CENTRO UNIVERSITÁRIO FAMETRO

CURSO DE DIREITO

ISAAC DE ARAÚJO LIMA

CIBERCRIMINALIDADE: DISCUSSÕES SOBRE A COLISÃO DE DIREITOS FUNDAMENTAIS E A DIFICULDADE PUNITIVA

Fortaleza-CE

2020

ISAAC DE ARAÚJO LIMA

CIBERCRIMINALIDADE: DISCUSSÕES SOBRE A COLISÃO DE DIREITOS FUNDAMENTAIS E A DIFICULDADE PUNITIVA

Artigo apresentado à banca examinadora e à Coordenação do Curso de Direito do Centro Universitário Fametro – UNIFAMETRO – como requisito para a obtenção do grau de bacharel, sob a orientação da Prof.ª. Me. Isabelle Lucena Lavor.

Fortaleza-CE

2020

ISAAC DE ARAÚJO LIMA

CIBERCRIMINALIDADE: DISCUSSÕES SOBRE A COLISÃO DE DIREITOS FUNDAMENTAIS E A DIFICULDADE PUNITIVA

Este artigo científico foi apresentado no dia 14 de dezembro de 2020 como requisito para obtenção do grau de bacharel em Direito do Centro Universitário Fametro – UNIFAMETRO – tendo sido aprovado pela banca examinadora composta pelos professores abaixo:

BANCA EXAMINADORA

_____

Prof.ª. Me. Isabelle Lucena Lavor

Orientadora - Centro Universitário Fametro – UNIFAMETRO

_____

Prof.ª. Esp. Anna Claudia Nery da Silva

Membro – Centro Universitário Fametro – UNIFAMETRO

_____

Prof.º Esp. Ismael Alves Lopes

Membro – Centro Universitário Fametro – UNIFAMETRO

CIBERCRIMINALIDADE: DISCUSSÕES SOBRE A COLISÃO DE DIREITOS FUNDAMENTAIS E A DIFICULDADE PUNITIVA

ISAAC DE ARAÚJO LIMA[1]

RESUMO

O presente artigo discorre acerca da evolução normativa do Direito Cibernético, além da aplicabilidade e importância no que concerne a necessidade de adaptação conforme o avanço da era digital. Abordar-se-á o início da regulamentação dispondo sobre o avanço das condutas que mereciam ser criminalizadas. Para tanto, relevante conceituar *deep web*, explorando seu conceito e alcance, além do cuidado que o usuário deve ter em seu acesso. Ademais, discutir-se-á sobre uma possível colisão entre de direitos fundamentais: privacidade e liberdade de informação, para então analisá-los sob a ótica das teorias discriminantes do estado de necessidade, das quais compara a teoria diferenciadora em detrimento da teoria unitária. Como resultado, entende-se os desafios existentes na regulamentação das condutas referidas aos crimes cibernéticos, retratando a importância de se pesquisar o crime informático e cibernético, trazendo suas classificações e conceitos, além de abordar a dificuldade punitiva. A metodologia respaldou-se em análise bibliográfica, qualitativa, exploratória, investigação normativa, para identificar aspectos sobre a insegurança jurídica, o cometimento de crimes e suas consequências no cibermundo. Sendo assim, conclui-se que a legislação vigente no Brasil ainda está longe de destinar à devida proteção e alcançar a justiça para os usuários que utilizam o meio virtual no seu dia-a-dia.

Palavras-chave: Direito cibernético; *deep web*; privacidade; liberdade de informação.

[1] Discente do Curso de Direito do Centro Universitário Fametro – UNIFAMETRO.

AGRADECIMENTOS

A Deus toda honra, toda glória, todo louvor, toda gratidão e toda adoração. Agradeço a minha mãe Ana Liduína Lima de Araújo por ter me dado a educação necessária e assim contribuído na formação de minha índole e meu caráter. Agradeço as lições repassadas a trancos e barrancos por meu pai Paulo Sérgio Silva Lima, onde percebi desde cedo que o homem colhe aquilo que plantou. A meu irmão Wesley Lima Caldas como fonte inspiradora de conhecimento, do qual mostrou-me que sem estudo e sem esforço o homem não é nada e a meu irmão Paulo José Silva Lima que mesmo longe mantivemos os laços afetivos.

A minha esposa, companheira, amiga, amante e as vezes minha mãe Maria Luisa Parente Gadelha Lima, a quem me atura há mais de uma década juntos, onde compartilho todas as vitórias e frustrações, angústias e alegrias, onde despejo meu sono bom, meu porto seguro.

Aos meus Filhos Ítalo Douglas Pereira Lima e Ana Carolina Parente Gadelha Lima, aos quais meu amor é infinito, minha vontade de crescer baseia-se em promover uma vida melhor para ambos.

A minha amada sogra, que é para mim, minha terceira mãe, aquela que sempre está em estado de graça, sempre amável e acolhedora.

A minha falecida avó Isaura Lima Araújo que foi e é minha mãe mesmo não estando mais neste plano, saiba que não lhe esqueço um só momento, te amo.

A meu falecido sogro dr. Aloísio Gadelha a quem me deu acolhida e sempre me inspirava, dizendo que eu iria chegar a realizar meus sonhos, que ele tinha fé nisso.

Agradeço muito a Coordenadora do curso de Direito da Unifametro Juliana Wayss a quem me é fonte de humanismo e conhecimento.

Aquela que é a peça fundamental na conclusão dessa jornada, minha maravilhosa profa. Isabelle Lucena Lavor, a quem corroborou com diversos ensinamentos, paciência e louvor para a realização deste trabalho.

Não posso concluir sem agradecer aos funcionários, colegas e em especial, a todos que compõe o corpo docente da Unifametro na figura das professoras Milena Felizola, Patrícia Lacerda, Neurilane Viana, Camile Figueiredo, Vanessa Gomes e aos professores João Marcelo, Flávio Brilhante, Oscar Dalva, Leonardo Vieira, Rogério Silva, Adriano Nóbrega, dentre outros.

INTRODUÇÃO

Busca-se neste artigo esclarecer de forma clara e objetiva o concerne sobre os desafios relacionados a normatização, regulamentação e evolução de condutas no mundo digital. A ideia de uma internet amedrontadora, obscura e por muitos, nefasta, é dirimida a partir do conceito-relato do que se encontra na deep web, seus usuários, o que praticam, o que buscam, como acessar e os cuidados devidos. Aborda o uso de ferramentas que agreguem segurança aos usuários de aparelhos eletrônicos com acesso à internet, onde a privacidade está ameaçada frequentemente por brechas existentes no cibermundo.

A era digital contribuiu para a evolução humana, possibilitando a interação entre os indivíduos e abolindo distâncias, tornando o mundo interligado a uma rede de computadores, a qual se destaca como principal meio de comunicação existente na atualidade. Diante do uso de tecnologias que hoje tornaram-se comuns e de fácil acesso a todos, cresce também o uso destas por parte de pessoas com más intenções, que usam de diversos modos, artifícios e má fé para ludibriar suas vítimas, passando a ferir sua privacidade e acometendo estes a inúmeros problemas. É indispensável a busca de proteção contra aqueles que praticam tais invasões e fazem uso das informações adquiridas para práticas escusas que em sua maioria transcorrem em crimes.

Tendo cada vez mais pessoas acessando redes sociais digitais, se torna mais constante a exposição das suas vidas através da internet, articulando uma notória e crescente prática de crimes cibernéticos onde é de fácil constatação que nos acessos a mídias sociais digitais em dispositivos eletrônicos tais como celulares, notebooks, desktops e tablets, ou meramente fazendo uso da internet para trabalho, são alvos de diversas formas delitivas no cibermundo.

Perante a grande volúpia daqueles que atuam na prática de crimes informáticos e cibernéticos, é destacado o grande desafio que os legisladores detém a ser trasposto, visto que a burocracia em tornar uma conduta delitiva regulamentada não é fácil, e com isso, mediante a lépida evolução tanto das tecnologias quanto das condutas delitivas é uma adversidade a se superar.

Neste sentido, será aludido, como objetivo geral demonstrar as vulnerabilidades existentes no cibermundo, as condutas ali existentes bem como a insegurança e as precauções devidas.

A metodologia escolhida será empregada na forma descritiva exploratória, visto que tratará de forma explicativa, expondo todos os detalhes vinculados sobre o tema, coletando ao máximo de informações possíveis, contribuindo para que os conhecimentos adquiridos possam

ser compartilhados por todos aqueles que assim tiverem interesse. Irão ser utilizadas pesquisas bibliográficas cuja desenvoltura terá como base materiais já existentes, constituído principalmente por livros, dissertações, teses, artigos científicos e sites jurídicos. O Método escolhido será o qualitativo, pois a complexidade do tema necessitava de métodos abertos a complexidade. A abordagem será a indutiva, pois deverá discorrer de maneira concreta e real suas causas e efeitos diante das leis.

1 EVOLUÇÃO NORMATIVA DO DIREITO CIBERNÉTICO

Toda evolução parte de uma necessidade adaptativa sobre determinada condição, a qual devem existir cuidados dos quais são postos na forma de normas que regulam seu uso e responsabilidades, isso também acontece com a evolução normativa do Direito Cibernético. É impreterível o estudo da origem terminológica da palavra "cibernético", que teve origem com a evolução de um simples componente eletrônico, precursor do hoje chip, que está presente em quase todo equipamento eletrônico existente no mundo – o transistor, tornando possível o processamento de impulsos eletrônicos, extremamente velozes e utilizando o modo binário de comunicação – interrupção e amplificação, resultante de toda tensão mundial no período da Guerra Fria e seus subsequentes anos de uma corrida armamentista e tecnológica que influenciaram diretamente a evolução humana como um todo, em especial a cultura cibernética atuante desde o mais simples ato do cotidiano a complexos processos de trocas de informações por grandes empresas e até governos.

Observa-se que o direito deve estar sempre atento a evolução humana no aspecto cultural e regulador das condutas humanas vide que "Para Hans Kelsen, o comportamento é normatizado pelo Direito, que lhe confere um tributo de valor e uma sanção, sem a qual não há como garantir a eficácia da norma." (PINHEIRO, 2010, p. 51 apud HANS KELSEN), coexistindo com o sistema coercitivo ao qual exerce o poder de Estado sobre o indivíduo, determinando normas e efetivando a sua aplicabilidade.

De acordo com PINHEIRO (2010, p. 51) "A meta do ordenamento jurídico é ser uma organização centralizada do poder que teria como vantagens a adaptabilidade diante das mudanças, o que garantiria o seu grau de certeza e eficácia na sociedade". Cabe ressaltar que o dever latente dos legisladores ao criarem normas que acompanhem as necessidades regulamentadoras contemporâneas. Esse dever é um paradigma haja vista que as tentativas de normatizar as lacunas existente esbarram na morosidade que atrapalha e acaba deixando brechas, pois há um círculo vicioso, que incide diretamente nas demandas por regulações. A evolução

da sociedade é frenética assim como a primordialidade de presteza na elaboração e nos debates que envolvem toda forma de regulamentação. Comportam-se alguns contrários ao conteúdo já demonstrado.

Defendem que já há leis em grande número e a culpa está contida na ineficácia da norma. Alegam que a falta de fiscalização, de isonomia e de uma justiça célere é o nó que deve ser desatado. Reflete o mau governo demonstrado pela decadência por tornar maus costumes vigentes e que os deixam legislar mais e mais. Segundo o doutrinador REALE (2002, p. 607) "afirma o alude que toda a norma vigente se destina a influir efetivamente no meio social e é porque vige e influi que se torna positiva".

Eis que surge com o advento da tecnologia cibernética novas práticas e condutas que não existiam regulamentação através de normas ou quaisquer dispositivos jurídicos, desta feita, não podendo permanecer inerte, o Direito em cada país deu início a uma fase expiatória onde foram observados o quanto do comportamento humano poderia ferir os bens jurídicos existentes diante do mundo virtual, havendo na Itália, no início dos anos de 1980 a criação da primeira lei destinada a regular as novas tecnologias da informação. A Lei nº 121 de 1981, na qual procurou o governo italiano a adequação dos novos tipos penais que surgiram com os que já existiam em seu ordenamento, sempre em busca de extinguir a inexistência da norma no que concerne a inclusão digital.

Nos Estados Unidos da América, se deu uma tentativa quase semelhante à ocorrida na Itália, mas distinta no tocante ao incentivar mais e mais o uso universal da internet em seu país e no mundo, onde o vice-presidente norte-americano Al Gore, defendia acesso global através de metas a serem alcançadas por todos os países, desta feita, buscaria proporcionar as oportunidades digitais a todos seus cidadãos, por meio de um trabalho conjunto entre as nações. Perante a estratégia utilizada e posta em plena prática pelo governo norte-americano, alcançou em maio de 2007, a resolução de nº 205 (S.RES 205) determinando o mês de junho de 2007 como o National Internet Safety Moth.

No Brasil, a Constituição Federal assegura em seu artigo 5º a todos os cidadãos o acesso à informação, tratando esse direito como fundamental, vide:

> XXXIII – todos tem direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

Baseado no artigo supracitado, encontra-se diretamente interligado a própria dignidade da pessoa humana, onde o acesso a tecnologias das quais a internet é o atual carro chefe, atua de forma contributiva no desenvolvimento da sociedade como um todo, coadjuvando com os

demais ramos do direito previstos em nosso ordenamento jurídico, percepcionado que a informação originou novas relações sociais e jurídicas servindo de base para a construção da atual sociedade da informação, concerne no sentindo amplo de informação como aduz José Afonso da Silva:

> A liberdade de informação compreende a procura, o acesso, o recebimento e a difusão de informações ou ideias, por qualquer meio, e sem dependência de censura, respondendo cada qual pelos abusos que cometer. O acesso de todos a informação é um direito individual consignado na constituição, que também resguarda o sigilo da fonte, quando necessário ao exercício profissional. (SILVA,2004. Pág. 245)

A pesquisa mais recente sobre o quantitativo da população que não acessam a internet, informou nos dados coletados, que uma em cada quatro pessoas no Brasil não tem acesso à internet. Em números totais, isso representa cerca de 46 milhões de brasileiros que não acessam a rede.

De acordo com o portal EBC / Agência Brasil:

> Os dados, que se referem aos três últimos meses de 2018, mostram ainda que o percentual de brasileiros com acesso à internet aumentou no país de 2017 para 2018, passando de 69,8% para 74,7%, mas que 25,3% ainda estão sem acesso. Em áreas rurais, o índice de pessoas sem acesso é ainda maior que nas cidades, chega a 53,5%. Em áreas urbanas é 20,6%. Quase a metade das pessoas que não têm acesso à rede (41,6%) diz que o motivo para não acessar é não saber usar. Uma a cada três (34,6%) diz não ter interesse. Para 11,8% delas, o serviço de acesso à internet é caro e para 5,7%, o equipamento necessário para acessar a internet, como celular, laptop e tablet, é caro... (AGÊNCIA BRASIL. EBC, MARIANA,TOKARNIA,2020).

Mesmo com toda dificuldade o Brasil em 2018 tinha 120 milhões de usuários e estava em quarto lugar do ranking mundial de usuários da internet, atrás da China em primeiro, com 705 milhões, da Índia em segundo com 333 milhões e dos Estados Unidos (USA) em terceiro com 242 milhões. O portal Inclusão Digital, que faz parte do programa governamental Inclusão Digital, apresenta as iniciativas em curso no país, garantindo a visibilidade decorrente das ações praticadas pelo setor público, na qual a política é realizada por incentivo maior no compromisso estatal ao qual busca incentivar a população a fazer parte da revolução tecnológica na era da informação.

Hoje, a realidade digital é outra, ao lembrar as intenções já descritas, é fácil comprovar que todos deveriam fazer uso do sinônimo de conforto e praticidade, mas que em decorrência de indivíduos aos quais extrapolam os limites da moralidade e legalidade, deixando como resultado, o ônus decorrente do mal uso dessas tecnologias das quais poderiam ser empregada em usos benéficos.

1.1 Início da regulamentação digital

O universo paralelo da internet evoluiu com a digitalização e tem por características principais a troca de informações/dados, sejam eles privados ou públicos dos quais houve um avanço significativo no tocante a evolução dos equipamentos digitais, possibilitando o avanço das telecomunicações, fomentando o surgimento de mercados e estimulando novos hábitos na sociedade mundial.

Com essa evolução, se fez necessário que cada país regulamentasse sobre as condutas adotadas no meio virtual, que em tom emergencial, não conseguiam ajustar algumas condutas das quais eram práticas na internet com relação a legislação já existente. As repercussões no mundo jurídico desprendiam de grande preocupação devido a velocidade na qual deu-se esta evolução, deixando claro que se não houvesse também uma evolução normativa encadearia um comprometimento com a segurança jurídica de seus cidadãos.

Na Europa, países tiveram uma iniciativa dirigida especificamente aos crimes relacionados ao uso do computador e da internet, a exemplo de terrorismo eletrônico, venda de drogas, fraudes, crime organizado, exploração sexual de criança e povos fragilizados como por exemplo alguns localizados na África, iniciativa que ficou conhecida pelo nome de *"A CONVENÇÃO EUROPEIA DOS CRIMES CIBERNÉTICOS"*, esta convenção obteve status de mais importante e abrangente evento que se tratava de ato normativo de incriminação dos crimes cibernéticos.

A convenção foi assinada pelo Estados Unidos da América e mais vinte e nove outros países, em 23 de novembro de 2001, na cidade de Budapeste, na Hungria, onde em busca de unirem esforços para combater um problema que vinha evoluindo numa crescente vertiginosa aos quais era o intuito há alguns anos, vide que seus debates tiveram origem em meados de 1998 na cidade de Birmingham, Inglaterra, devido a exibição de um vídeo demonstrativo dos delitos cibernéticos pelo então Primeiro Ministro britânico Tony Blair, onde naquele dia e local, encontravam-se representantes dos países-membros do chamado (G8): Alemanha, Canadá, Estados Unidos da América, França, Inglaterra, Itália, Japão e Rússia.

A partir dessa interação, cada país tratou de adequar novas normas aos seus respectivos ordenamentos jurídicos internos, como forma de frear e sancionar às condutas lesivas no âmbito do ciberespaço. Decorrente desse encontro, desenvolveram-se à diligência da Comissão Europeia onde o (G8) classificaria a União Europeia como ambiente mais propício ao nascimento de tamanho feito internacional, onde obteve ainda colaboração da Justiça norte-americana, a qual disponibilizou todo o seu aparato técnico.

Houve a necessidade de ajustes na redação de alguns artigos, pois feriam as liberdades

individuais, resultando em ser posto a submissão do Parlamento Europeu para aprovação em 24 de abril de 2001, onde após os devidos ajustes foi aprovado pelo Comitê de Ministros da União Europeia em 11 de novembro de 2001.

O objetivo da Convenção, está relacionado substancialmente ao Direito Penal, onde se busca a efetiva melhoria dos meios de prevenção e eliminação do crime informático e os relacionados a computadores haja vista a necessidade de uma norma mínima comum agregadora dessas espécies de infrações. As trocas de informações entre as nações participantes da Convenção, resulta em uma busca pela compatibilidade nas legislações nacionais, defendida pelo Tratado, possibilitando assim o intercâmbio de experiências partilhadas e, assim, auxiliando a autuação nos casos práticos a exemplo de extradição ou na assistência jurídica mútua.

Compactuaram ao tratarem de crime cibernético, em transpor suas fronteiras, permitindo o livre acesso de seus territórios, inexistindo limites territoriais e jurisdicionais, pois se assim não o fosse, a repressão tornar-se-ia impraticável.

Optaram por listar em cinco títulos as infrações compreendidas na Conversão, onde o primeiro discorre sobre confiabilidade, da integridade e da disponibilidade dos sistemas informáticos e dos danos informatizados, temas de alta relevância quando se apura as incidências sobre eles, enquanto os de títulos dois ao quatro, tratam de infrações as quais os sistemas informáticos e telemáticos são usados como meios de acesso com intuito de atingir bens jurídicos, que em geral, já se encontra protegido pelo Estado na forma de normas vigentes.

Por fim, no título quinto, deliberaram sobre as modalidades de tentativa, auxílio e cumplicidade, delimitando as respectivas sanções e medidas, resultando essa classificação uma representatividade do consenso mínimo, ao qual fora construído sob as diretrizes das Recomendações do Concelho da Europa, resultado dos trabalhos realizados por outra mais organizações, tais como a Organização para a Cooperação do Comércio Econômico e a Associação Internacional do Direito Penal, resultante ainda das bem sucedidas experiências norte-americana, onde a mesma já combatia ilícitos e abusos cometidos na rede mundial de computadores, antes mesmo que muitos outros países pudessem manter contato com tais tecnologias.

Assinada em 2001 e tão somente entrado em vigor em 2004, conta hoje com 62 Estados Partes (entre os quais, a maior parte dos membros da União Europeia, Argentina, Chile e Estados Unidos da América) e com 10 países observadores. Ao final do ano de 2019, precisamente no mês de dezembro, o Brasil foi convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética, dando-se a devida atenção para o prazo de três

anos como limite para a anuência da mesma a qual proporcionará acesso às autoridades brasileiras de forma célere aos dispositivos de jurisdição estrangeira, tornando a cooperação jurídica internacional, o grande dispositivo relacionado ao combate direto e persecutório dos crimes previstos como crimes cibernéticos.

No Brasil, nos meados do ano de dois mil e sete (2007), diante de muita resistência e alcunhada como AI5 digital, surgiu a ideia de se criar o Projeto de Lei de cibercrimes, mais conhecido como Lei Azeredo, em alusão ao autor do Projeto. Após ser desenvolvido colaborativamente em um debate aberto por meio de um blog, teve em seguida, sua elaboração através de intensos debates abertos por meio do blog supracitado, seu resultado foi apresentado no ano de dois mil e onze (2011), o consequente Projeto de Lei que viria a se tornar a maior norma existente que trata de leis voltadas à internet em nosso ordenamento jurídico, o Marco Civil da Internet, buscando a delimitação das condutas permitidas, buscando a adequação por detrimento da ocasião da construção legal da norma, gerando a fidúcia por conta da sociedade, em coerência que ela sabe quando, como e porque o direito será aplicado.

Diante da criação do Marco Civil da Internet, insta citar que, A Lei Geral de Proteção de Dados (LGPD), publicada em agosto de 2018, é considerada a primeira lei brasileira acerca do tema, mas não deixa de reluzir que o Marco Civil da Internet foi inovador no sentido de regulamentar, juridicamente, as atividades online. Essa introdução marcou com tamanha importância o Direito Digital brasileiro, pois, em detrimento das mudanças na norma o direito pode normatizar as relações devidas aos aspectos digitais por quanto se aplicava à exemplo, legislação de direito penal, de direitos autorais e direitos da personalidade.

Mesmo que haja as similaridades das relações jurídicas virtuais já previstas na legislação brasileira, não se permite deixar de levar em consideração as devidas particularidades do meio, mesmo que ainda se tenha adaptado alguns institutos já existentes às modificações da modernidade, resultando ainda em algumas incoerências e lacunas das quais não foram sanadas ainda.

O Marco Civil da Internet se destacou por prover princípios, garantias, direitos e deveres para o uso da Internet no Brasil, a qual necessitava de uma maior regulamentação em relevância ao Direito Digital, no entanto, ainda assim, existia uma importante lacuna: a questão dos dados pessoais no direito digital. Passou a ser reconhecido, as relações jurídico-virtuais e os efeitos delas no ordenamento jurídico, evidenciando, por exemplo, acerca dos crimes cibernéticos, mas a mesma deixou de abordar como devidos dados fornecidos pelos usuários poderiam ser utilizados pelas empresas, restando muitas críticas e a criação da Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº13.709/18) que discorre exclusivamente sobre

tratamento e armazenamento de dados pessoais.

1.2 O lado sombrio da internet: *deep web*

Sir Tim Berners-Lee é o inventor da Rede Mundial de Computadores, da qual utiliza tecnologia da informação e que hoje é conhecida como Word Wide Web. Tim, engenheiro e cientista da computação inglês, buscava solucionar um problema de comunicação entre cientistas de diversas regiões no mundo. Tinham a necessidade de compartilhar seus experimentos com seus colegas de laboratórios e de universidades em diversos locais, onde realizaram a primeira transferência de dados no dia 12 de novembro de 1990, assim originando a web, que possui sua origem diferente da internet, pois é sabido que a internet já existia e que teve seu início com os primeiros protocolos de internet nos anos 70 dos quais surgiram o e-mail[2], FTP[3], IP[4] e VoIP[5] abrindo espaço para o advento do TCP/IP [6]nos anos de 1983.

Antes de se obter uma junção das características de ambas e até que se possa refletir que a internet englobou a web (*conhecida como Surface Web*), se faz necessário esclarecer que a estrutura existente de internet encontrava-se pronta e ociosa pelo uso global, na qual se detectou que o retardo na evolução se dava pela restrição ainda existente em alguns países detentores dessa tecnologia dos quais o uso era exclusivamente por instituições militares e escolas e podendo ser utilizada por Tim Berners-Lee para que pudesse desenvolver a espinha dorsal da web.

Poucos dentre as pessoas que acessam a internet sabem o que seja ou ouviram falar em deep web, o lado oculto da rede, onde seu acesso é restrito e dependente de ferramentas específicas como softwares[7] criptografados para acessá-los. Deve considerar que a internet é

[2] Um correio eletrônico ou correio eletrônico ou, ainda, e-mail, é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação. O Correio Eletrônico é tipicamente um modo assíncrono de comunicação.
[3] Protocolo de Transferência de Arquivos é um protocolo padrão/genérico independente de hardware sobre um modo de transferir arquivos/ficheiros e é um programa de transferência. A transferência de dados em redes de computadores envolve normalmente transferência de arquivos e acesso a sistemas de arquivos remotos.
[4] Um Endereço de Protocolo da Internet, do inglês Internet Protocol address, é um rótulo numérico atribuído a cada dispositivo conectado a uma rede de computadores que utiliza o Protocolo de Internet para comunicação.
[5] Voz sobre IP, também chamada de VoIP (Voice over Internet Protocol), telefonia IP, telefonia Internet, telefonia em banda larga ou voz sobre banda larga é o roteamento de conversação humana usando a Internet ou qualquer outra rede de computadores baseada no Protocolo de Internet, tornando a transmissão de voz mais um dos serviços suportados pela rede de dados.
[6] O TCP/IP é um conjunto de protocolos de comunicação entre computadores em rede. Seu nome vem de dois protocolos: o TCP e o IP.
[7] Programas que dão função aos computadores. Os programas são escritos em linguagem de programação e comandam todo o funcionamento do computador. Software é a parte lógica do computador, que nos permite administrar, operar, manter e usar o equipamento. (SILVA JÚNIOR, 2009, p.23).

composta de camadas, das quais uma é a deep web mas que ao mesmo tempo se torna invisível onde não há qualquer regulamentos ou jurisdição e que imprescindivelmente deveria se existir esforços que conseguissem chegar nesse seguimento com o intuito de normatizar lhe.

Preliminarmente, é obrigação saber que esse termo deep web tem sua origem conhecida através de Michael K. Bergam, onde o mesmo faz alusão à todo aquele conteúdo ao qual não se pode ser indexado pelos sites de busca, restando assim a indisponibilidade a quem realizar determinada busca por conteúdos disponíveis na internet, dos quais estejam na armazenados na deep web. Essa web oculta não faz parte da *Surface Web* diante de seu conteúdo não está disponível para buscas em sites comuns, estando em sua maioria em desacordo aos limites legais, usufruindo da ineficácia e em sua maioria, ausência de fiscalização dos órgãos e entidades competentes.

O acesso a *Dark Web*, assim como também é conhecida a deep web, não é possível através de um navegador padrão como o *Google Chrome*, ou *Internet Explorer*, deste modo às páginas não são indexadas com palavras já que não serão alvo dos buscadores. Então, para encontrar alguma coisa na deep web é necessário conhecer o endereço exato da máquina cujo acesso você pretende acessar. Uma das maneiras mais habituais de acessar a deep web é com a utilização de um software especial, o *TOR*[8] *– The Onion Route* – que corresponde a uma rede de túneis virtuais que dificulta e embaralha a identificação dos equipamentos ao acessarem determinado conteúdo. O *TOR* dificulta o rastreamento, no entanto ao contrário do que alguns dizem, não garante a inviolabilidade dos dados nem a identidade da máquina porque não é criptografado. Mas o *TOR* não é a única forma de acessar a deep web, existem outras opções como o *Morphmix / Tarzan*[9]*, Mixminion / Mixmaster*[10]*, JAP*[11]*, MUTE / AntsP2P*[12]*, Haystack*[13]. Em resumo, a deep web é tudo o que está disponível em máquinas que não estão identificadas pelo *DNS*[14] nem pelos motores de busca.

[8] Tor é um software livre e de código aberto que proporciona a comunicação anônima e segura ao navegar na Internet e em atividades online, protegendo contra a censura e principalmente a privacidade.
[9] Morphmix e Tarzan são ambos totalmente distribuídos, redes ponto a ponto de proxies anônimos, permitindo que as pessoas façam um túnel através da rede mista de baixa latência. Há código-fonte disponível para ambos os sistemas, mas não temos conhecimento de seu uso fora dos ambientes acadêmicos.
[10] Mixminion e Mixmaster são redes de suporte a e-mail anônimo contra um adversário muito poderoso.
[11] JAP (Java Anonymous Proxy) é uma rede de cascatas combinadas para anonimato de solicitações da web e, como tal, tem alguns nós centralizados (participantes na cascata) que combinam e combinam solicitações de clientes por meio da sequência de nós (a cascata) antes de fazer proxy na web.
[12] Ambos os sistemas funcionam por meio do mesmo roteamento antnet básico, fornecendo algum grau de anonimato com base no modelo de ameaça de negação plausível contra um adversário simples sem conluio.
[13] Esta era uma rede de código fechado voltada para usuários iranianos.
[14] O Sistema de Nomes de Domínio, mais conhecido pela nomenclatura em inglês Domain Name System, é um sistema hierárquico e distribuído de gestão de nomes para computadores, serviços ou qualquer máquina conectada à Internet ou a uma rede privada.

Os círculos fechados de pessoas na deep web formam a *Dark Web*, onde as únicas regras são o anonimato e a liberdade de expressão, resultando em grandes números de perfis heterogêneos que vão desde ativistas, sejam políticos ou não, pervertidos, curiosos, passando por cibercriminosos e porque não, simples usuários em busca de privacidade.

O conteúdo das páginas encontradas na *Dark Web* das quais estão à disposição do usuário que dispuserem de conhecimento mínimo de criptografia, poderão acessar conteúdos tais como: compra e venda de drogas (Ex: caso Silk Road, investigado e descoberto pelo FBI no ano de 2013); anúncios de assassinos de aluguel; venda de produtos roubados e contrabandeados; fotos e vídeos eróticos proibidos (incluindo casos de pedofilia); violação de direitos autorais; venda de armas; e os mais macabros, vídeos com experimentos científicos realizados com humanos entre inúmeras coisas que sem sombra de dúvida, expõem o escárnio civilizatório como fatores ilícitos, imorais, proibidos e repulsivos.

Como a deep web é dotada de "estado de natureza", sem objeções e nem regras, cogita-se por não haver tutela jurisdicional, implicando que o ciberespaço é de acordo com Pierre Levy (LEVY, 1999, p. 92-93), "o espaço de comunicação aberto pela interconexão mundial de computadores e das memórias dos computadores", comprovando que este meio é dotado de uma série de conteúdos antijurídicos, tornando indispensável o interesse legislativo ao conteúdo presente nas esferas das pesquisas, devendo ter interesse em agir com a finalidade de regular e organizar conteúdos e ainda censurar objetos de análise dos quais exibem riscos e ofensas a dignidade da pessoa humana e ainda aos usuários de que algum modo se sintam lesados ou ofendidos por alguma conduta não jurisdicionalizada.

A imagem ou pensamentos que se têm é a que somente hackers detêm o acesso a esse mundo escondido, mas isso não condiz com a realidade. Hoje com a publicidade dada a este assunto, "Internet Secreta" ou "Profunda", inúmeras são as pessoas buscando acesso a essa plataforma, seja por curiosidade ou até mesmo, para negócios lícitos e ilícitos, como, por exemplo: mercado de Bitcoins, lojas virtuais ou até mesmo para troca de mensagens secretas; rádios semi-secretos, e-mails criptografados, espaços seguros para denúncias anônimas e redes sociais/sites tais como Facebook e Wikileaks em versões "não rastreáveis".

É importante ter ciência que a maior parte do conteúdo da deep web não é ilícito e também não é perigoso, desmitificando histórias e lendas a este respeito, a forma de acesso a certos conteúdos indexados é o grande gerador de todo folclore envolvido, pois há conteúdos restritos que somente através do meios específicos terão acesso desejado a tal busca. Considera-se que o intuito maior do usuário que busca acesso pela deep web é ter sua privacidade assegurada e garantida, de forma que não disporá à coletivo ou ao governo independentemente

se forem lícitas ou ilícitas.

2. A PRIVACIDADE *VERSUS* LIBERDADE DE INFORMAÇÃO

Ao abordar essa realidade fática, é preciso definir a origem e o sentido etimológico, assim, privacidade é o direito à reserva de informações pessoais e da própria vida pessoal e tem sua origem do inglês *privacy* que conforme o jurista norte-americano Louis Dembitz Brandeis, ao qual, é supostamente, o primeiro a formular o conceito de direito à privacidade, expunha em *The Right to Privacy the: "right to be let alone"* literalmente "o direito de ser deixado em paz", podendo ainda ser compreendida como a vontade de controlar a exposição e a disponibilidade de informações acerca de si mesmo, o que é chamado de regulação dos limites e a quantidade de controle que um indivíduo exerce sobre a entrada e saída de declarações de si mesmo e a quantidade de contato que se tem com outras pessoas resultando em implicações diretas no tipo de relação que o indivíduo desempenha voltado à sua vida e a de terceiros (LUANA,APARECIDA,2020).

A concepção de privacidade pessoal surge entre os séculos XVII e XVIII, onde teve início a oferta de quartos privados nas construções à época em que passou a fazer sentido a elaboração de diários pessoais. Resulta então que, a privacidade atravessou um percurso inexistente à cessação espontânea, passando para a consolidação do senso coletivo de privacidade. Atualmente, a privacidade é entendida como direito fundamental, expressão da dignidade da pessoa humana, pois as informações pessoais criam a imagem do indivíduo diante toda a sociedade. Exercitar a privacidade não consiste apenas em subtrair certos dados, mas em acessar e controlar o processamento e a utilização de todas as informações pessoais (LUCIANOPIRESDEMORAIS.JUSBRASIL, 2017).

Rotineiramente, a privacidade se protege por três instrumentos imprescindíveis. A princípio, tem-se o direito ao sigilo, isto é, a vedação à coleta de informações sensíveis, sem a devida justificativa. Em sequência, destaca a existência do direito de acesso, que é ter ciência dos próprios dados pessoais, pela conexão com os bancos de dados em que são armazenados. Por fim, é consagrado o uso da responsabilidade civil, para reparar danos gerados pela má utilização de informações pessoais.

A privacidade enfim, é a tutela da vida privada na qual fazem parte a intimidade, o resguardo de informações desde a privacidade corporal, privacidade territorial, inviolabilidade das comunicações onde estão de certo modo atrelados a outro direito fundamental, o da informação, neste sentido, ALEXANDRE DE MORAES (2000, p.39) conceitua tais direitos

como “o conjunto institucionalizado de direitos e garantias do ser humano que tem por finalidade básica o respeito a sua dignidade, por meio de sua proteção contra o arbítrio do poder estatal e o estabelecimento de condições mínimas de vida e desenvolvimento da personalidade humana”.

Com o advento da tecnologia, se faz uso da criptografia nos meios eletrônicos, que surge propriamente para dar sustentação à proteção da privacidade quando se é utilizado no mundo digital. Distinta por ser a ciência ou arte de escrever mensagens em código é, hoje, um dos principais mecanismos de segurança utilizado nos meios eletrônicos protegendo dos riscos existentes na Internet, evitando assim que suas mensagens eletrônicas sejam lidas ou que seus dados bancários ou empresariais sejam furtados, enfim, dificultando o acesso a terceiros sem a prévia autorização, garantindo uma forma de proteção de dados sigilosos que é, efetivamente, a essência da criptografia.

Contemporaneamente, a criptografia é classificada como uma ramificação da criptologia, que, por sua vez, dado o grau de sofisticação e embasamento teórico que envolvem o seu estudo, é hoje tida como uma ciência, no campo das Ciências Exatas. E, ao lado das técnicas criptográficas para codificar a mensagem, o estudo dos métodos para decifrá-la, sem conhecer a senha, é chamado de criptoanálise, estabelecendo-se em outra subdivisão da criptologia. Pactuando um critério entre o emissor e o receptor, a criptografia torna possível o envio de mensagens codificadas, incompreensíveis para um terceiro que eventualmente venha a interceptá-las, mas que poderão ser lidas pelo seu destinatário, que conhece o método para decifrar o texto encriptado.

Contudo, além do uso para fins militares – historicamente ligado ao surgimento da própria criptografia – quase tudo que se faz na atualidade em tecnologias eletrônicas demanda encriptação de dados, sem que sequer isso seja notado pelos usuários. Dos aparelhos de TV por assinatura via satélite, ao uso de um simples envio de e-mail, há uso de codificação de dados, a presença dela é necessária, e, sem ela, muitos dos serviços que os usuários de internet realizam não seriam possíveis.

Até este momento, o consentimento é instrumento significativo para a tutela da privacidade, ao menos parte das informações só poderiam ser coletadas e processadas com permissão da pessoa a quem se referem. Não obstante, seja este um instituto clássico, pode ser atualizado pela funcionalização a partir da perspectiva constitucional. Nesse ínterim, o consentimento assume dupla função: por um lado, legitimar a coleta pelos agentes públicos e privados; por outro, a garantir a autodeterminação informacional da pessoa.

Liberdade de informação é uma amplificação da liberdade de expressão, um dentre os

direitos humanos reconhecidos pela lei cosmopolita, que hoje em dia é geralmente melhor compreendida como liberdade de expressão em qualquer meio, seja oralmente, na escrita, no formato impresso e na Internet ou através de formas de arte, por isto, significa que a proteção da liberdade de expressão como um direito incluiu não só o conteúdo, mas também os meios de expressão.

A overdose de informações, representado pela multiplicidade de dados que a internet comporta, tem dificultado a capacidade de controle pelos órgãos fiscalizadores e causado inúmeros conflitos aos usuários quanto ao seu valor perceptivo e confiabilidade das mensagens disponibilizadas. É evidente que na vinculação de uma informação em um dos polos se encontra o emissor da mensagem e do outro o receptor, impondo-se, desta forma, ajustamento, exatidão, percepção e vericidade dos dados que sustentam e alimentam a base da informação.

Para BARROSO (2004), a liberdade de informação "diz respeito ao direito individual de comunicar fatos e ao direito difuso de ser deles informados", em outras palavras, significa que a liberdade de informar encontra-se diretamente alusiva a divulgação de fatos, devidamente definida, onde a liberdade de expressão se dá por qualquer manifestação pensada ou expressa por ato no qual estão diretamente voltadas as suas opiniões e ideias.

A liberdade de informação não é absoluta, não devendo ir de encontro as normas já lincadas na própria Constituição, dado que, deve respeitar limites jurídicos e éticos, tendo em vista o interesse coletivo e, designadamente, o individual.

As novas técnicas de informação têm ampliado as esferas de exposição permanente da pessoa, não só pela internet, mas pelas câmeras que filmam cada situação da vida diária dos indivíduos, como uma espécie de vigilância intermitente, típica da sociedade pós-moderna. Razões de segurança impõem, pelo interesse coletivo, limites à esfera privada de liberdade de locomoção com privacidade.

Partindo da premissa de que são direitos fundamentais, deve-se garantir a aplicabilidade ao caso prático, onde surge a possibilidade de colisão entre eles, da qual surge a celeuma, dentre os dois direitos onde constata que há a possibilidade de um se sobrepor ao outro e que sua incidência no mundo atual é constantemente conflitante.

Assim, diante do avanço da tecnologia e o uso de fontes variadas de informação, bem como a evolução do direito, cria-se a possibilidade de existir um eminente conflito de normas, onde há a possibilidade de um anular o outro e vice-versa, em uma clara demonstração de que um direito constitucional pode limitar outro.

2.1 Dos direitos fundamentais à privacidade e à liberdade de informação

Nos meados do século XVIII, houve a consagração de forma permanente da positivação da liberdade de informação nos Estados Unidos e na França, onde traz em sua Constituição (1789), diante da primeira emenda, em 1791 e na Declaração do Homem e do Cidadão de 1789. Já em 1948, com a Declaração Universal dos Direitos Humanos onde foi reconhecido o direito à liberdade de informação adotada e proclamada pela resolução 217 A (III) da AGNU em 10 de Dezembro de 1948, aduz em seu artigo XIX que, "todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e ideias por qualquer meio de expressão" (GOV.BR/MDH, 2018).

A partir da Declaração Universal dos Direitos do Homem, aprovada pela Assembleia Geral das Nações Unidas, a tutela do direito à intimidade foi inserida na categoria dos direitos à personalidade.

Seguindo este princípio declarado, para ANTONIO ENRIQUE PÉREZ LUÑO (apud TAVARES, 2002, p. 362), os direitos fundamentais são "um conjunto de faculdades e instituições que, em cada momento histórico, concretizam as exigências da dignidade, da liberdade e da igualdade humanas, as quais devem ser reconhecidas positivamente pelos ordenamentos jurídicos em nível nacional e internacional".

Contudo, se deve pautar sempre nos valores e princípios, dos quais dever-se-ia agregar a qualquer lei, necessitando provir como referência ao buscar um norte supraconstitucional, posto que, alude aos princípios e garantias individuais elencados no ordenamento jurídico da maioria das nações, dispondo dos seguintes aspectos : a universalidade, a inviolabilidade, a irrenunciabilidade, a imprescritibilidade, a interdependência, a complementaridade e a efetividade.

No Brasil, versa-se sobre estes direitos fundamentais aos quais estão elencados na Constituição Federal da qual deve-se observar a importância de uma possível colisão entre eles, diante que há a garantia à liberdade de informação, sem nenhuma forma de censura prévia, e tem-se o direito à privacidade do qual é considerado como o direito de personalidade, garantido em seu objetivo resguardar a integridade e a dignidade da pessoa humana, conforme o artigo 5º em seus incisos X e XIV, vide:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

> XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;

Para GRINOVER (1982. p. 69.), acerca da problemática da intimidade, pondera que, "se cada um de nós tivesse que viver sempre sob as luzes da publicidade, acabaríamos todos perdendo as mais genuínas características de nossa personalidade, para nos dissolver no anônimo e no coletivo, como qualquer produto de massa." O direito à privacidade tem como premissa primaria adequar-se com o uso de ferramentas que possam proteger a intimidade, traçando como objetivo uma espécie de modelo mínimo de dignidade privada podendo ser definida como um momento de existência privilegiada.

O direito à liberdade de informação tem sua extrema relevância ao se fazer assegurado na Constituição Federal, onde no Estado Democrático de Direito é imprescindível a participação popular, onde o cidadão passa a ter a possibilidade de conhecer sobre fatos e notícias das quais decorrem ao mundo social no qual vive, havendo a oportunidade de compartilhar tais informações aos demais membros da sociedade, formando assim, a opinião pública, partindo então a relevância de um direito fundamental.

Discorrendo ainda sobre qual o sentido que se baseou para esta consagração, dá-se o prisma da liberdade individual referendada pela liberdade à informação onde está intrinsicamente ligada ao direito de cada indivíduo expressar suas vontades de manifestação e pensamento que figura certo individualismo, onde com o advento das tecnologias e avanço nas áreas econômicas e sociais, tornou a liberdade de informação diretamente voltada ao coletivo, onde todos buscam informações a todo momento e tornando base essencial do Estado Democrático de Direito, assim expõe JOSÉ AFONSO DA SILVA (1998, p.249) "nesse sentido, a liberdade de informação compreende a procura, o acesso, o recebimento e a difusão de informações ou idéias, por qualquer meio, e sem dependência da censura, respondendo cada pelos abusos que cometer."

Compreende-se como informação pessoal aquela que é passada de um indivíduo para outro corriqueiramente e refere-se à toda informação amplamente divulgada com caráter abundante e massivo de estatal, onde é usado meios de divulgação em massa. Obsta a existência de duas vertentes relacionadas a liberdade de informação, a primeira contendo a liberdade de informar e a segunda o direito de ser informado, neste contesto afirma FREITAS NOBRE (1988, p.33) que, "a própria liberdade de informação encontra um direito a informação que não é pessoal, mas coletiva, porque inclui o direito de o povo ser bem informado."

Para JÔNATAS MACHADO:

> Relativamente ao direito de informar o mesmo encontra-se intimamente relacionado com a liberdade de imprensa e de comunicação social e com os direitos dos jornalistas. No entanto, importante salientar que, particularmente no domínio da autodeterminação político-democrática da comunidade, as idéias de verdade e objetividade, a despeito de suas limitações, assumem centralidade como instrumentos de salvaguarda de bens jurídicos de natureza individual e coletiva. Isso se traduz na existência de uma obrigação de rigor e objetividade por parte das empresas jornalísticas e noticiosas para além de uma obrigação de separação, sob reserva do epistemologicamente possível entre afirmações de fato e juízos de valor, informações e comentários. (MACHADO, 2002, p.474-475)

A exemplo do entendimento expressado previamente, julga ser resguardado ao indivíduo a sua privacidade, mas nem toda via esse direito é efetivado, sob este mesmo aspecto, em decisão recente, o Tribunal de Justiça de Santa Catarina condenou emissora de televisão ao pagamento de indenização por danos morais, pela divulgação de fato íntimo e restrito ao âmbito familiar. A emissora, por sua vez, alegou que a notícia limitava se a narrar fatos de interesse público, vídeo caso estar relacionado à troca de bebês, onde no Brasil é considerado crime contra o estado de filiação. O eminente relator prolatou sentença na qual entendeu que, na medida em que o direito à intimidade dos autores colide com a liberdade de informação, a deliberação diante de tal colisão deve ser "ponderada segundo a necessidade, adequação e razoabilidade em sentido estrito. Sob esse diagnóstico, verificou-se que a divulgação dos nomes e das imagens contribuiu apenas para devassar a intimidade familiar".

2.2 Análise a partir das teorias discriminantes estado de necessidade: diferenciadora x unitária

Em breve análise onde o estado de necessidade está inserido, que seja no Código penal, entre os desígnios de causas de justificação. Exclui, assim, à luz dos art. 23, I e 24, a antijuricidade do fato. É o estado de necessidade justificante. Não obstante, as doutrinas, descrevem também uma espécie de estado de necessidade que exclui a culpabilidade, cabendo examinar-se a distinção entre ambos e indagar-se em que medida ou dentre quais limites se poderiam acolher, entre todos, o estado de necessidade exculpante. O Código Penal Brasileiro de 1969, a exemplo das legislações modernas, adotava a teoria diferenciadora, mas com a reforma penal de 1984, passou a adotar a teoria unitária, onde acolhe o estado de necessidade, sem restrições, não estabelecendo expressamente, como a ponderação de bens, como também não define a natureza dos bens em conflito ou a condição dos titulares dos respectivos bens.

Com o advento do Código Alemão onde o revogado § 54 do cuidava de algumas

hipóteses muito restritas de estado de necessidade (ato não culposo, necessário, praticado para salvar de perigo atual o corpo ou a vida do próprio agente ou de um paciente) (TOLEDO, 1994, p177) (DAMÁSIO, 1997, p.365).

Isso levou a doutrina e a jurisprudência daquele país, diante de casos concretos insolúveis perante o dispositivo mencionado, a construir, sob a influência de idéias, o estado de necessidade justificante "supralegal", apoiando no princípio da ponderação de bens e deveres, pelo qual, diante de perigo iminente, inevitável, não provocado, o indivíduo, para salvar um bem de valor superior, pode sacrificar o de valor inferior, desde que, seja a única forma de salvação do primeiro. Faz-se a ponderação dos bens e deveres em conflito o que for reputado de menor valor pode ser licitamente sacrificado para proteção do de maior valor.

Com efeito, a jurisprudência alemã passou a admitir, com ou sem lei, a exclusão da antijuricidade em determinadas situações de estado de necessidade e, com isso, consagrou a denominada "teoria diferenciadora", que acolhia as duas formas básicas do estado de necessidade, mais tarde incorporadas ao texto ora em vigor do StGB (§ 34 e 35), isto é, o estado de necessidade justificante (excludente da ilicitude) e o estado de necessidade exculpante (excludente da culpabilidade) (TOLEDO,1994).

O primeiro se configura quando o agente comete o ato para afastar, de si ou de outrem, perigo inevitável para a um outro bem jurídico, se, na ponderação dos interesses conflitantes, o interesse protegido sobrepujar sensivelmente aquele que foi sacrificado pelo ato necessário.

O segundo é verificado quando o agente realiza uma ação ilícita, afastando de si ou de um terceiro, perigo não-evitável, por outro meio, para o corpo, para a vida ou para a liberdade, excluída a hipótese em que o mesmo agente esteja obrigado, por uma especial relação jurídica, a suportar tal perigo e também a de que este último tenha sido por ele provocado.

O princípio da ponderação de bens e deveres está presente no estado de necessidade justificante e o esgota. Como, entretanto, esse princípio, portador de um critério puramente objetivo – a diferença de valor entre os bens e deveres em conflito – não consegue fundamentar a impunibilidade do fato necessário, quando esses bens e deveres sejam de igual valor (vida contra vida) ou quando o bem sacrificado seja maior do que o protegido, reservou-se para estas últimas situações, que traduzem verdadeiros comportamentos ilícitos, a possibilidade de incidência de uma excludente da culpabilidade – a do estado de necessidade exculpante – se e quando as circunstâncias do ato revelam um quadro de inexigibilidade de outra conduta.

Portanto, isto significa que, com a teoria diferenciadora, algumas vezes o estado de necessidade exclui a ilicitude (casos de sacrifício de valores menores para salvar valores maiores), outras vezes exclui a culpa (casos de sacrifício de valores iguais aos que se salvam,

ou mesmo de valores maiores, quando ao agente não era exigível outro comportamento).

Discorre FERNANDO CAPEZ (1998, p.225), que "o estado de necessidade jamais atuará como causa supralegal ou de exclusão da culpabilidade, pois tal interpretação aflora o art. 24 § 2º, do Código Penal, que dispõe, quando o sacrifício não for razoável, o agente deverá responder pelo crime, tendo apenas direito a uma redução da pena". Ficando assim, caracterizado o fato e ilícito, e, além disso, o agente for considerado responsável por ele.

Finalmente, não houve nítida separação entre o estado de necessidade, como excludente da ilicitude, e o estado de necessidade, como excludente da culpabilidade. Assim na mesma linha de pensamento de JOSÉ MANUEL GOMES BENITEZ (1984, p.174) "na primeira hipótese, ficaria afastada a ilicitude porque o mal causado, pela sua natureza e importância, é consideravelmente inferior ao mal evitado. Na segunda hipótese, por existir um conflito entre bens de igual valor, "o agente atua num estado de alteração motivacional que faz com que não se possa dele exigir uma conduta distinta da que realizou, lesionando um bem jurídico, esta inexigibilidade de conduta diversa é a base da inexistência de uma censura ao agente e, portanto, da culpabilidade. Em tais casos, o fato é típico e antijurídico, quer dizer, objetivamente não está valorizado de forma positiva pelo Direito, ainda que, por não ser censurável, o agente deva ficar impune".

3. OS DESAFIOS DA REGULAMENTAÇÃO DAS CONDUTAS QUE CONFIGURAM CRIMES CIBERNÉTICOS

Diante da "era cibernética", os desafios existentes ao intuito necessário para regulamentar toda e qualquer conduta que configura crime cibernético deve ser tratado com extrema atenção a evolução das ferramentas, máquinas e principalmente aos usuários e a forma que estes utilizam a tecnologia por meios escusos voltados sempre a práticas delituosas, mas é árdua essa missão do legislativo, haja vista que, regulamenta-se uma conduta virtual e logo surgem variedades desta, da qual a lei não tem especificidade abrindo margem a interpretações e quase sempre há a injustiça através da impunidade, devido as brechas, resultando em uma certa imunidade do responsável, causador da lesão ao direito.

Entende-se como crime cibernético todo delito efetuado por indivíduos marginais em meio ao uso de ferramentas ou ambientes virtuais dos quais prejudicam a terceiros. Utilizam práticas diversas, que em sua maioria já estão tipificadas como crime, mas não dentro do mundo virtual, das quais por analogia são aplicadas a cada caso concreto que falte tipicidade especificada em nosso ordenamento jurídico. Tais condutas ainda demandam da criação de

legislação específica, onde os crimes estão em constante evolução, e, também se encontram indeterminadamente ao se restringirem a um meio de rede exato, seja ela pública, doméstica ou privada.

Um dos desafios existentes para a regulamentação das condutas que configuram crimes cibernéticos é o sigilo, é o não conseguir identificar o criminoso, onde ele se encontra, do local que age, quais os métodos empregados para a concretização do delito, é um ato solitário ou está ligado a outros que comungam do ilícito. Tais desafios em sua maioria quando prontamente identificado, ainda terão a análise da conduta, que pode ou não estar tipificada e dependendo do caso concreto, a não configuração de crime. Esta corda bamba entre a normatização e a regulamentação das condutas denota a volatidade que a evolução normativa necessita para acompanhar o comportamento e atos praticados no mundo virtual.

Das condutas com tipificação normatizada, *os crimes contra a honra* descritos no Código Penal, traz a luz da justiça os crimes de injúria, calunia e difamação. Tais crimes estão em evidência no mundo virtual, seja em condutas relacionadas diretamente a pessoa ou a sua função que exerce em sua atividade laboral.

Aduz o catedrático NOBERTO AVENA, "o crime é a conduta que lesa direitos individuais e sociais. Sendo assim, a sua prática gera ao Estado o poder-dever de punir. Como punição não pode ser arbitrária e nem ocorrer à revelia das garantias individuais do indivíduo, é necessária a existência de uma fase prévia de apuração, assegurando-se ao possível responsável o direito de defesa, o contraditório e a produção de provas".

Ao discorrer sobre os Crimes Cibernéticos, assim dispõe a Lei nº 12.737/2012, em seu artigo 154-A. Ipsis litteris: Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Ocorre que as disposições impostas pela mencionada lei, ao se arrazoar, também, ao tipo de ação penal cabível quando da prática de delitos de natureza cibernética, os quais foram elencados no artigo 154-A, acima transcrito. Essa é a inteligência do artigo 154-B da Lei 12.737/2012. In verbis: Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

A variedade de crimes que os indivíduos marginais cometem está intrinsicamente

ligada ao objetivo deles, pois pode se ter facilmente o intuito de apenas expor a vida particular de outrem como ademais, obter para si vantagem ilícita ou dinheiro por meio de extorsão, fraude, dentre outros, podendo ter amplos objetivos, que conseguem incidir diretamente na vida de uma pessoa por meio da internet ou apenas a obtenção de informações. De acordo com o portal EBC: "O Brasil tem hoje 134 milhões de usuários de internet" (AGENCIABRASIL.EBC, 2020), número que aumenta a cada dia pois a internet hoje é fonte indispensável de informações e o meio mais utilizado para interação mundial, daí a necessidade irremediável de se buscar regulamentar todo e qualquer tipo de conduta dentro do mundo virtual em detrimento aos crimes cibernéticos.

No Brasil, "Estudo mostra o mercado negro de "cursos" para crimes virtuais" e que o país "encontra-se também em segundo país em número de sistemas infectados por malware bancário, atrás apenas dos EUA". Diante de tais dados alarmantes, o desafio de regulamentar as condutas que configuram os crimes cibernéticos é surreal, conforme o estudo avançado realizado por uma empresa multinacional de cibersegurança denominada "*Trend Micro*", estudo esse lançado como *"The Brazilian Underground Market"*, demonstrou os problemas de segurança digital no Brasil dos quais, de acordo com o estudo, o submundo do cibercrime do país é o único que possui treinamentos para pessoas que querem entrar nesse mercado.

No mercado negro, as ferramentas e técnicas que são oferecidas quase sempre facilitam com que pessoas que detenham pouco conhecimento tecnológico consigam aplicar golpes e fraudes online com sucesso. Algumas dessas técnicas necessitam de ferramentas que permitem a esses indivíduos modificarem boletos bancários podendo ser adquiridas por R$ 400, enquanto outra, pode usar o envio remoto de SPAM via SMS na qual o valor é de R$ 499 existindo ainda uma lista contendo números de telefones cujo o custo a ser investido é a partir de R$ 750. (FERNANDAFAV.JUSBRASIL, 2014).

3.1 Do crime informático e cibernético: classificação e conceitos

O Código Penal Brasileiro é atualmente o norteador quando se trata de crimes cometidos por advento da informática ou através dos meios cibernéticos, haja vista a falta de legislação regulamentadora para definir tais condutas. Se faz necessário a definição de tais crimes, vejamos, o crime informático ou digital é aquele que se utiliza do computador para a prática delitiva, já o crime cibernético ou cibercrime/virtual é aquele que além de utilizar o computador, usufrui também do ciberespaço, mais conhecido como rede mundial de computadores "*Internet*". Resume-se que todo crime cibernético é um crime digital, mas nem

todo crime digital é cibernético.

No Brasil, o primeiro caso esclarecido de crime informático foi 1997, uma jornalista recebia ameaças e conteúdo de cunho erótico-sexual por e-mail. O crime foi investigado e chegou a um analista de sistemas, ele foi condenado a prestar serviços junto a Academia de Polícia Civil, dando aulas de informática para policiais (NOGUEIRA,2008).

Quando se faz o uso da aplicabilidade do Código Penal aos crimes cibernéticos, destacam-se os crimes contra a honra, são eles: os crimes de ameaça, difamação, calúnia, injúria, constrangimento ilegal, apologia ao crime ou criminoso, falsa identidade e outros. Destaca-se que o emprego da legislação existente, como do Código Penal, quando utilizada para defesa da vítima, é aplicada, uma vez que, operadores do direito, compreendem que a conduta é a mesma já tipificada pela lei, apenas o cenário da prática que muda. Tal analogia só é permitida nesses casos, quando visa beneficiar a defesa, quando se estabelece a conduta como ilícita e aplica-se a sanção, não podendo acrescentar limitações além daquelas previstas pelo legislador, pois as mesmas, trata-se da liberdade do indivíduo.

Com essa definição, não se pode afirmar que não há proteção jurídica no espaço virtual. Revelando-se reiteradas vezes, cada vez mais frequentes, a perspectiva penal, conforme os avanços na tecnologia, permite a existência de delegacias especializadas em crimes cometidos no âmbito virtual, em que buscam investigar de forma mais acentuada, com conhecimentos mais voltados ao cenário específico informático, alcançando assim maior resultado em detectar o dano causado a vítima, visando maior proteção e menor margem de erro na conclusão.

A classificação dos crimes informáticos é importante, uma vez que o legislador possa elaborar normas eficientes, ou indicar normas vigentes que podem ser aplicadas, por isso é imprescindível estudos dos delitos de informática (COSTA, 2011).

Tem se como preceito classificatório os crimes informáticos e cibernéticos da seguinte forma, c*rime virtual comum ou impróprio:* é aquele cujo utiliza a internet como simples ferramenta necessária para executar um crime já previsto e tipificado na lei (exemplos: estelionato e ameaça). No caso, a utilização da internet é apenas outro meio de praticá-lo; c*rime virtual puro ou próprio*: qualquer conduta ilícita que tenha exclusivamente o intuito de comprometer o sistema informático através de violações técnicas ou físicas ao sistema ou a dados. Ataca-se a "tecnologia da informação em si". Aqui ocorre a complexidade da tipificação do crime (JESUS, MILAGRE, 2016).

Segundo Marco Túlio Viana, crimes virtuais próprios “são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)” (VIANA, 2003 apud CARNEIRO, 2012); c*rime virtual misto*: crimes onde o uso da internet é

condição imprescindível (sine qua non) para que esta ação criminosa se efetive, mesmo que se aspire prejudicar outro bem jurídico. Ou seja, a lei protege, além do bem informático, outro bem diferente deste, existindo dois tipos penais em vista.

Não obstante, há de se considerar, pelos ensinos de DAMÁSIO DE JESUS E CELSO ANTÔNIO MILAGRE, uma quarta classificação: a do "*crime informático mediato ou indireto*", que abrange a situação em que um crime informático é efetuado para consumar um outro delito não informático. Trata-se de executar o crime-meio para cometer o crime-fim, devendo trazer à tona o princípio da consunção/absorção. Destaca um óbice com relação a esses crimes ao se referir a sua modalidade pura, já que não se encontram previstos na lei penal brasileira, e, considerando-se o princípio da legalidade, seria inexequível punir condutas deste tipo, ainda que se cause danos a outrem.

Nesse caso ainda se deve ponderar sobre a vedação à analogia que prejudique o réu. GUILHERME DE SOUZA NUCCI corrobora, acerca da analogia, que "é um processo de autointegração, criando-se uma norma penal onde, originalmente, não existe" (NUCCI, 2008). Assim, não se deve admitir a analogia in malam partem, visto que, se for posto em prática prejudica o réu.

A corrente majoritária ao tratar de crimes cibernéticos, classifica como delito de natureza formal, posto que se consumam no momento da prática da conduta delitiva, independente da ocorrência do resultado naturalístico. Mesmo observando as lacunas, a lentidão, juntamente com tamanhas burocracias existentes na criação das leis, é meritório aludir que a legislação pátria aborda diversos outros elos entre crime e a internet, dentre estes, evidência o racismo, os crimes contra a honra, a pornografia infantil, os crimes contra o consumidor, o vilipêndio ao cadáver e divulgação de fotos de acidentes, a lei Carolina Dieckmann, o Marco Civil da Internet, a criação de delegacias especializadas em crimes cibernéticos, a LGPD e etc.

3.2 Da dificuldade punitiva

Ao discorrer da dificuldade punitiva, é necessário que ocorra uma intensa investigação, buscando assim requerer o máximo de eficiência, valendo-se de inúmeras ferramentas, tais como doutrinas, estudos e levantamento de técnicas a serem empregadas a cada caso concreto, das quais são necessárias para a resolução dos crimes digitais e para uma percepção mais assertiva. Desenvolver novas técnicas investigativas, facilitando a prévia identificação dos agentes delituosos e assim expandindo o conhecimento para que se possa não somente combater, mas quiçá, prever certos tipos de crimes que possam a ser cometidos.

Considerando os ensinamentos de ROSSINI (2004, p. 110):

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

Diante o explanado, a legislação brasileira tem grande dificuldade de acompanhar e manter-se junto a evolução tecnológica, pois com o decorrer dos dias surge no âmbito digital algo novo e o legislador não é capaz de caminhar simultaneamente com tais mudanças, e consequentemente os crimes virtuais são praticados diariamente não sendo punidos devidamente, hora esta que a morosidade na mutação legislativa se torna aparente. A essencialidade de tipificação de alguns crimes cibernéticos é clara, mas carece de observar que a formulação de novas leis deve ser feita com acautelamento, pois são inúmeras as leis que foram criadas e não foram postas em prática, pois no contexto penal se cria leis para tudo, sem pensar nas outras áreas para a resolução do problema.

Nesse sentido CRESPO (2011, p. 161):

> O Em tempos onde tudo se torna alvo de leis incriminadoras é preciso ter bom senso e cuidado ao se pretender criar novos crimes. Todos estão exauridos de verificar a enxurrada de tipos penais em nosso ordenamento sem que tragam efetiva contribuição para o convívio em harmonia, para que haja paz social. Isso se dá pela incriminação indistinta de condutas que, no mais das vezes, deveriam ser objeto de políticas sociais mais cuidadosas e de áreas Civil e Administrativa, deixando no ramo Penal como a *última ratio*, sempre tão discutida cientificamente, mas que, na prática, não é observada.

O legislativo Brasileiro explorou a ameaça de forma morosa, e para agir em razão ao combate dos crimes cibernéticos, não ousou utilizar da mesma velocidade a qual o crescimento virtual se desenvolveu, acostando a criação de leis e alterando algumas normas já existentes. Pela falta de atualização na legislação vigente, estes crimes são praticados rotineiramente e em sua maioria encontram-se impunes, transmitindo a imagem de que na internet tudo pode ser feito e que os atos ilegais cometidos não serão vistos, criando assim uma metáfora conhecida como "internet uma terra sem lei".

É notório o abastardo conhecimento virtual dos indivíduos que cometem delitos cibernético. Diante dos seus crimes, passam a ser respeitados e ganham fama entre seus pares delituosos, onde o prestígio conquistado, reflete por toda comunidade criminosa cibernética. Coexiste diversos tipos de delinquentes atuando nessas práticas delitivas, onde os mais conhecidos são os Hackers e Crackers.

Os hackers são indivíduos que procedem no lado bom da informática, combatendo e criando estratégias e técnicas que dificultem o acesso daqueles que procuram vantagens ilícitas e cometimento de crimes virtuais, além de desenvolverem softwares, programas que ajudam os usuários a usarem a rede. Chegam a trabalhar em repartições e empresa reconhecidas como a Pentágono, FBI para evitar que os crackers invadam seu sistema. Temos no mundo vários exemplos de hackers, como por exemplo, Bill Gates (criador da Microsoft), Steve Jobs (criador da Apple), onde, através de seus vastos conhecimentos, criaram duas das mais importantes empresas contemporâneas.

Em resumo, podemos considerar que todos os crakers são hacker, porém os hackers não são crackers. Os crackers fazem uso de ilícitos, burlando os sistemas, em suma, para obter dinheiro ou vantagens, invadem sistemas, decifram as criptografias, invadem softwares de empresas em busca de arquivos confidenciais. Consequentemente, estes grupos são pessoas que possuem notório conhecimento sobre a informática, mas que fazem uso do livre arbítrio e aplicam o mesmo da forma que preferirem. Por fim, evidencia uma certa competição acirrada onde se pode considerar uma espécie de "polícia-e-ladrão". Por onde os Crackers movimentam-se, os Hackers tentam encalçar seus passos na tentativa de evitar que os problemas sejam mais catastróficos.

Assim, devido a isso muitas pessoas não conhecem a palavra cracker e se conhecem acham que os dois termos têm o mesmo significado. (TERCEIRO, 2011).

É dever de todos valorar aqueles que são de suma importância, os profissionais de segurança e combate aos crimes cibernéticos, pois quando se tem profissionais capacitados, obtêm-se um maior êxito, tanto no combate direto, quanto na prevenção, resultando cada vez menos a incidência de crimes virtuais. Tais atitudes são necessárias para que se alcance uma sociedade digital segura e igual, não podendo deixar também de citar o dever de se especializar os legisladores e dar expertise à magistratura são medidas essenciais para combater esta nova onda de crimes tecnológicos, que infelizmente não parece diminuir a cada ano.

Por tanto, resume-se propondo um confronto direto a legislação pátria, para que com o auxílio de jurisprudências e doutrinas capazes de preencher as lacunas existentes, alertando o Governo, que deva-se ter mais interesse e atenção ao combate dos crimes cibernéticos desempenhando toda uma atualização tecnológica encadeada a todas esferas possíveis ligadas ao enfrentamento dessa modalidade de crime, principalmente elaborando campanhas periódicas voltadas a educação do uso digital agregando a implementação de mais delegacias especializadas neste assunto.

CONSIDERAÇÕES FINAIS

Quando se iniciou o trabalho de pesquisa, constatou-se que as regulamentações quanto ao Direito Cibernético hoje, é debatido e acordado através de tratados entre países de todo o mundo, além de suas legislações internas tentarem acompanhar a evolução frenética das máquinas, tecnologias e meios digitais "informação", onde há uma descomunal dificuldade em regulamentar as condutas que se originam desta evolução, e que por isso era importante estudar o tema.

Diante disso a pesquisa teve como objetivo geral, identificar as condutas dolosas praticadas no mundo digital e o impacto delas na vida particular das pessoas, analisando a regulamentação digital buscada pelos legisladores e posta em vigor na tentativa de identificar, coibir e punir aqueles que as praticam, resultando assim em uma suposta segurança jurídica. Foi verificado ainda os meios utilizados para o cometimento dos crimes cibernéticos bem como o lado "sombrio" e até então desconhecido da Internet, apresentando quais ferramentas necessárias para acessar e os "modus operandi" de quem acessa esta realidade oculta. Descobriu-se ainda, que não há somente práticas delituosas na deep web, que alguns usuários fazem uso dela para simplesmente terem sua privacidade assegurada e garantida, e que o Estado não lhe determinará o modo de uso, pois não possui tutela jurisdicional para tal.

Constata-se que o objetivo geral foi atendido, porque efetivamente o trabalho conseguiu demonstrar que existem vulnerabilidades ora desconhecidas, mas que estão descritas neste trabalho, demandando assim uma leitura enriquecedora. Verificou-se a origem das regulamentações existentes no mundo e particularmente as do ordenamento pátrio. Descobriu que pode haver choque de normas das quais estão consagradas como direitos fundamentais. Identificou que a criptografia é ferramenta primordial na defesa da privacidade quando se trata de compartilhamento de dados ou mensagens.

O objetivo específico inicial era trabalhar a insegurança existente com relação ao uso de toda conexão com o mundo cibernético, visto que esse tema é superabundante e engloba vários conceitos específicos, onde foram amplamente intentados. Ele foi atendido por demostrar com clareza as formas de precaução expostas para que o usuário que pretende acessar o mundo cibernético, reconheça ameaças e possa de forma segura, utilizar as tecnologias.

A pesquisa partiu da hipótese de que a Internet não é segura, onde não importa o que o usuário tente realizar para obtenção de segurança, pois não seria eficaz a sua aquisição. Durante o trabalho, verificou-se que a tecnologia digital é hoje a principal ferramenta do mundo globalizado, conectando os países e diminuindo diferenças diante o desenvolvimento

tecnológico. Descobriu-se que, mesmo com a evolução da criminalidade cibernética, evoluiu também o combate a mesma, onde a precaução aliada com cuidados básicos, assegura o usuário uma relativa proteção, visto que, não se pode garantir em sua totalidade a inviolabilidade de redes, softwares e dispositivos.

A metodologia empregada consistiu na forma descritiva exploratória uma vez que tratou de forma explicativa expondo os detalhes sobre o tema, coletando ao máximo de informações possíveis, contribuindo para que os conhecimentos adquiridos possam ser compartilhados por todos. Agregou-se conceitos para fomentar a definir uma opinião, atitude ou comportamento para aos quais tenham interesse nesse trabalho descrito. Foram utilizadas pesquisas bibliográficas cuja desenvoltura tem como base materiais já existentes, constituído principalmente por livros, dissertações, teses, artigos científicos e sites jurídicos. Em relação ao método adotado, o escolhido foi o qualitativo, pois a complexidade do tema necessitava de métodos abertos a complexidade. A abordagem indutiva empregada foi baseada por princípios, descrevendo de maneira concreta e real suas causas e efeitos diante das leis.

Durante a produção deste artigo, diante da metodologia proposta, percebe-se que o trabalho poderia ter sido realizado com uma pesquisa ampla na bibliografia, contudo é notório que o tema é vasto, podendo ser amplamente mais explorado, mas é insuficiente os livros existentes que abordam os assuntos, dificultando muito a pesquisa, ademais, diante da limitação de tempo, da limitação de recursos e por conta da pandemia de Covid-19 enfrentada atualmente, fez com que o grau de dificuldade para produzir este trabalho fosse descomunal.

Recomenda-se este trabalho como fonte futura de pesquisa para um aprofundamento maior sobre os assuntos abordados.

REFERÊNCIAS

AGÊNCIA BRASIL. EBC. Publicado em 29/04/2020 – 10:05 Por Mariana Tokarnia – Repórter da Agência Brasil – Rio de Janeiro – Acesso em: 27 set 2020.

BARROSO, Luís Roberto. **Colisão entre liberdade de expressão e direitos da personalidade**. **Revista de Direito Administrativo**. Rio de Janeiro, v,1, n .235, p. 1-36, jan/mar 2004.

BITENCOURT, Cesar Roberto. **Invasão de dispositivo informático**. Disponível em http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-dedispositivo-informatico Acesso em: 20 nov 2020.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BUDAPESTE, CONVENÇÃO. **Convenção sobre o Cibercrime**. Budapeste, 2001.

CAPEZ, Fernando. **Curso de Direito Penal** – parte geral. 2ª Ed. São Paulo: Saraiva, 1998.

CARNEIRO, Adeneele Garcia. **Crimes virtuais**: elementos para uma reflexão sobre o problema na tipificação. Âmbito Jurídico, Rio Grande, XV, n.99, abr. 2012.

COLLI, Maciel. **Cibercrimes:** limites e perspectivas para a investigação preliminar policial brasileira de crimes cibernéticos. 2009. Disponível em: http://tede.pucrs.br/tde_busca/arquivo.php?codArquivo=2477 . Acesso em: 15 set 2020.

_____. **Cibercrimes:** limites e perspectivas para a investigação preliminar policial brasileira de crimes cibernéticos. 2009. Disponível em: http://tede.pucrs.br/tde_busca/arquivo.php?codArquivo=247 . Acesso em: 11 out 2020.

COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática**: Introdução e História do Computador. 2011. Disponível em: https://egov.ufsc.br/portal/sites/default/files/29402-29420-1-pb.pdf. Acesso em: 09 out 2020.

CRESPO, Xavier de Freitas. Diretivas Internacionais e Direito Estrangeiro. **Crimes Digitais.** São Paulo: Saraiva, 2011.

GRECO, Rogério. **Comentários sobre o crime de invasão de dispositivo informático. Art. 154-A do Código Penal.** Disponível em: http://www.rogeriogreco.com.br/?p=2183 Acesso em: 04 nov 2020.

GRINOVER, A. P. **Liberdades públicas e processo penal:** as interceptações telefônicas. 2. ed. São Paulo: Revista dos Tribunais, 1982. p. 69

JESUS, Damásio de. MILAGRE, Celso Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. Pag. 54.

_____. ***Direito Penal*** – Parte Geral. 15ª Ed. São Paulo: Saraiva, 1997. Vol. 1.

LÉVY, Pierre. **A Inteligência Coletiva**. São Paulo: Editora 34, 2000.

_____. **Cibercultura**. Editora 34. 2000.

LUÑO, Antonio Enrique Pérez. ***Derechos Humanos, Estado de Derecho e Constitución.*** 6ª ed., Madrid: Tecnos, 1999.

_____. **Teoría de los derechos fundamentales**. Madrid : Centro de Estudios Constitucionales, 1993.

MACHADO, Jônatas E. M. **Liberdade de expressão**. Dimensões constitucionais da esfera pública no sistema social. Coimbra: Coimbra, 2002, p.474-475.

MILAGRE, José Antônio, **O que mudou com a Lei Carolina Dieckmann?**, 2013, Disponível em: https://webinsider.com.br/2013/04/16/o-que-mudou-com-a-leicarolina-dieckmann . Acesso em: 23 set. 2020.

NOBRE, Freitas. **Imprensa e liberdade**: os princípios constitucionais e a nova legislação. São Paulo: Summus, 1988, p.33.

NOGUEIRA, Sandro D'Amato. **Crimes de Informática**. São Paulo:BH Editora, 2008.

NUCCI, Guilherme de Souza. **Código penal comentado**. 9 ed. rev., atual. e ampl. - São Paulo: Editora Revista dos Tribunais, 2008. Pag. 54.

OLIVEIRA JÚNIOR, Eudes Quintino de; OLIVEIRA, Pedro Bellentani Quintino de. **Entra em vigor a Lei Carolina Dieckmann**. Disponível em: https://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-leiarolinadieckmann . Acesso em: 19 set 2020.

PAESANI, Liliana Minardi. **Direito e internet.** 5. ed. São Paulo: Editora Atlas S.A.,2012.

PALAZZO, Francesco; PAPA, Michele. *Lezioni di Diritto Penale comparato*. Torino: Giappichelli Editore, 2005, pp. 59-60.

PANDOLFI, Robson (org). ***O guia da Deep Web***. *Mergulhe na parte mais obscura da internet*. Revista Dossiê – Super Interessante, edição 382-A, novembro/2017.

PINHEIRO, Patricia Peck. ***Direito Digital***, São Paulo, Ed. Saraiva, 4ª edição, 2010.
REALE, Miguel. *Filosofia do direito*, São Paulo, Ed. Saraiva, 19ª edição, 2ª tiragem, 2002, pág. 607.

ROCHA, C. B. **A evolução criminológica do direito penal**: Aspectos gerais sobre os crimes cibernéticos e a lei 12.737/2012.JUS NAVEGANDI, Teresina, 2012, v.18.

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

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 16ª ed. rev. atual. São Paulo: Malheiros,1998, p.249

SILVEIRA, Sergio Amadeu da. ***Tudo sobre tod@s:*** *Redes digitais, privacidade e venda de dados pessoais.* Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=Hj0qDwAAQBAJ&oi=fnd&pg=PT3&dq=privacidade+digital&ots=JlfUFsKU6U&sig=WYLZzTRFODq40tLRNsZP2crADoc#v=onepage&q=privacidade%20digital&f=false Acesso em: 02 jun 2020.

TERCEIRO, C. d. F. V. R. **O problema na tipificação penal dos crimes virtuais**. 2011.

TOLEDO, Francisco de Assis. ***Princípios Básicos de Direito Penal***. 5ª Ed. São Paulo: Saraiva, 1994.