepções, nota-se, no momento presente, o realce de infratores no que corresponde à esfera dos equipamentos tecnológicos. Como resultado, há diversos acometimentos, que ferem a integridade moral e acarreta danos materiais, a depender do contexto. Do ponto de vista de Rodrigo Simarães Colares, esses crimes podem ser pautados em:

> Crime contra a segurança nacional, preconceito, discriminação de raça-cor- etnias, pedofilia, crime contra a propriedade industrial,

interceptação de comunicações de informática, lavagem de dinheiro e pirataria de software, calúnia, difamação, injúria, ameaça,

> divulgação de segredo, furto, dano, apropriação indébita, estelionato, violação de direito autoral, escárnio por motivo de religião, favorecimento da prostituição, ato obsceno, incitação ao crime, apologia ao crime ou criminoso, falsa identidade, inserção de dados em sistema de informações, falso testemunho, exercício arbitrário das próprias razões e jogo de azar (COLARES, 2002, p. 02).

Adentrando-se na análise dos crimes em espécie, sabe-se que os crimes contra a honra são pautados em calúnia, difamação e injúria. Baseado no conceito descrito na Constituição Federal, a honra deve ser encarada como um coeficiente, que preza por resguardar o princípio da dignidade da pessoa humana.

No dizer de Damásio, tais tipos penais visam proteger a honra, a qual consiste em “conjunto de atributos morais, físicos, intelectuais e demais dotes do cidadão, que o fazem merecedor de apreço no convívio social”. Em seguimento, para ser enquadrado nessa modalidade, é primordial que haja a ofensa ao decoro de outrem (DAMÁSIO, 2003, p. 201).

Seguindo o conceito dado por Mirabete, qualquer pessoa física pode ser o agressor. Nestes casos, a pessoa jurídica - por não possuir honra subjetiva - não pode figurar como sujeito passivo do crime de injúria. Em relação aos completamente ou relativamente incapazes, os menores de idade e os doentes mentais, deverá ser analisado se possuem a capacidade de discernir sobre as ofensas (MIRABETE, 2002, p. 273).

Cabe ressaltar, embora menores de idade e doentes mentais não possuam capacidade de discernir sobre as ofensas, isso não exclui a hipótese do cometimento de crimes executados por eles. Principalmente ao se tratar de jovens, em razão de serem geralmente mais hábeis no manuseio dos recursos tecnológicos, se encontram em uma situação mais tentadora para cometer infrações contra familiares, conhecidos ou até mesmo, estranhos.

O crime de calúnia recai sobre a ofensa, direcionada a outras pessoas. Diferente do crime de injúria, que visa atingir a reputação de outrem. Ainda por cima, o crime de calúnia indica três pontos cruciais que os distinguem das demais

infrações: “a imputação de um fato - o fato imputado à vítima deve – obrigatoriamente - ser falso - além de falso, o fato deve ser definido como crime (GRECO, 2008, p. 421/422).

A calúnia e a difamação restarão configuradas, quando houver a publicação do ato praticado. Sem demora, quando chegar a conhecimento de um ou mais intercessores. Para ilustrar aludida teoria, cita-se, por exemplo, a plataforma do *Instagram*. Importante salientar, a quantidade de usuários que estão abandonando aplicativos como *Facebook – Snapchat – Twitter,* para migrarem para o *Instagram*. Devido ao renome construído, o aplicativo vêm ganhando cada vez mais espaço, entre pessoas de todas as faixas etárias, gêneros e lugares.

O acesso aos aplicativos é permitido, desde que, logrado com contas cadastradas. Aproveitando-se da oportunidade de alcançar um grande público, acabam por surgir constantemente, diversas postagens impiedosas e de caráter hostil, referentes a outros usuários registrados. O ofensor, desfruta desse incidente para propagar a imagem errônea e distorcer a índole das vítimas em seu meio social. Além de que, se direciona com palavras de baixo calão.

Apesar do *Instagram* ser o mais bem apreciado recentemente, o *Facebook* continua sendo uma plataforma forte para a execução de tais crimes. Dado que, as pessoas possuem total liberdade, não há limites específicos na plataforma. Há ainda, uma grande concentração de dados pessoais - partilhado nos perfis - postagens na linha do tempo, e em grupos dos mais diversos por toda a rede.

Nesse espaço, há o compartilhamento e debate no que se refere aos gostos musicais – culinários - políticos, como também, desabafos diários sobre os empregadores. Nesse último caso, por vezes, o empregador é caracterizado como intolerável por seus empregados, na ocasião em que, são sobrecarregados ou incomodados em seus serviços. Assim sendo, os empregados partilham comentários em suas redes, dos quais, qualquer um que tenha registro na plataforma vai conseguir comentá-lo.

Por fim, para que o crime de injúria seja concretizado, não há necessidade de publicização. Basta que a própria vítima se sinta lesada em sua honra subjetiva. Nesse sentido entende a doutrina. Segundo palavras da autora Carla Rodrigues:

> No crime de injúria, o agente não imputa à vítima a prática de um fato, como na calúnia e na difamação, mas sim uma característica, qualidade, enfim, o conceito que o agente tem sobre a vítima. Exemplo: Tiago diz que Renata é preguiçosa e malandra (RODRIGUES, 2003, p. 17).

Um famoso caso concreto que exemplifica o delito de injúria foi o da jornalista Maria Júlia Coutinho, conhecida por Maju. Ela foi vítima, por diversas vezes, de piadas racistas, o que gerou muita comoção social. Sobre o caso, Will Soares se pronuncia que “Além dos ataques à apresentadora da previsão do tempo do Jornal Nacional, o grupo se dedicava a tirar do ar diversas páginas da rede social sem qualquer justificativa”. Os principais alvos eram páginas de fã clubes de artistas e de pessoas que, por motivo desconhecido, os integrantes do grupo apontavam como inimigos (G1/SÃO PAULO, 2020, online).

Nas publicações, é notório perceber bárbaros comentários oriundos de internautas, distribuindo perversas críticas tocantes à vida profissional e identidade personalista da jornalista. Há quem possa falar que a nova geração, apesar de conter muitas pessoas ainda preconceituosas e maldosas (até porque, a vida é muito complexa) também pode ser muito positiva, com pessoas menos intolerantes e mais atentas às mazelas do muito – tanto é que os movimento sociais hoje estão muito mais fortes do que antes.

Em partes, alguns aplicativos como o *Snapchat,* responsabilizam os administradores. Contudo, existem sites e demais plataformas que não honram com compromisso de responsabilização para com seus consumidores. Como já bem asseverado, todos os elementos que forem compartilhados ou digitados, podem ser utilizados contra quem os compartilhou. Todavia, na maioria dos casos, a exposição de tais elementos, é feita por uma terceira pessoa, o que gera um transtorno maior.

A pornografia infantil e a pedofilia, estão entre os crimes que geram aversão e repugnância para toda a sociedade. Nesse ambiente virtual, o infrator fará sua pesquisa ao *google* para ter acesso a estes conteúdo. Isto pois, as ferramentas de pesquisa possuem filtros justamente para impedir que conteúdos pornográficos apareçam aleatoriamente, a não ser que seja pesquisado.

Os administradores de sites que incitam a pornografia, tem ainda, um ramo de opções relativos ao conteúdo. Com esse destino, os condutores, tem a opção de partilhá-las ou vendê-las ilegalmente. Em virtude dessas considerações, aquele que apoiar o conteúdo ou fazer uso dele, incorrerá também em crime de pornografia, tipificado no artigo 218-C do Código Penal Brasileiro.

Diferentemente das condutas anteriormente descritas, os delitos acontecem em sigilo, na maioria das vezes. Alguns aplicativos de telefone celular facilitam a troca de informações e mensagens, de forma instantânea, o que leva diversos usuários a compartilhar informações sem perceber que estão incorrendo, necessariamente em crime (CUNHA, 2014).

Na perspectiva de Reis, a pornografia pode ser descrita de tal maneira:

> A pornografia infantil no ambiente da rede eletrônica pode ocorrer diversas maneiras: o material pode ser oriundo de fatos reais ou criado e montado através do computador; pode ser distribuído através dos sites web, *newsgroups*, salas de bate-papo e e-mail; pode estar no formato de imagem, vídeo ou até mesmo em formato de áudio (2003, p. 309).

No que concerne ao crime de Furto, tornou-se comum à prática de transferências bancárias ilegais pela *internet*. Seguindo esse ponto, o crime de furto, é então uma subtração do bem alheio, buscando a aquisição da posse, consuma-se o crime no local onde o bem foi afastado do verdadeiro dono.

A apropriação de valores de conta corrente, mediante transferência bancária ilícita sem a licença do correntista, consiste em crime fraudulento. Segundo decisão do STJ “fraude é utilizada para burlar o sistema de proteção e

vigilância do banco sobre os valores mantidos sob sua guarda" estabelecendo também que a atribuição para esse tipo de delito, é do juízo do campo onde o bem foi subtraído da vítima, na qual ali se consuma (SUPERIOR TRIBUNAL DE JUSTIÇA, 2020, *online*).

Similarmente, é possível fazer a comparação do crime de *phishing* com o crime de furto, em virtude dos agentes precisarem ter o acesso das contas para conseguir subtrair dados essenciais das vítimas. Nos dois delitos, os documentos necessários para a subtração são os mesmos, sendo eles de uso individual e intransferível.

O crime de *phishing,* também é um dos acontecimentos mais rotineiros. É comum que as pessoas através dos seus e-mails, recebam propostas imperdíveis de aparelhos que ganharam, sem ter feito sua participação. De tempos a tempos, não recorda-se de tal site que esteja oferecendo, tal prêmio. Através disso, internautas, aproveitam para colher informações do cartão de crédito e dados pessoais, como CPF e identidade, para seu benefício. (PUBLICA DIREITO, 2020*, online*).

Em via de sua vulnerabilidade, a faixa etária dos idosos é atacada constantemente. Infratores acreditam que é mais fácil chegar até eles, pois alguns encontram-se atrasados no que se refere a tecnologia. De acordo com o autor Sandro D'Amato Nogueira, o *phishing* pode ser considerado: "o envio de e-mails enganosos (com iscas) - com a finalidade de disseminação de vírus - furto de dados pessoais e senhas - entre outros" (2009, p.45).

Logo, a prática contínua desses crimes banais, demanda um enriquecimento maior não só de decretos, mas de leis especificas. Dessa maneira, poderá qualificar melhor cada uma das transgressões, assim como todas demais peculiaridades. Enfim, garantir que a *internet* possa vir a ser um ambiente, o qual as pessoas se sintam seguras, para navegar.

2.2 Legalidade dentro do espaço-tempo *internet*

Há muito o que se discutir ao tratar das diferenças entre o permitido e o proibido no que tange aos conteúdos em plataformas digitais. É claro que, para a convivência em sociedade é preciso haver regras e normas. Na internet, por se tratar de outra realidade onde a nova geração está, também é preciso garantir que a tranquilidade possa predominar. Destarte, cada um possa respeitar o direito de ir e vir do outro.

Bauman afirma que “vida social pós-moderna é marcada pela extraterritorialidade do poder, passível de ser levado a cabo a partir de qualquer lugar, devido à facilidade de circulação de pessoas e capitais e pela fluidez das relações”. O autor reafirma a ideia de que a *internet* permite a aproximação do locutor e do interlocutor, não importando o percurso da distância entre eles. Dessa forma, é possível estar em um mesmo patamar através da rede, igualando-se como se permanecessem em um mesmo local (2004, *online*). Com efeito, a tecnologia foi viável para agregar um funcionalismo mais eficaz nos quesitos educação, trabalho e lazer.

Por esse ângulo Recuero aborda que:

> Redes são dinâmicas e estão sempre em transformação. Essas transformações, em uma rede social, são largamente influenciadas pelas interações”. Com a evolução tecnológica a sociedade foi surpreendida com avanços tecnológicos e teve que se adaptar aos novos meios de comunicação, já que tudo ao redor culminava em tecnologia (2009, p. 77).

Em suma, é impossível descrever todas as atividades norteadas por uso da tecnologia pois a cada dia surgem diversas oportunidades para que o homem amplie seus conhecimentos, frente a esse novo universo o qual a sociedade está inserida. A *internet* é uma ferramenta, que está parcialmente distribuída em todos os campos, seja para uso particular ou como ferramenta de trabalho.

2.3 Inibições da prática virtual

Considera-se que alguns dos internautas praticam ações dentro do meio virtual, que são caracterizadas como crime. Não é possível descrever qual será o desfecho que as façanhas possam acarretar para as suas vidas, pois no dia a dia, há uma gama de opções. A internet foi feita para descomplicar e facilitar determinadas situações. Um exemplo, é o direcionamento a links desconhecidos, aceitando conscientemente de que o site navegado não é seguro ou confiável.

Devido ao potencial da *internet*, pode-se constatar de que os riscos estão cada vez maiores. Porquanto, a liberdade que foi concedida a todos foi ampla e sem restrição definida, o que facilita que engenheiros desse meio perpetuem por lugares como a *deep weeb*. O título de *deep web* conota a ideia de rede obscura, ou seja, sites ocultos que não mostra-se no mecanismo de busca (G1, 2016, *online*).

Para melhor exemplificar, se imagina um iceberg. Sua ponta representa tudo o que é previsto em lei. Já o restante, submerso, representa o ilícito, o desconhecido, o que deve ser escondido. Já a parte submersa representa o conteúdo acessado por pessoas que possuem um conhecimento mais aprofundado de informática e buscam conteúdos se não proibidos, questionáveis.

Pode ser citado como exemplo o massacre na cidade de Suzano, em 13 de março de 2019. Na ocasião, dois jovens atiradores (Guilherme Taucci Monteiro de 17 anos e Luiz Henrique de Castro, 25 anos), entraram na escola estadual Raul Brasil e mataram oito pessoas. Após investigações, a polícia encontrou vestígios de mensagens enviadas a comunidades online na *Deep Web*. Os autores utilizavam essas comunidades para obter informações com outras pessoas de como atuar no ataque (G1, 2019, *online*).

Em síntese, o Direito penal brasileiro não prevê a *deep web* como parte do conteúdo jurisprudencial e nem tão pouco há lei que o defina ou proteja aqueles atacados por meio desse ambiente. Devido ao seu poder de invisibilidade, se torna penoso fazer o reconhecimento dos autores de forma eficaz.

Assim, a *deep web* é um ambiente de área oculta na *internet* carente de legislações. As características desse espaço, acabam atraindo pessoas interessadas em abrigar conteúdo questionável - macabro e ilegal – incluindo-se a pornografia infantil. Seus conteúdos geralmente incitam a violência, porém também encontra-se objetos procurados em mecanismos de busca comum (JUSBRASIL, 2016, *online*).

Algumas modalidades de crimes cometidos utilizado como ferramenta a internet estão previstos no Código Penal brasileiro. Não obstante, o espaço virtual tem sido palco para discussões e avanços no que tange à produção legislativa. Apesar da conscientização para a falta de legislação, o Judiciário ainda não dispõe de instrumentos legais suficientes para a proteção da população que vive em constante evolução. De acordo com Vladimir Aras:

> O único método realmente seguro de atribuição de autoria em crimes informáticos é o que se funda no exame da atuação do responsável penal, quando este se tenha valido de elementos corporais para obter acesso a redes ou computadores. Há mecanismos que somente validam acesso mediante a verificação de dados biométricos do indivíduo. Sem isso a entrada no sistema é vedada. As formas mais comuns são a análise do fundo do olho do usuário ou a leitura eletrônica de impressão digital, ou, ainda, a análise da voz do usuário (JUS NAVEGANDI, 2001, *online*).

Logo, foi demonstrado que a *internet* é outra realidade que o homem ainda não é capaz de dominar. Além da *deep web* existem milhares de espaços inexplorados. Por todos os lugares, há pessoas sendo vítimas de eventos como este, carregando pesares inapagáveis.

Dessa forma, acredita-se que mesmo com a prisão de agentes não será possível reverter os momentos inoportunos que houveram. Apesar disso, ainda pode ser trabalho para que aja uma diminuição quantitativa no número de vítimas afetadas, a fim de que no futuro elas sejam capazes de sentir-se abraçadas e acolhidas pelo próprio Estado.

CAPÍTULO III- INVESTIGAÇÃO SOB A LUZ DO ORDENAMENTO BRASILEIRO

Neste capítulo serão apresentados os sistemas processuais penais e o modo com que as autoridades brasileiras respondem aos delitos cometidos entreredes. Abordará também a maneira que o ordenamento jurídico julga a aplicabilidade e competência dos crimes detidos nesse ambiente. Ainda por cima, explana o impasse legislativo quanto ao modo que o crime virtual foi inserido pelo Código Penal Brasileiro e a carência do sistema judiciário, em adotar jurisprudências e conteúdos legislativos específicos que abarquem toda o espaço da *interweb.*

3.1 Investigação e sistemas processuais penais

Diante da investigação percorrida nos delitos informáticos, verifica-se que continua a seguir a mesma linha de procedimento de uma operação realizada em modo presencial. O investigado, também será em regra submetido a inquérito policial dirigido pelo delegado de polícia competente. Sem embargo, difere-se na apuração realizada no espaço-tempo *internet,* no quesito de admitir apurações investigativas utilizando o auxílio de programas espiões, trojans.

Com o auxílio desses *malwares,* a polícia responsável instalará no computador da vítima programas espiões. Então, serão utilizados para poder ter acesso ao dispositivo empregado para a prática do crime. De acordo com David Silva Ramalho a definição de *malware* pode ser compreendida como:

> Programa simples ou autoexplicativo que diretamente se instala num sistema de processamento de dados sem o conhecimento ou consentimento do utilizador, com vista a colocar em perigo a confidencialidade dos dados, a integridade dos dados e a disponibilidade do sistema" (Revista de Concorrência e Regulação n.º 16, 2013, p. 201 e 202).

A investigação de crimes cibernéticos pode ser descrita em duas fases distintas, fase técnica e fase de campo. A fase técnica investigativa é encarregada de averiguar todos os dados pertinentes tendo como propósito final encontrar o dispositivo informático que foi utilizado para poder constituí-lo como material probatório. Por conseguinte, quando a posição do computador já for exata, e os agentes policiais forem convocadas para realizar as diligências presididas pela autoridade responsável, a fase de campo restará configurada (WENDT & HIGOR VINICIUS, 2013).

A partir da descoberta da identificação da conexão criminosa, é possível se chegar ao local de onde se desencadeou o ato delitivo, abrindo oportunidade de se identificar os autores de crimes através do protocolo, endereço IP. Todavia, é um processo que exige muita cautela, em vista de que é por ele que o computador consegue captar e acessar dados na *internet*. Em consequência, há possibilidades dos infratores utilizarem de mecanismos para ocultar o número identificador.

No sistema processual penal vigora-se o princípio da legalidade da prova, portanto, o recolhimento da prova, para ser válido, deve cumprir todos os parâmetros legais estabelecidos. Por se tratar de um assunto pouco perscrutado, não é possível ainda denotar a prova digital de forma absoluta, apesar da inópia conceitual. O autor Dias Ramos observa que:

> Qualquer tipo de informação, com valor probatório, armazenada em repositório eletrônico-digitais de armazenamento, ou transmitida em sistemas e redes informáticas ou redes de comunicações eletrônicas, privadas ou publicamente acessíveis, sob a forma binária ou digital (2014, p. 186).

No espaço-tempo internet, a prova digital se não observado aos requisitos previstos em lei, perderá sua indenidade. Deste modo, o agente responsável pela investigação terá que ponderar a prova em via de seu caráter

temporário. Isto posto, ao mesmo tempo em que possui curta duração também demonstra-se mutável, cabendo ao próprio investigador identificá-la cuidadosamente, para assegurar que a prova digital não se modifique.

É necessário ponderar que a teoria da prova é regida atualmente tanto pelo sistema inquisitório quanto pelo acusatório, Luigi Ferrajoli perpetua que a verdade dentro deste modelo de sistema, deve ser recebida como relativa ou formal e para ser adquirida precisa ter avançado algum procedimento anteriormente. Sendo assim, de prova ou até mesmo, erros que passaram despercebidos. (FERRAJOLI, 2014, p. 494).

A Lei 13.964/2019 conhecida como Pacote Anticrime aperfeiçoou o campo penal e processual penal trazendo consigo adaptações na legislação brasileira, alvejando obter maior valência contra toda as demais organizações criminosas. Com presteza, passou também a integrar a infiltração de maneira virtual através de agentes competentes no rol dos meios de obtenção de prova da Lei 12.850/2013. Cabe ressaltar que a infiltração já havia sido inserida antes da vigência da lei descrita.

Mendroni leciona que o procedimento incorpora o agente na atividade criminosa, com intenção de que o mesmo seja no ato da operação interpretado como o próprio infrator. Ademais, prossegue o autor:

> Agindo assim, penetrando no organismo e participando das atividades diárias, das conversas, dos problemas, das decisões, como por vezes de situações concretas, ele passa a ter condições de melhor compreendê-la para melhor combatê-la através do repasse de informações às autoridades (2007, p. 53).

Gilson Langaro Dipp, por sua vez aponta como sendo atividade da organização:

> A organização criminosa pode também, eventualmente ou ordinariamente, exercer atividades lícitas com finalidade ilícita, apesar de revestir-se de forma e atuação formalmente regulares. Um estabelecimento bancário que realiza operações legais e lícitas em deliberado obséquio de atividades ilícitas de terceiro, é o

> exemplo que recomenda cuidado e atenção na compreensão de suas características (2015, p. 11).

Para que haja a infiltração dos agentes, o juiz precisa tomar conhecimento Será aceito pelo juiz, quando já houverem sido explorados todos os recursos investigativos, declarando sua subsidiariedade ou *ultima ratio* (último recurso) do instituto. Destarte, não havendo triunfo, será dado a abertura do processo de infiltração virtual, descartando a infiltração de agentes que não abarcam o quadro de polícia judiciaria, responsáveis exclusivamente pela averiguação dos delitos penais.

Sannini Neto e Higor Vinícius Nogueira Jorge, criticam o marco do determinado instituto por ter mirado em proteger os policiais infiltrados. Pelo fato de consentir com a execução da operação, o agente aceita os riscos conforme o procedimento descrito pela Lei de Drogas e da Lei de Organização Criminosa, sendo esse o real motivo da limitação. Sucede- se que os riscos são meramente mais leves, dado que não existe contato físico. Descrevem os autores referenciados:

> A razão para tal determinação na Lei 12.850/13 é óbvia e visa resguardar a integridade dos policiais diante dos riscos intrínsecos ao procedimento. Contudo, parece-nos que a mesma cautela não se faz necessária na infiltração virtual, uma vez que a forma como se desenvolve a medida (por meio da internet) não coloca em risco a integridade física do agente infiltrado. Assim, não vemos razão para a exigência de subsidiariedade em relação a esta técnica de investigação, constituindo, tal requisito, um embaraço desnecessário no combate aos crimes em questão (JUS NAVEGANDI, 2017, *online*).

A infiltração de agentes pode ser classificada em duas modalidades: *Light Cover* ou Deep cover. A primeira, perdura pelo prazo de 6 meses. A *Deep Cover* ou infiltração profunda, é prolongada por mais de seis meses. Em vista dos riscos intrínsecos, na maior parte o agente infiltrado acaba assumindo uma outra personalidade dentro daquele cenário. Ademais, é distanciado de seus familiares para manter sua segurança (CONJUR, 2016, *online*).

Para a materialização desse procedimento, é necessário primeiro analisar cada um dos requisitos exigidos. Depois de verificado o perfil do agente, será possível discriminá-lo como habilitado ou não para a operação. Sobre a fase inicial, exemplifica Renato Brasileiro:

> Recrutamento: divide-se em duas etapas distintas. A primeira delas é a captação, que funciona como um procedimento no sentido de baixo para cima, que situa seu eixo central nas peculiaridades de um sujeito (de baixo) para satisfazer as necessidades institucionais (acima). A segunda etapa é a seleção, que consiste em um procedimento inverso de cima para baixo. Nesta etapa, a polícia difunde de maneira restrita a informação acerca de suas necessidades, com o objetivo de capacitar o infiltrado, escolhendo o candidato dentro de um rol de agentes pré-selecionados e que apresentam características pessoais e profissionais adequadas a este procedimento investigatório (2016, p. 573).

A segunda etapa também chamada formação, é responsável pelo treinamento dos agentes. Portanto, os agentes terão que se preparar para as funções designadas. Por essa razão, a fase é essencial. Através dessas habilidades, o agente poderá se distinguir de outros policiais. Já a terceira fase, simula uma operação que já esteja em curso e utilizará da infiltração para conseguir deter os agentes infratores.

Ainda nessa terceira fase, será feito todo um roteiro a ser seguido além do Estado começar a reformular a figura individual do agente para transforma-lo com contornos similares de transgressores e colocado em pratica o caso hipotético para estudar como o agente reage e se comporta ao novo perfil. Serão trabalhados minuciosamente o relato de dados que trabalhem o psicológico, principalmente pelo fato de resguardar o sigilo da operação e do próprio agente policial, com o propósito de evitar possíveis lapsos futuros.

A infiltração de agentes de polícia, só pode ser empregada por policiais civis ou federais, autorizados constitucionalmente a investigar delitos penais (artigo 144 da CF). Não estão abrangidos nesse módulo os policiais militares, policiais rodoviários federais ou guardas municipais, mesmo que na eventualidade de que o delegado de polícia o convoque sob seu comando. Tampouco agentes de inteligência, agentes do Ministério Público, parlamentares membros de CPI e

servidores da Receita, particulares ou detetives profissionais que sequer são policiais (CONJUR, 2017, *online*).

José Luis Seoane Spiegelberg (apud JESUS, 2002) lecionam que:

> A pessoa integrada na estrutura orgânica dos serviços policiais, é introduzida, ocultando-se sua verdadeira identidade, dentro de uma organização criminosa, com a finalidade de obter informações sobre ela e, assim, proceder, em consequência, a sua desarticulação.

O infiltrado, depois de iniciada a operação, começará então a se misturar em busca de identificar os chefes das organizações criminosas, tal como toda a atividade realizada por eles e seus parceiros. Após esse primeiro contato, o agente poderá aos poucos começar juntar informações que possam responder as perguntas do Judiciário. É considerada uma das fases mais arriscadas e ousadas pois caso o agente não tome as devidas precauções pode estar colocando em risco sua vida particular e de toda investigação.

Após finalizada a operação e colhido elementos que sirvam para coleta das provas, a equipe policial fará a retirada do agente infiltrado do seio da organização criminosa o qual está inserido. Destarte, serão pontuados cada tópico desenvolvido para que o agente possa voltar a se reintegrar dentro da sociedade, e voltar a manter o contato com familiares e amigos de forma segura. É essencial também ao final das operações, que se realize o atendimento médico para amparar os agentes que estão a linha de frente.

Após a implantação da medida ser autorizada pela autoridade judiciária, deve-se proceder à distribuição do pedido e providência das medidas necessárias. Observe-se o artigo 12 da Lei nº 12.850/13, bem como seu § 1º:

> Art. 12. O pedido de infiltração será sigilosamente distribuído, de forma a não conter informações que possam indicar a operação a ser efetivada ou identificar o agente que será infiltrado. § 1o As informações quanto à necessidade da operação de infiltração serão dirigidas diretamente ao juiz competente, que decidirá no prazo de 24 (vinte e quatro) horas, após manifestação do Ministério Público

> na hipótese de representação do delegado de polícia, devendo-se adotar as medidas.

Conforme o disposto no art. 10, §3º da Lei 12.850/2013, após o encerramento de todas as apurações, serão feitos os relatórios que devem detalhar cada acontecimento durante o prazo que o agente esteve dentro daquele ambiente. Sendo assim o relatório será comunicado ao Ministério Público que fará a apresentação da denúncia, momento em que há a presença do contraditório, o infrator terá o direito de defender-se das acusações que estão lhe sendo feitas.

3.2 Limites jurídicos e o modo de execução e os Tribunais Superiores

Os Tribunais Superiores, apresentam um grande déficit no que se refere a matéria jurisdicional, a qual rege os delitos informáticos. Nesse seguimento, Vogt (2012, p. 87) destaca em suas pesquisas que sem a devida tipificação, frente ao delito, não é possível realizar a condenação de um indivíduo por algo que não está descrito previamente em lei.

No entanto, conseguir classificar um delito, como sendo um crime determinado, acaba por ser muitas vezes sendo um processo demorado. Em face do princípio do *in dubio pro reo* (na dúvida, em favor do réu), o qual, expressa o princípio da presunção da inocência, sendo um dos pilares do Direito Penal, e estando ligado ao princípio da legalidade.

Uma representação do feedback da justiça em relação a esses crimes foi o caso ocorrido em 2017, no qual o ministro Rogerio Schietti Cruz manteve a prisão preventiva de um jovem acusado de cometer crimes sexuais e extorsão, contra mulheres e adolescentes pela *internet*. De acordo com os autos, ele utilizava redes sociais para compelir suas vítimas a enviar fotos e vídeos íntimos, e depois utilizava desse conteúdo como forma de extorquir a vítima, e assim não levar a público seus dados ou bens pessoais (REDAÇÃO O SUL, 2019, online).

Em contrapartida, o presidente do Conselho Nacional de Justiça (CNJ), Luiz Fux, criou um Comitê de Segurança Cibernética do Poder Judiciário e

estabeleceu prazos para que sejam apresentadas medidas para evitar novos crimes virtuais contra os sistemas judiciais, medida ocorre após um ataque cibernético, ter derrubado todos os sistemas do Superior Tribunal de Justiça (AGÊNCIA BRASIL, 2020, *online*).

Em outro giro, em relação as ações executadas pelos superiores, tem-se o Ministro do Superior Tribunal de Justiça, Gilson Dipp. O ministro faz alusão aos princípios fundamentais, no qual, de um lado, estão assegurados os direitos e garantias individuais, do outro, estão inseridos o interesse coletivo da sociedade. Afirma ainda que os métodos excepcionais, apesar de invasivos, são necessários na medida de infiltração. Quando houver crimes de alta complexidade, a infiltração é o método mais competente de lidar com a situação. (CONJUR, 2012, *online*).

Como um exemplo da ineficácia da justiça, tem-se o caso do ministro que criou um comitê contra esses delitos, somente depois do ataque ao núcleo do Tribunal Superior de Justiça. Ou seja diversos casos desses ocorrerem diariamente e a justiça não conseguem solucionar mas quando há o sistema judiciário envolvido, as soluções surgem de imediato. (G1, 2020, *online*).

Resumidamente, é notório perceber a quantidade de casos que sobem todos os dias em ambiente virtuais, e a legislação ainda é falha no julgamento desses crimes. Os casos, só ganham visibilidade por parte da população quando há o sensacionalismo, por parte da mídia.

3.3 interpretação dentro do cenário atual

No Brasil, o projeto de lei n.º 84/99, de autoria do deputado Luiz Piauhylino, buscou dar um tratamento mais adequado aos crimes cibernéticos. Em novembro de 2003, um substitutivo da proposta foi aprovado pela Câmara dos Deputados. Atualmente aguarda a manifestação do Senado. A legislação não apresenta muitas lacunas em matéria de crimes cibernéticos, havendo, inclusive, tipos penais específicos relativos a esses delitos (Crimes cibernéticos manuais práticos de investigação, 2006).

A Lei 12.737/ 2012, apelidada de Carolina Dieckmann, segue preceitos expostos pela teoria tridimensional do direito. Essa teoria é fomentada por Miguel Reale, o qual opina que sua gênese adveio da adequação do direito a sociedade, precisamente o que a teoria esboça. Aborda ainda o autor, que o fenômeno jurídico deve ser sondado e compreendido sob uma visão que alcança a norma propriamente dita - o valor - e fato jurídico. (2002, p. 499 e ss).

Diante do exposto, percebe-se a íntima relação da criação da lei 12.737/2012, com o contexto social vivido. Já que, a lei surgiu de um fato ocorrido com a atriz brasileira Carolina Dieckmann. Essa foi a mola propulsora para a criação da lei. Tanto foi assim, que a lei foi apelidado com o nome dela.

No Brasil, a primeira legislação que resultou na figura do agente infiltrado foi a Lei n. 9.034, de 3 de maio de 1995. Lei essa, conhecida como Crime Organizado. Destarte, assim dispôs:

> Art. 2°- Em qualquer fase de persecução criminal que verse sobre ação praticada por organizações criminosas são permitidos, além dos já previstos na lei, os seguintes procedimentos de investigação e formação de provas (BRASIL, 1995, *online*).

Em 2004, com o advento do Decreto Legislativo n. 5.015, o Brasil promulgou a Convenção das Nações Unidas contra o Crime Organizado Transnacional. Intitulado Convenção de Palermo. Assim sendo, definiu o crime organizado e, em conjunto, em seu artigo 20, técnicas especiais de investigação. Inclui-se a infiltração de agentes, não regulamentados no ordenamento jurídico, porém sua prática foi aduzida. Nesta vereda, Maria Jamile José pondera:

> Como diretrizes, a Convenção propõe que o uso do agente infiltrado seja regulamentado de forma a não entrar em conflito com o ordenamento jurídico interno brasileiro, e que seja sempre precedido de autorização da autoridade competente. O documento autoriza, ainda, o estabelecimento de alianças bi ou multilaterais entre países para que a infiltração possa ocorrer em diversos Estados, desde que respeitadas as soberanias nacionais (2010, p. 97).

A Lei n. 11.343/2006, Lei de Drogas, também abordou em seu artigo 53, a figura do agente infiltrado. Nestes termos:

> Em qualquer fase da persecução criminal relativa aos crimes previstos nesta Lei, são permitidos, além dos previstos em lei, desde que mediante autorização judicial e ouvido o Ministério Público. Dessa maneira, são admitidos os seguintes procedimentos investigatórios: I - a infiltração por agentes de polícia - em tarefas de investigação - constituída pelos órgãos especializados pertinentes (BRASIL, 2006, *online*).

Como observadores externos, os Estados-Unidos, Canadá, Japão e África do Sul coadjuvaram na estruturação da Convenção de Budapeste. No que tange ao *cibercrime.* A Convenção, em comento entrou em vigor em 01 de julho de 2000. Os propósitos pretendidos pela própria Convenção, estão expostos como:

> Os principais objetivos da Convenção de Budapeste sobre cibercrimes estão expostos em seu preâmbulo: Convictos de que a presente Convenção é necessária para impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados, assegurando a incriminação desses comportamento e da adopção de poderes suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infracções, tanto ao nível nacional como internacional. (Convenção de Budapeste*,* 2017, *online*).

O legislador, optou pela eficácia e permitiu o uso do agente infiltrado como meio de investigação de prova. Além de regulamentar a medida, devido ao crescimento da criminalidade - tráfico de drogas – e crimes sexuais, motivou a regulamentação do agente infiltrado, como opção de justiça criminal. De resto, é notório que a infiltração policial objetiva, em um primeiro momento, luta contra os desafios das transgressões, caminhando em conjunto com o princípio da proporcionalidade e o *due process of law* (devido processo legal)*.* O projeto é harmonizável com o garantismo penal.

Dita Flávio Cardoso:

> O garantismo como modelo constitucional de inspiração juspositivista consiste em um movimento jurídico penal que busca a

> legitimação da intervenção punitiva do Estado através da observância por este dos direitos e garantias individuais e coletivos, em razão do que não é incompatível com a persecução aos delitos graves praticados especialmente por organizações criminosas de atuação transnacional em um sentido único de defesa dos direitos fundamentais de índole individual frente a eventuais abusos estatais (2013, p. 313- 334).

Na concepção de Ferrajoli, o juiz deve ser um mero espectador, capaz de valorar a prova que foi produzida pelas partes e levadas ao seu conhecimento. Ao sistema acusatório, lhe corresponde um juiz espectador, dedicado, sobretudo, à objetiva e imparcial valoração dos fatos. Por isso, o rito acusatório exige, sem embargo, um juiz-ator, representante do interesse punitivo, versado no procedimento e dotado de capacidade de investigação (1997, p. 575).

Observa-se os direitos e garantias daquele que é investigado, em uma operação de infiltração de agentes. É devida a atenção, aos princípios constitucionais para que estes não sejam feridos. Dentre os princípios, um deles chama a atenção em relação a sua violação para com o investigado, o Direito à Intimidade (BRASIL, 2015, *online*).

Para Franco:

> A atividade de infiltração, por violar a intimidade e outros direitos fundamentais, somente se legitima quando está voltada à coleta de provas a serem utilizadas no processo penal. Portanto, a medida só pode ser ultimada por agentes que possuem funções de polícia judiciária (2007, p. 587).

A Constituição da República Federativa do Brasil, traz em seu bojo direitos e garantias fundamentais que devem ser respeitados no momento da aplicação da infiltração policial. Uma vez que, essa se apresenta como medida que deve ser adotada em *ultima ratio* (como último recurso). A periculosidade e a complexidade inerentes a toda organização criminosa, justifica o emprego de tal procedimento investigatório (JUSBRASIL, 2017, *online*).

A título de conclusão, é importante ressaltar que os métodos utilizados pelo ordenamento jurídico durante a persecução penal no procedimento de

infiltração policial, são métodos ainda pouco contextualizados sob a égide brasileira.

A legislação é falha principalmente no que refere a figura do agente, e aos inúmeros riscos, que a operação trará. Por fim, é preciso caminhar para uma evolução legislativa, para que os delitos sejam julgados de forma correta.

CONCLUSÃO

Nesse estudo encontram-se algumas reflexões sobre a modalidade de infiltração no crime virtual. Procurou-se no decorrer do trabalho, compreender sobre a importância de apresentar novos métodos para melhor tratar este delito.

Constatou-se na realização desse estudo que a infiltração ainda é um método pouco utilizado, apesar da grande demanda de crimes informáticos. Nesse aspecto, superar os modelos adotados anteriormente é uma alternativa jurídica. Esse processo deve visar suprir as necessidades da sociedade, primando por um corpo social saudável. Á vista disso, a navegação e identidade pessoal dos usuários cibernéticos será preservada, e estes serão respeitados como seres de direito.

Se faz necessário, novos modos de inspeção, assim como a elaboração de diretrizes forenses. O conjunto de normas existente, ainda é ineficaz para responsabilizar-se por eventos delinquentes na categoria cibernética. Portanto, por as legislações nacionais apontarem lacunas, a população fica à mercê de suas necessidades, receosas de acessar as plataformas digitais.

Esses elementos de resistência, a construção de novas práticas, são somados a falta de resguardo aos seus direitos de expressão e liberdade, necessária a mudança e a interferência dos tribunais. Nesse sentido, é urgente os legisladores reverem os conceitos e abandonarem velhos paradigmas, para buscar meios de melhorar e também prevenir-se de futuros e possíveis ataques.

Através dessa pesquisa, ressalta-se a importância de compreender o processo de investigação, seja presencial ou virtual. Deve-se buscar acompanhar e

transformar esse processo, de acordo com as necessidades que a população vem a apresentar. De modo que, a função da infiltração seja para atender as necessidades da nação e demais pontos carentes.

REFERÊNCIAS

ARAS, Vladimir. **Crimes de informática**. Uma nova criminalidade. In: Jus Navigandi, n. 51. [Internet]. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=2250. Acesso em: 13 ago. 2020.

Agência Brasil. **Após ataque ao STJ, Fux cria comitê para combater crimes virtuais**. Disponível em https://agenciabrasil.ebc.com.br/justica/noticia/2020-11/apos-ataque-ao-stj-fux-cria-comite-para-combater-crimes-virtuais. Acesso em 9 nov.2020.

ALMEIDA, Ivo Filipe de. **A Prova Digital**. Orientador: Rui Manuel de Freitas Rangel. 2014. 111 f. Dissertação (Mestrado em Direito) - Universidade Autonoma de Lisboa. Lisboa, 2014. p. 26.

BAUMAN, Z. (2004) **Amor líquido:** Sobre a fragilidade dos laços humanos. Rio de Janeiro: Jorge Zahar.

BARBOSA. Marra Fabiane**. Desafios do Direito na Era da Internet: uma breve análise sobre os crimes cibernéticos.** Rev. Campo Jurídico, barreiras- BA v.7 n.2, p.145-167, Julho-Dezembro,2019. Disponível em: http://fasb.edu.br/revista/index.php/campojuridico/article/view/289 Acesso em 18 mai.2020.

BASTOS, M.T.A (2005). **A epifania digital dos chats**. Escritura e subjetivação cultural. Dissertação de Mestrado, ECA-USP, São Paulo.

BORDENAVE, Juan E. Díaz. **O que é comunicação**. 2.ed. São Paulo: Brasiliense, 1982.

BRASIL, **Lei n. 12.737, de 30 de novembro de 2012**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso em 03 jun.2020.

BRASIL. **Lei nº 11.343, de 23 de agosto de 2006**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm. Acesso em: 27 de nov. 2020.

BRASIL, **Lei nº 9.034 de 03 de maio de 1995**, Diário Oficial da União de 04 de maio de 1995, Brasília.

BRASIL, **Lei nº 12. 965 de 23 de abril de 2015**. Princípios, Garantias, Direitos e Deveres Para o Uso da Internet no Brasil. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2014/lei/l12965.htm. Acesso em 11 jun.2020.

BRASIL, **Decreto nº 5.015, de 12 de março de 2004.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.html Acesso em 08 nov.2020.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática:** e seus Aspectos Processuais. 2. ed. Rio de Janeiro: Lumem Júris, 2003.

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

CABETTE, Eduardo Luiz Santos; SANNINI NETO, FRANCISCO, Francisco Sannini Neto. Infiltração virtual: alguns breves apontamentos. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 22, n. 5082, 31 maio 2017. Disponível em: https://jus.com.br/artigos/58136. Acesso em: 20 out. 2020.

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

CERQUEIRA, Sílvio Castro; ROCHA, Claudinor. **Crimes cibernéticos:** desafios da investigação. Cadernos Aslegis, p. 131-161, 2013. Disponível em file:///C:/Users/Usuario/Downloads/crimes_ciberneticos_cerqueira_rocha%20(2).pdf. Acesso em: 15 mai.2020

COSTA, Marco Aurélio Rodrigues. **Crimes de informática**. Disponível em: Revista Eletrônica Jus Navegandi, site http://www.jus.com.br/doutrina/crinfo.html Acesso em 17 mai.2020.

Convenção sobre o cibercrime. Disponível em: http://www.mpf.mp.br/atuacaotematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-dobrasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em 09 mai.2020.

CUNHA, Rogério Sanches. **Manual de Direito Penal:** Parte Geral, 2014.

DIPP, Gilson Langaro. **A delação ou colaboração premiada**: uma análise do instituto pela interpretação da lei. Brasília: IDP, 2015, p. 11**.**

FRANCO, Alberto Silva**. Leis penais especiais e sua interpretação jurisprudencial.** 7 ed. São Paulo: RT, 2002.

FERRAJOLI, Luigi. **Direito e Razão**: teoria do garantismo penal. 3. ed. rev. São Paulo: Revista dos Tribunais, 2010, p. 494.
_____. **Derecho y Razón**: *Teoria del Garantismo Penal. 2. ed. Trad. Perfecto Andrés Ibáñez et al. Madrid: Trotta, 199.*

FELICIANO, Guilherme Guimarães. **Informática e criminalidade**: parte I: Lineamentos e definições. Boletim do Instituto Manoel Pedro Pimentel, São Paulo, v.13, n.2, 2000.

GRECO, Rogério. 2015. **Curso de Direito Penal**. Parte Geral. 17. Ed. Rio de Janeiro: Impetus.

GUIBSON, W. ***Neuromancer***. São Paulo: Aleph, 1991.

GRECO, Rogério. **Curso de Direito Penal**- Parte Especial. 5 ed. Niterói: Impetus, 2008

G1, São Paulo. **Denunciados por ofensas a Maju tinham 'verdadeiro exército', diz MP**. Disponível em: <http://glo.bo/28QdJHo> f Acesso em 2020.

HIMANEN, Pekka. **A Ética dos Hackers e o Espírito da Era da Informação**. Rio de Janeiro, Campus, 2001.

JESUS, Damásio Evangelista. **Direito Penal**. 26 ed. São Paulo: Saraiva, 2003.

JOSÉ, Maria Jamile. **A Infiltração Policial como meio de investigação de prova nos delitos relacionados à criminalidade organizada**. – Faculdade de Direito da Universidade de São Paulo, 2010.

LÉVY, Pierre. **Cibercultura.** 2.ed. São Paulo: Editora 34, 2000.

LEMOS, André. **Ciber-socialidade:** tecnologia e vida social na cultura contemporânea. Disponível em: http://www.facom.ufba.br/ciberpesquisa/txt_and3.htm Acesso em 27 mai.2020.

LIMA, Renato Brasileiro **de. Manual de Processo Penal**: Volume Único. Salvador/BA: JusPODIVM, 2017.

MIRANDA, A. L. **Da natureza da tecnologia**: uma análise filosófica sobre as dimensões ontológica, epistemológica e axiológica da tecnologia moderna. 2002. 161f. Dissertação (Mestrado em Tecnologia) - Programa de Pós-graduação em Tecnologia, Centro Federal de Educação Tecnológica do Paraná, Curitiba, 2002.

MIRABETE, Júlio fabbrini. **Manual de Direito penal**. 18. ed. são Paulo: Atlas,2002.

Merkle, E. R., & Richardson, R. (2000). **Digital dating and virtual relating:** Conceptualizing computer mediated romantic relationships. *Family Relations, 49*, 187-192.

MENDRONI, Marcelo Batlouni. **Crime organizado***:* aspectos gerais e mecanismos legais. 2. ed. São Paulo: Atlas, 2007.

NOGUEIRA, Sandro D'Amato. **Crimes de Informática**. 2ª ed. Leme: BH, 2009.

PEREIRA, Marcelo Alves. **A tutela jurisdicional da Internet** . Disponível em https://www.jusbrasil.com.br/topicos/27400211/deep-web Acesso em 24 ago. 2020.

PEREIRA, Flávio Cardoso. **Agente encubierto como medio extraordinario de investigación – perspectivas desde el garantismo procesal penal. Bogotá**: Grupo Editorial Ibañez, 2013.

PODESTÁ, Fabio Henrique. **Direito à Intimidade em Ambiente da Internet.** Direito e Internet. São Paulo: Edipro, 2001.

RAMOS, Armando Dias**. A prova digital em processo penal**: o correio electrónico. Chiado Editora, 1.º ed. Novembro,2014.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **Crimes virtuais**. 2005. Disponível em: http://www.advogadocriminalista.com.br Acesso em: 22 jun.2020.

ROSSINI, Augusto Eduardo de Souza. **Condutas ilícitas na sociedade digital**, Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, Direito e Internet, n. IV, julho de 2002, p.133. Disponível em: http://www.mpsp.mp.br/portal/page/portal/Escola_Superior/Biblioteca/Cadernos_Tematicos/direito_e_internet.pdf Acesso em 01 jun.2020.

REID, Robert H. 1997. **Architects of web**: 1000 Days That Built The Future Of Business. New York. John Wiley and Sons Inc.

Reis, F. (2003). **Enfrentamento da distribuição da pornografia infantil na internet**: uma experiência institucional. In CEDECA- BA (Org.). Construindo uma História: tecnologia social de enfrentamento à violência sexual contra crianças e adolescentes (pp. 23-36). Salvador, BA.

REALE, Miguel. **Teoria Tridimensional do Direito**. 5ª ed., Editora Saraiva, São Paulo, 2003.

RECUERO, R. **Redes sociais na internet**. Porto Alegre: Sulina, 2009.

REVISTA DE CONCORRÊNCIA E REGULAÇÃO n.º 16, 2013, páginas 201 e 202).

REVISTA JURÍDICA. Faculdade de Direito de Franca. v.14, n.1, jun.2019.

REVISTA EXAME INFORMÁTICA**. "FBI faz busca a cassinos do Second Life"**. Disponível em: http://exameinformatica.clix.pt/noticias/internet/214975.html Acesso em 05 jun. 2020.

REDAÇÃO O SUL. **Veja como o Superior Tribunal de Justiça tem julgado crimes sexuais pela internet.** Disponível em: https://www.osul.com.br/veja-como-o-superior-tribunal-de-justica-tem-julgado-crimes-sexuais-pela-internet/ Acesso em 05 nov. 2020.

SISNEMA, Informática. **Cracker e Hacker:** Experts trabalhando em sentidos opostos. Disponível em: http:// http://sisnema.com.br/Materias/idmat014717.htm Acesso em: 22 mai.2020.

SPIEGELBERG, José Luís Seoane. ***Aspectos procesales del delito de tráfico de drogas***. Actualidad Penal. F. 1, 1996, p. 341-370. In: JESUS, Damásio E. de. *Particular*

pode atuar como agente infiltrado? Jus Navigandi, 2002. Disponível em: <http://jus.com.br/revista/texto/3215>. Acesso em: 12 out.2020.

SIMAS, Diana Viveiros de. **O ciber crime**. Universidade Lusófona de Humanidades e Tecnologias. Lisboa. 2014.

SUPERIOR TRIBUNAL DE JUSTIÇA. Disponível em: https://www.stj.jus.br/sites/portalp/Inicio Acesso em 10 out.2020.

VIANNA, Túlio Lima**. Do Acesso Não Autorizado a Sistemas Computacionais**: Fundamentos de Direito Penal Informático. Disponível em http://www.bibliotecadigital.ufmg.br/dspace/bitstream/handle/1843/BUOS96MPWG/disserta o_t_lio_lima_vianna.pdf?sequence=1. Acesso em 10 jun.2020.

VEJA, São Paulo. **Atiradores discutiam massacre em fórum na deep web**. 2019. Disponível em https://www.google.com.br/amp/s/vejasp.abril.com.br/cidades/atiradores-massacre-forum-deep-web/amp/ Acesso em 20 ago. 2020.