



**Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"**

ÉRIKA GENEROSO DOS SANTOS

**A EFICÁCIA DA LEGISLAÇÃO BRASILEIRA NO COMBATE AO CRIME
CIBERNÉTICO**

**Assis/SP
2022**



**Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"**

ÉRIKA GENEROSO DOS SANTOS

**A EFICÁCIA DA LEGISLAÇÃO BRASILEIRA NO COMBATE AO CRIME
CIBERNÉTICO**

Projeto de pesquisa apresentado ao curso Direito do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

**Orientando(a): Érika Generoso dos Santos
Orientador(a): Lenise Antunes Dias**

**Assis/SP
2022**

FICHA CATALOGRÁFICA

S237e Santos, Érika Generoso dos.

A eficácia da legislação brasileira no combate ao crime cibernético / Érika Generoso dos Santos – Assis, SP: FEMA, 2022.

48 f.

Trabalho de Conclusão de Curso (Graduação) – Fundação Educacional do Município de Assis – FEMA, curso de Direito, Assis, 2022.

Orientadora: Prof.^a M.^a Lenise Antunes Dias.

1. Crime cibernético. 2. Crime digital. 3. Legislação Brasileira. I. Título.

CDD 340.0285

Biblioteca da FEMA

A EFICÁCIA DA LEGISLAÇÃO BRASILEIRA NO COMBATE AO CRIME CIBERNÉTICO

ÉRIKA GENEROSO DOS SANTOS

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: _____
Lenise Antunes Dias

Examinador: _____
Hilário Vetore Neto

DEDICATÓRIA

Dedico este trabalho à Deus, fonte de sabedoria e inteligência. A meus pais, meus irmãos e minha sobrinha por todo apoio. A minha orientadora Prof.^a Ma. Lenise Antunes Dias, que com muita humildade me auxiliou no desenvolvimento desta monografia.

AGRADECIMENTOS

Agradeço a Deus pelo dom da vida e a graça de poder finalizar este trabalho de conclusão do curso de Direito com excelência.

A meus pais Airton (in memoriam) e Edna a quem serei eternamente grata pela oportunidade e o incentivo que me deram ao ingressar na graduação. Meus queridos irmãos Brígida, Oscar e Roberto, que muito me motivaram a continuar meus estudos e hoje pudesse estar colhendo os bons frutos da caminhada acadêmica.

A minha orientadora Prof.^a Ma. Lenise Antunes Dias, exemplo de ser humano que com toda a sua sabedoria, humildade e disciplina me auxiliou no desenvolvimento desta monografia. Meu carinho e eterna gratidão por ter tido está excelente professora ao meu lado que se mostrou ser uma grande fonte inspiradora para aqueles que querem aplicar o direito.

A minha prima Deusalira Generoso e minha amiga Elisângela Canhadas, que muito contribuíram para que eu pudesse dar os primeiros passos na caminhada acadêmica. Meu respeito, carinho e eterna gratidão.

A minhas amigas Amanda Rótoli e Caroline Nakamura, pessoas maravilhosas que tive o prazer de conhecer durante a graduação, e Stephanie Santos minha amiga de longa data com quem tive o prazer de dividir toda a construção deste trabalho.

Qual é a primeira coisa que deve fazer quem começa a filosofar? Rejeitar a presunção de saber. De fato, não é possível começar a aprender aquilo que se presume saber.

Epicteto

RESUMO

Em pleno desenvolvimento da era digital, o ambiente cibernético tem-se expandido a novos horizontes visando sempre proporcionar ao público que dele utiliza novas modalidades de execução a diversas tarefas. Por isso, cabe ao Direito como ciência jurídica demonstrar se suas leis vigentes são de fato ou não eficazes no combate ao crime cibernético. Por isso, a presente monografia traz em sua pesquisa como foi o início do desenvolvimento da Internet, bem como aplicabilidade da Lei Carolina Dieckmann (Lei nº 12.737/2012), o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Trazendo em seu texto apontamentos referentes a crimes cibernéticos realizados no Brasil na atualidade.

Palavras-chave: Crime cibernético. Crime digital. Legislação Brasileira.

ABSTRACT

In the full development of the digital era, the cyber environment has expanded to new horizons, always aiming to provide the public that uses it with new ways to perform several tasks. Therefore, it is up to the Law as a legal science to demonstrate whether its current laws are in fact effective or not in fighting cybercrime. In hence, this monograph brings in its research how was the beginning of the development of the Internet, as well as the applicability of the Carolina Dieckmann Law (Law No. 12.737/2012), The Marco Civil da Internet (Law No. 12.965/2014) and the General Law of Data Protection (Law No. 13.709/2018). Bringing in its text notes referring to cybercrime carried out in Brazil today.

Keywords: Cybercrime. Digital crime. Brazilian Legislation.

LISTA DE ILUSTRAÇÕES

Figura 1: Acesso à internet no Brasil	36
---	----

SUMÁRIO

INTRODUÇÃO	11
1. A EVOLUÇÃO HISTÓRICA DO MUNDO VIRTUAL.....	13
2. LEGISLAÇÃO BRASILEIRA APLICÁVEL EM FACE DOS CRIMES CIBERNÉTICOS.....	22
3. CASUÍSTICA- CASOS CONCRETOS DE CRIMES DIGITAIS.....	36
CONSIDERAÇÕES FINAIS.....	42
REFERÊNCIAS BIBLIOGRÁFICAS	45

INTRODUÇÃO

O estudo tem por objetivo investigar qual o grau de eficácia da atual legislação brasileira em relação a prática do crime cibernético realizado contra e por meio da internet. Nesse contexto, é preciso considerar que não basta que a legislação seja válida, mas deve cumprir sua finalidade e mostrar-se eficaz.

Se uma lei não consegue cumprir aquilo pelo qual foi designada, entende-se que ela não deveria existir. Hoje temos uma legislação vigente que, segundo a avaliação de especialistas, possui qualificação teórica e instrumentos jurídicos suficientes para pôr em prática a sua eficácia.

No entanto, podemos observar que o crime cibernético tem aumentado e o problema concentra-se em tentar descobrir quais são os motivos e as razões que tem causado a ampliação deste tipo de crime. Sendo assim, indaga-se se a atual legislação vem sendo de fato totalmente eficiente em seu funcionamento.

Em título de hipótese acredita-se que quando uma legislação não está conseguindo cumprir com êxito aquilo ao qual foi determinada, presume-se que ela esteja com problemas em sua execução. Dessa forma, será possível explicar o tamanho crescimento em quantidade e qualidade técnica a invasão e apropriação de dados.

É válido salientar que a discussão a seguir servirá de modo positivo para o Direito que, ao executar uma lei voltada a crimes realizados virtualmente, está visando proteger um bem jurídico relevante. No universo jurídico, é imprescindível saber se de fato a lei que foi criada para proibir este tipo de prática criminal tem produzido de maneira efetiva os seus efeitos.

Já do ponto de vista da sociedade as pessoas que utilizam a internet precisam de uma maior segurança ao movimentar seus dados. Em virtude do que foi mencionado, conclui-se que todos os usuários precisam saber se a lei ao qual foi criada para protegê-los está funcionando para que se tenham seus dados invadidos saibam para onde recorrer.

Primeiramente trataremos sobre a evolução do mundo virtual, bem como foi realizado o seu desenvolvimento desde sua criação e quais foram as novas funcionalidades que o ambiente virtual trouxe para a sociedade, tendo em vista como ele trabalha, quais são as suas ferramentas e qual foi o impacto que ele trouxe para o mundo analógico. Disporá, também, sobre a conceituação de crime cibernético, bem como quais são as legislações vigentes aplicadas a esses crimes, discorrendo a respeito da Lei 12.737/2012,

mais conhecida como Lei Carolina Dieckmann, O Marco Civil da Internet disposto na Lei 12.965/2014 e por fim a Lei Geral de Proteção de Dados descrita na Lei 13.709/2018. E ao final, tratará a respeito da casuística voltada ao crime cibernético, demonstrando quais foram os principais crimes já realizados contra a população brasileira nos últimos anos.

1. A EVOLUÇÃO HISTÓRICA DO MUNDO VIRTUAL

A Internet é uma ferramenta capaz de suprir as necessidades de seus usuários cada qual na sua individualidade. Com o intuito de se beneficiarem de todas as opções advindas de seu uso, aqueles que a utilizam sabem que a Internet nada mais é do que um instrumento que continua em constante evolução tendo como objetivo e finalidade proporcionar um método célere e eficiente para obtenção e disponibilização de informações.

O Direito, como ciência jurídica que disciplina os direitos e deveres de todas as pessoas, é o responsável por ordenar o regramento jurídico dentro da sociedade. Com o dever e a missão de acompanhar toda evolução que possa surgir dentro do ambiente cibernético e por tratar-se de um novo instrumento que disponibiliza vários tipos de serviços aos indivíduos, cabe ao Direito regular as condutas humanas que podem ser realizadas mediante o uso da internet.

Por isso é importante sabermos de início como foi a criação da internet, quais foram os fatores que a compuseram e como a sua utilização desde o dia do seu surgimento foi causando impacto entre aqueles que a utilizavam. O seu desenvolvimento engloba toda a sociedade, diante disso, a internet não só fez as pessoas se adequarem ao seu uso como também passou a ter o dever de suprir ou ao menos tentar realizar todos os desejos de seus usuários.

A internet foi criada a partir de um projeto militar norte americano durante o auge da Guerra Fria entre os Estados Unidos da América e a União Soviética na década de 1960. (LIMA, 2016, p. 23). Naquela época para os americanos foi essencial a criação da internet, pois em plena guerra lhes foi possível manter em um local seguro, mesmo que abstrato, os seus dados importantes podendo ser acessado em qualquer lugar.

Ainda que se tratasse de um ambiente terminantemente não concreto, os militares não acabaram por perder todas as informações pertinentes a sua base. Com isso, a internet era uma nova arma pronta para ser utilizada assim como um novo artifício a ser usado para fins militares com a missão de restabelecer uma base de dados mediante um ponto de conexão que com facilidade poderia ser repostado em qualquer localização.

Para o entendimento de PINHEIRO (2021, p. 21):

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

Foi uma construção mediante muita cautela, tendo em vista que queriam uma rede capaz de suportar qualquer tipo de ataque. Tiveram segurança e credibilidade, pois mesmo mudassem sua rota, independente do lugar para onde fossem, conseguiriam remontar um ponto de conexão com o intuito de assim reestabelecer todos os arquivos já armazenados anteriormente, independentemente do tempo de duração que a guerra tivesse.

De acordo com Lima, em 1970 quando a internet ainda era um ambiente onde os dados eram livres para trafegar, levando e trazendo conhecimento, a internet passou a ser utilizada pelas universidades como forma de trocar informações. (p. 23, 2016). Ao passo que cada pessoa na sua particularidade utilizava a internet para realizar um benefício próprio, a adequação do ambiente virtual para desenvolvimento de projetos voltados a área acadêmica, como uma ferramenta disponível para a troca de informação entre os centros de ensino, veio para contribuir na expansão da popularidade da internet, pois tratava de um novo mecanismo cujo qual promovia celeridade na resolução de pesquisas, o que por hora era essencial para as universidades.

Essa relação mútua que estava sendo dividida entre as universidades agregava na polarização do uso da rede, tendo em vista que apenas tratava-se de um novo método básico e completo para troca de informações e novos conhecimentos, que certamente serviriam como uma luva regada de um aparato de garantia nas pesquisas que posteriormente seriam realizadas pelas próprias instituições.

Conclui PINHEIRO (2021, p. 21) que:

“esse sistema passou a ser usado para fins civis, inicialmente em algumas universidades americanas, sendo utilizado pelos professores e alunos como um canal de divulgação, troca e propagação de conhecimento acadêmico-científico. Esse ambiente menos controlado possibilitou o desenvolvimento da internet nos moldes os quais a conhecemos atualmente.”

O uso da internet no meio acadêmico trazia mais benefícios no desenvolvimento de pesquisas, pois era utilizada como ferramenta de troca de informações entre elas. A internet

estava sendo usada pelos universitários de maneira exclusiva, mas já era hora de atingir o grande público e promover uma significativa expansão, aquilo anteriormente criado para guardar dados de uma base militar tornava-se essencial para o uso generalizado atingindo toda a sociedade contemporânea.

O uso da rede mundial de dados tornava-se uma plataforma indispensável, tendo em vista que se tratava de um ambiente virtual consideravelmente promissor para o desenvolvimento da sociedade, que não podia ficar recluso seu uso apenas destinado para determinada classe, mas sim acessível a todos os povos. A tecnologia da informação estava em desenvolvimento e por isso a internet precisava adequar-se as necessidades da coletividade.

Até então, qual malefício haveria em um espaço que estava sendo destinado a troca de informações entre centros de ensinos? Não obstante que por tratar-se de um novo instrumento para utilização dos usuários, subsequente a sua criação quando começaram a expandir-seu desenvolvimento e suas novas formas de uso, a internet não detinha regras para disciplinar o que poderia ser realizado em seu ambiente virtual sendo considerada uma terra sem leis.

Por isso, posteriormente, no ano de 1971, com os avanços das comunicações via internet, temos a criação do e-mail. Usado de maneira simples e direta, capaz apenas de encaminhar textos simples para o destinatário sem conseguir o remetente anexar qualquer outro arquivo no corpo da mensagem eletrônica. Tratava-se de um pequeno marco, se comparado com a grandeza que estava por vir. (LIMA, 2016, p. 23).

Ao passo que a transformação da era cibernética ia tomando novas formas, com a chegada do e-mail foi possível avistar uma nova modalidade de aproximar as pessoas e disponibilizar um apetrecho destinado a trocas de mensagens com mais celeridade. Dada a proporção de que se tratava de uma nova invenção terminantemente dirigida a incorporar mensagens de textos ora relevantes a serem direcionadas aos endereços eletrônicos que passariam a existir adiante.

É importante ressaltar que com todo esse avanço tecnológico desde a guerra, passando pela polarização da internet no meio acadêmico e a chegada dos e-mails, ainda não tínhamos algo disciplinando o uso dessa rede de dados que trafegava de maneira ilimitada. Por não haver restrições sobre o que poderia ser feito durante seu uso, era permitido a qualquer um fazer aquilo que bem entendesse no ambiente eletrônico sem

quaisquer tipos de limites ou punição, por esse motivo “Foi então que em 1978, houve o primeiro encaminhamento de spam (propaganda não autorizada pela internet capaz de ser enviada a diversas pessoas). (LIMA, 2016, p. 24).”.

Diante do exposto, de qual forma seria responsabilizado o indivíduo que estivesse usando o ciberespaço para difundir mensagens não permitidas, ou até mesmo como ele poderia ser banido daquele ambiente por estar trazendo notícias falsas em um ambiente até então dado como seguro para sua utilização. Por isso, antes mesmo de ser enviada a mensagem inoportuna, como seria possível para a rede já conseguir de imediato visualizar a mensagem de spam e conseguir bloqueá-la antes mesmo de ser entregue ao seu destinatário final?

Desta forma, estaria disciplinando o que poderia ou não ser incorporado a um correio eletrônico. Ao conseguir localizar seu remetente e já instaurando novos deveres para aquele que estaria se beneficiando de seu uso, mesmo que de forma maléfica do novo instituto disposto pela internet, seria um grande passo para a limitação do uso indisciplinado da rede, por isso era um avanço rumo a limitação do uso do espaço cibernético.

Para PINHEIRO (2021, p.21):

“Entretanto, o grande marco dessa tecnologia se deu em 1987, quando foi convencionalizada a possibilidade de sua utilização para fins comerciais, passando-se a denominar, então, “Internet”. Na década de 90, a Internet passou por um processo de expansão sem precedentes. Seu rápido crescimento deve-se a vários de seus recursos e facilidades de acesso e transmissão, que vão desde o correio eletrônico (e-mail) até o acesso a banco de dados e informações disponíveis na World Wide Web (WWW), seu espaço multimídia.”

Ao falarmos de algo que com uma ótima conexão e apenas um clique permite que se crie diante de nós um ambiente preparado para nos trazer diversas informações sobre determinado conteúdo, com seu avanço tecnológico desde sua criação e desenvolvimento, a internet trouxe o poder e o benefício de nos mantermos atualizados de toda e qualquer informação do mundo, logo que permite ao seus internautas (que mantem-se conectados através da rede mundial de computadores) o acesso a informações em tempo real.

Para LIMA (2016, p. 24):

“Já na década seguinte, continuou a internet longe do grande público, integrando-se, prioritariamente, a centros de ensino. Contudo, foi ainda nessa época que houve a criação dos primeiros endereços com terminação “.com”. Em 1991, Tim Berners-Lee lançou um sistema que permitiu a navegação mediante um revolucionário modelo que utilizava *hiperlinks*: o *browser* ou navegador. Dois anos depois, tínhamos o Mosaic, o primeiro navegador mais avançado a ser distribuído.”

Com a criação e o desenvolvimento de um novo navegador, foram aumentando as novas modalidades de pesquisas trazidas para este meio e então foi possível que mais pessoas pudessem usá-la de forma positiva. Os novos provedores de acesso foram capazes de alcançar os usuários comuns, e a internet não estava mais destinada a apenas a um público, mas sim a todos que dela quisessem desfrutar.

Salienta PINHEIRO (2021, p. 21) ao definir este marco que:

“Tecnicamente, a Internet consiste na interligação de milhares de dispositivos do mundo inteiro, interconectados mediante protocolos (IP, abreviação de Internet Protocol). Ou seja, essa interligação é possível porque utiliza um mesmo padrão de transmissão de dados. A ligação é feita por meio de linhas telefônicas, fibra óptica, satélite, ondas de rádio ou infravermelho. A conexão do computador com a rede pode ser direta ou através de outro computador, conhecido como servidor. Este servidor pode ser próprio ou, no caso dos provedores de acesso, de terceiros. O usuário navega na Internet por meio de um browser, programa usado para visualizar páginas disponíveis na rede, que interpreta as informações do website indicado, exibindo na tela do usuário textos, sons e imagens. São browsers o MS Internet Explorer, da Microsoft, o Netscape Navigator, da Netscape, Mozilla, da The Mozilla Organization com cooperação da Netscape, entre outros.”

“Devido a esta grande expansão, segundo o provedor de acesso norte-americano AOL (America On Line), a internet passara por sua primeira grande revolução quando alcançou o seu primeiro milhão de usuários. (LIMA, 2016, p. 24).”. Com a expansão dos números de internautas chegando, cresceram também os novos institutos nos meios de utilização da rede, foi o início de uma revolução que trouxe para os nossos lares, empresas e principalmente para o Estado um olhar transformador perante a sociedade digital que tomava um novo rumo e assim foram trazidas e disponibilizadas novas funções a serem destinadas para uso dos novos usuários.

Era chegada a hora da internet acompanhar as necessidades da população cibernética, tendo em vista que ao passo que cresciam os números de usuários da rede, cresciam também os anseios advindos desta determinada classe. Não podia ficar apenas ao Direito o dever de ajustar-se aos novos institutos apenas com o fim de disciplinar o convívio da sociedade digital no espaço cibernético.

Pontua PINHEIRO (2021, p. 21) que:

“Da transmissão de pacotes de dados simples, evoluímos para a transmissão de áudio e vídeo, ou seja, conteúdo multimídia. Esse foi o segundo passo a caminho da convergência. Para a transmissão multimídia, passou-se a exigir equipamentos mais capazes e redes de maior velocidade ou com maior largura de banda. Assim,

a velocidade dos recursos tecnológicos foi crescendo rapidamente, até chegar à Banda Larga (broadband), com conexões ADSL¹¹, cabo e satélite. Estamos seguindo para um mundo de transmissões em tempo real, por meio de tecnologia streaming, uma evolução do conceito de videoconferência e a inserção de redes multimídias digitais que possibilitem interatividade, como a desenvolvida com linguagem MPEG4.”

A Internet por sua vez deveria acompanhar também a evolução humana, pois precisaria criar ferramentas para atrair novos usuários e facilitar ainda mais o seu uso. Com isso, chegavam os conteúdos multimídias a fim de disponibilizar novos institutos com amplo desenvolvimento e capacidade de abranger imagens, vídeos e sons, deixando disponível para uso do próprio usuário que para utilizá-lo, teria de ter um tipo de conexão mais potente.

Com mais uma função disponível, transformava-se em algo mais atrativo o uso da rede, ao passo que eram desenvolvidas novas funções, passava a ser ainda mais empregado o seu uso por toda a comunidade de maneira generalizada, e chamava atenção pois havia muita oportunidade disponível em um único sistema, sendo este capaz de permitir acesso a todo um aparato de informações.

É válido ressaltar a importância de se ter uma ferramenta desse tipo, pois, a forma de se receber acesso simultâneo a determinada informação, de forma mais rápida, mostrava que a transformação digital estava de fato conseguindo acompanhar aquilo que a sociedade pretendia ter. O recebimento de informações mediante áudio e imagem demonstrava que grandes avanços estavam acontecendo e a comunidade estava obtendo respostas para aquilo que procurava.

O que antes era comumente realizado de forma presencial, passara a poder ser realizado por intermédio da Internet, um exemplo que se pode considerar frequente é a nova forma de conseguir realizar as transações diante de ambientes comerciais, instituições bancárias, faculdades de ensino à distância (EAD) ou até mesmo unidades hospitalares, e tantos outros ambientes essenciais que poderiam aderir um sistema para fazer transitar dados relevantes.

Conclui PINHEIRO (2021, p. 22) que:

“Todas essas relações entre pessoas e empresas passam a exigir novas regras, princípios, regulamentos, assim como possibilitam a aplicação de antigos princípios que continuam tão atuais para o Direito como o eram em sua origem.”

Tudo aquilo que foi vindouro de um projeto militar, que logo depois passara a ser usado para troca de informações de centros de ensino, posteriormente com a chegada do e-mail e o desenvolvimento de navegadores para facilitarem o usufruto dos internautas, a internet foi tomando formas anteriormente nunca previstas. Logo, ao se adequar as necessidades humanas e terminantemente estar disponível para realização de mais de uma função, a internet mostrou para o que foi criada.

Ressalta LIMA (2016, p. 25) que:

“Contudo, entre 1999 e 2004, começaram a ser criados fóruns de discussões nos quais era possível que um usuário sem conhecimentos técnicos pudesse enviar uma informação com o simples apertar de um botão “publicar”. Foi, portanto, o embrião das grandes redes sociais que viriam poucos anos depois. Em 2004, surge uma segunda revolução da internet com a criação das primeiras grandes redes sociais. Surgem, nesse ano, por exemplo, o Orkut e o Facebook. É o início da chamada Web 2.0, período em que a publicação das informações estaria mais popularmente distribuída. Expandem-se as possibilidades de conexão entre as pessoas e a facilidade de publicar material na internet. Todos passamos a estar a um clique de publicar algo que pudesse prejudicar alguém e a poucos links de visualizar algo que pudesse nos ofender ou nos deixar feliz”.

Ao Direito, passou a responsabilidade de regradar todos estes recursos provindos do desenvolvimento cibernético, como ente capaz e disponível para criar recursos disciplinares, a fim de pôr ordem e fazer valer todos os instrumentos legais dispostos, não somente em sua carta magna, mas também em diversas leis que foram criadas, ficou o dever de organizar e dispor para a sociedade quais recursos poderiam ser utilizados em caso de conflito de interesses no que diz respeito ao uso cibernético.

Tendo em vista que a Internet tem a capacidade de levar e trazer informação a todos os lugares e, mediante um clique, qualquer pessoa tem acesso a aquela publicação ou anúncio, tornou-se ainda mais atrativo o uso da rede de dados como também uma forma de interação social promovendo a comunicação entre todos os povos, sendo para manifestar seus interesses pessoais como também para conseguir expor opiniões e discutir sobre os seus ideais religiosos, políticos e pensamentos adversos.

Dessa forma, criou-se modos de práticas delitivas que passariam a ser executadas no ambiente virtual. Crimes que anteriormente eram realizados fora da internet mesclaram para dentro da rede de dados, pois seriam praticados de maneira mais fácil por tratar-se de um ambiente ainda não disciplinado e regrado pelo ordenamento jurídico e que por meio

da rede mundial de computadores os criminosos poderiam atingir ainda mais usuários, visto que se tratava de maior circulação de informações trafegando sem limites.

Com a criação do Youtube no ano de 2005, foi possível que os usuários pudessem divulgar e assistir a vídeos publicados na internet (LIMA, 2016, p. 25). Com isso, para as empresas no geral, a utilização da rede serviria como uma base para conseguir auxiliar os meios de comercialização, fazendo com que determinado produto chegasse ao seu consumidor final de forma virtual, assim também para realização de prestação de serviços.

A divulgação através da internet, seja de um determinado serviço prestado por uma empresa ou por uma pessoa, passou a atrair ainda mais atenção do público, logo que quando divulgada na rede ao invés de realizada a sua propaganda de porta em porta, sua publicidade não fica apenas destinada ao público local como também de forma regional, estadual e até mesmo mundial, conseguindo assim uma divulgação mais ampla do que o esperado.

De acordo com as demandas que passaram a existir após o contínuo e duradouro desenvolvimento da rede mundial de informações, a sociedade passou a usufruir ainda mais do ambiente eletrônico. Diante de novas necessidades que as pessoas precisavam suprir, ficava a busca incessante pela celeridade na resolução de pesquisas e por resultados imediatos, sendo diversas as formas de uso como por exemplo a utilização da internet como um instrumento essencial na realização de trabalhos anteriormente prestados de forma presencial.

Ao entender de muitos, a internet não passava de uma terra sem leis onde sua crescente evolução e aperfeiçoamento acabou por permitir que criminosos continuassem a cometer seus delitos neste novo ambiente sem que pudessem ser encontrados. Seria importante que pudessem ser identificadas essas pessoas e fosse realizada por elas o cumprimento de uma sanção quando realizado um crime tipificado na lei vigente, mas para isso também seria necessário que a comunidade no geral tivesse o conhecimento mínimo sobre quais os crimes cibernéticos que poderiam ser praticados e como seriam responsabilizados os delinquentes que o cometeram, tendo em vista que o crescimento da rede de internet a cada dia expandia seus horizontes atraindo mais internautas ao disponibilizar métodos fáceis de acesso à rede.

Relata LIMA (2016, p. 26) que:

“Até que, no início de 2007, Steve Jobs surpreende o mundo com o lançamento do primeiro iPhone. Temos um novo gigante passo. O mundo migraria grande parte das atividades de computadores para estes dispositivos menores e, com a melhoria na qualidade da conexão móvel, passaríamos a estar conectados a todo momento, recebendo e enviando informações no carro, no ônibus, na rua, na cama... Com a evolução dos smartphones, em especial a entrada do sistema Android produzido pelo Google, temos a popularização desses dispositivos, que passaram a ser usados, cada vez mais cedo, por crianças e adolescentes. Nesse momento, vivemos a explosão de aplicativos criados para essas plataformas, com a criação de redes de usuários conectados, transferindo todo tipo de informação.”

Com a finalidade de acompanhar a evolução digital dentro da sociedade, o Direito passou a dispor de novas leis para que pudessem ser disciplinadas as condutas meramente realizadas na internet. Com isso, boa parte das novas funções que passariam a ser desenvolvidas por intermédio da rede seriam terminantemente reguladas por legislações específicas dentre as quais: Lei Carolina Dieckmann (**LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012**); Marco Civil da Internet (**LEI Nº 12.965, DE 23 DE ABRIL DE 2014**) e Lei Geral de Proteção de Dados (**LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**).

2. LEGISLAÇÃO BRASILEIRA APLICÁVEL EM FACE DOS CRIMES CIBERNÉTICOS

Dada relevância de conhecer toda a evolução histórica da Internet, desde seu surgimento até seu uso atualizado nos dias de hoje, demonstrando todo o conjunto de novas funções e informações que a mesma, com tanto aperfeiçoamento, passou a dispor para que os usuários a utilizassem como um instrumento notoriamente indispensável, fica explícito que o seu uso fez com que a maioria das atividades anteriormente realizadas de forma presencial fossem praticadas dentro do ambiente cibernético com intuito de evidenciar mais praticidade e celeridade em sua execução.

O Direito é o responsável em disciplinar as condutas humanas praticadas dentro e fora do espaço digital. Ao tratar de condutas efetuadas dentro do ambiente virtual, posteriormente a realização de sua execução, serão acarretadas consequências para o mundo real. Com isso, ao passo em que a comunidade passou a utilizar com mais intensidade a Internet, o Direito passou a dispor de novas legislações para que fossem tomadas as devidas providências dentro do ambiente eletrônico com a objetividade de regradar os comportamentos humanos praticados dentro da rede de alcance mundial. Tornou-se extremamente necessária a criação de um órgão disciplinador para as condutas e delitos meramente praticados por intermédio da Internet.

Para CORRÊA (2000, p. 107):

Os operadores jurídicos deverão utilizar o bom senso para dirimir questões jurídicas relacionadas à internet, procurando sempre relacionar a parte técnica com o ordenamento jurídico em exercício. São as análises simples e lógicas que possibilitarão um eficaz entendimento das questões cotidianas de nossos tribunais, sendo, principalmente, os bancos acadêmicos os futuros responsáveis pela construção deste, já que é neles que existe uma verdadeira interdisciplinaridade, essencial para a resolução dessas novas questões. Por ser algo muito novo, e por versar sobre rotinas falíveis, a grande Rede constitui-se em um desafio, muito especial, para aquilo que visa pacificar e dirimir conflitos sociais, o direito. É nosso dever evitar que a ciência jurídica seja desgastada por algo responsável pelo seu desenvolvimento: a tecnologia (CORRÊA, 2000, p. 107).

Com esse objetivo, todo desenvolvimento e criação de novas leis vem para tratar de métodos destinados à eficiência de manter a sociedade digital protegida. Tendo em vista que embora o Direito tenha tido considerável evolução referente a prevenção e utilização da rede de dados, é notável o aumento de novos meios pelo qual poderiam ser cometidas

as condutas delituosas. Por isso, mesmo que haja formas de precaução, ainda serão possíveis novas formas de praticar condutas criminosas contra ou através do ambiente cibernético.

Ao observar a expansão do cenário digital, é possível notar que aumentaram os crimes cibernéticos devido a facilidade de realizá-los por intermédio da conexão à Internet sendo possível atingir um número maior de pessoas. Considerando o aumento dos crimes, nota-se que dentre os mais variados delitos possíveis de realizar, alguns já estavam elencados na parte especial de nosso Código Penal Brasileiro que está em vigor até os dias de hoje.

Ao tratar da esfera penal, existem diferentes vertentes que tratam das definições de crime. Entretanto, as principais classificações estão diversificadas nos conceitos que descrevem a concepção de crime como sendo de configuração material, formal e analítica.

Para ESTEFAM e GONÇALVES (2022, p. 315):

“O conceito material é o que se ocupa da essência do fenômeno, buscando compreender quais são os dados necessários para que um comportamento possa ser considerado criminoso ou, em outras palavras, o que justifica seja uma conduta considerada penalmente relevante aos olhos da sociedade. O conceito formal intenta definir o delito focando em suas consequências jurídicas, isto é, na espécie de sanção cominada. Assim, por exemplo, o inadimplemento contratual não pode ser considerado um crime, pois não acarreta a imposição de nenhuma sanção penal (pena privativa de liberdade, pena alternativa ou medida de segurança), mas apenas provoca o dever de indenizar a parte contrária. O conceito analítico, sobre o qual nos deteremos ao longo deste capítulo, trata de conhecer a estrutura e os elementos do crime, sistematizando-os de maneira organizada, sequenciada e inter-relacionada.”

A importância de toda sociedade obter o devido conhecimento referente a definição de crime trazida pelo universo penal ajuda a comunidade, de maneira generalizada, a compreender o significado de Crime Cibernético. Esta compreensão é indispensável devido ao notável uso básico da Internet como uma ferramenta inevitavelmente necessária para o desenvolvimento das relações humanas. O uso da rede de alcance mundial teve um grande favorecimento desde a sua chegada e popularização de seu uso.

Ao passo que se tornou um mecanismo indispensável para a comunicação e busca de informação em tempo real, garantindo uma célere e gratificante eficácia em relação ao tempo entre pesquisar e obter resultados, a Internet passou a ser empregada para a realização de novas condutas definidas anteriormente como crime. Seu uso para a propagação de informações falsas ou intermediação na obtenção de dados bancários para

ocasionar uma fraude bancária, traz para nossa pesquisa a necessidade de entendermos a definição do que é um Crime Cibernético.

Para FERREIRA (2005, p. 261), crimes informáticos são:

“Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial.”

Já para CASSANTI (2014, p. 22), Cibercrime é:

“Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cibercrime. Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital.”

Toda ação considerada ilícita sendo promovida contra ou por intermédio da Internet é considerada um crime cibernético, por isso podemos notar que algumas condutas meramente realizadas por meio de um computador ou smartphone conectados à rede de internet, tendo a mesma como uma intermediadora para a realização de delitos, caracteriza o que comumente hoje chamamos de cybercrime.

Tratava-se de práticas ora vistas como não sendo passíveis de punição, logo que seus infratores realizavam estas em outro ambiente terminantemente considerável de forma abstrata. É dada a relevância de que a Internet não possui um corpo físico, mas traz em sua essência a incrível capacidade de causar danos a vida social de qualquer pessoa física ou jurídica, logo que ambas podem sofrer uma violação em face de sua dignidade tendo sua honra violada ou patrimônios atingidos. Estas condutas ilícitas descritas em texto de lei, ao serem praticadas no espaço cibernético, podem obter o resultado pretendido de maneira mais fácil e atingir um maior número de vítimas.

Conclui BERTHOLDI (2020, pág. 11) que:

“O aumento significativo da criminalidade cibernética em nosso país tem duas causas básicas: a primeira está relacionada diretamente com o fato de que a web permite que os criminosos tenham franco acesso a um número significativo de vítimas, sendo inegável a grande escalabilidade dessa atividade criminosa, especialmente em uma nação que pouco se preocupa com educação básica de uso e de segurança na internet.”

Um caso de crime cibernético que tomou repercussão a nível nacional foi quando no ano de 2012 a atriz Carolina Dieckmann sofreu uma invasão de dados em seu dispositivo

pessoal quando criminosos tiveram acesso a seu computador e divulgaram fotos íntimas da atriz na internet sem seu prévio consentimento. Quando os criminosos tiveram acesso ao e-mail pessoal da atriz e capturaram algumas fotos íntimas dela, passaram a extorqui-la a fim de obter dinheiro em troca de não divulgar essas imagens. (LIMA, 2016, p. 164).

Por tratar-se de um crime praticado por intermédio da plataforma digital e por envolver uma atriz nacionalmente conhecida, grande foi a propagação da notícia na mídia, e posteriormente ao acontecimento que repercutiu em grande escala, foi necessária a criação de uma nova lei que disciplinasse a invasão a outro dispositivo informático, pois está prática criminal chegou ao conhecimento do Poder Legislativo Brasileiro.

Sendo assim, nosso sistema ao ver a necessidade de tipificar delitos cometidos de forma virtualmente, apressou-se ao promulgar a Lei nº 12.737 de 2012 que criou a norma federal específica (LIMA, 2016, p. 164). A referida lei que recebeu o nome de lei Carolina Dieckmann é uma alteração realizada em nosso Código Penal Brasileiro e sua aplicação é voltada contra a realização de crimes virtuais e delitos informáticos, assim sendo possível a tipificação de crimes na Internet.

Após o ocorrido e a fim de promover uma maior seguridade no ambiente virtual, sabendo que já existiam essas práticas delitivas, mas que não eram tipificadas em nenhum texto de lei, com a objetividade de disciplinar o uso indevido de informações e desrespeito à privacidade de qualquer pessoa na internet, a referida Lei nº 12.737/12 acrescentou os artigos 154-A, 154-B e alterou a já existente redação dos artigos 266 e 298 do Código Penal.

Destaca-se, então, na íntegra os referidos artigos:

“Art. 154 – A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagens ilícita:

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 1.º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2.º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.

§ 3.º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

§ 4.º Na hipótese do § 3.º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5.º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I – Presidente da República, governadores e prefeitos;

II – Presidente do Supremo Tribunal Federal;

III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV – dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

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.

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:

Pena – detenção, de 1 (um) a 3 (três) anos, e multa.

§1.º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§2.º Aplicam-se as penas em dobre se o crime é cometido por ocasião de calamidade pública.

Art. 298. Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:

Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.”

Para que haja a existência de uma nova lei, deverão estar presentes nela dados básicos para sua interpretação. Embora a lei tenha sido criada, ainda foi possível observar que na mesma possui a existência de lacunas na descrição de seu texto legal. No tocante ao seu caput, considerado longo para uma lei de importância penal, fica enigmático o seu entendimento logo que por tratar de um texto de lei não deveria ocorrer este tipo de mau entendimento por parte daqueles que a utilizam (LIMA, 2016, p. 164).

É primordial que uma lei quando expressa e disponível tenha todos os mecanismos necessários para que possa ser empregada de maneira eficaz, tendo em vista que não podem faltar informações consideradas indispensáveis para sua compreensão. Após sua sanção realizada no dia 30 de novembro do ano de 2012, a Lei 12.737, que ficou popularmente conhecida como Lei Carolina Dieckmann, posteriormente ao representar um

precioso avanço em nosso ordenamento jurídico, acaba por deixar uma dúvida no tocante a aplicação de suas sanções de caráter brandas (WENT; JORGE, 2013, pág. 245).

Como visto anteriormente em nossa pesquisa, os atos praticados contra o sistema de internet com o desejo de conseguir invadir os dispositivos informáticos, não eram suscetíveis de punição pois não eram tratados como crime. Contudo, foi necessária a criação desta lei disciplinando os referidos crimes cibernéticos e com alteração em nosso Código Penal, trouxe a oportunidade de toda a sociedade digital ser protegida por uma legislação vigente.

Tendo como objetivo jurídico a seguridade em face de qualquer tipo de invasão na internet, no que diz respeito ao texto de lei, sua descrição retrata o acesso indevido em face de computadores, tablets, celulares e dentre outros dispositivos alheios, que possuem conexão a uma rede de internet, considerando esta prática um ato de violação. Muitas pessoas utilizam estes aparelhos a fim de facilitar suas atividades cotidianas, por isso esta limitação serviu para que fossem disciplinados atos que rompem os limites da particularidade das pessoas.

Pontua JESUS e MILAGRE (2016, p. 36) que:

“Na sociedade contemporânea, cada vez mais dependente de tecnologia da informação, é impossível se cogitar uma pessoa física ou jurídica que não interaja com pelo menos um dispositivo informático. Grande parte da população possui telefones celulares. Existem no Brasil mais de 250 milhões de aparelhos celulares.”

Este crescimento tecnológico fez com que as pessoas se direcionassem a utilização de novas ferramentas que estavam disponíveis para uso, ficando ainda mais fácil se expor ao risco. Por isso houve o crescimento significativo do uso de aparelhos celulares que passaram a dispor das funções que facilitariam o uso da comunidade e este emprego do aparelho eletrônico nas relações cotidianas, trouxe benefícios ao disponibilizar aplicativos que poderiam aproximar as pessoas umas das outras para troca de informações e demais funções disponíveis em seu sistema funcional.

Porém, manter todas estas informações localizadas em apenas um lugar, em um único dispositivo, fez com que aumentassem os riscos de indivíduos sofrerem uma invasão de dados. Por isso, a referida lei aponta em seu texto legal que a invasão indicada é exclusivamente cibernética, pois para sua execução é necessária que ela seja realizada

apenas por intermédio de computadores ou dispositivos que possuem conexão à Internet (BRASIL, 2012).

Com a criação da Lei Carolina Dieckmann, outra norma reguladora foi a inclusão do artigo 266 em nosso Código Penal. Este não era exposto ao abordar que tal “possibilidade de sistemas informáticos serem objeto do ataque envolvendo interrupção”. Por essa razão, tal espaço foi complementado com a disposição da Lei 12.737/12 (JESUS; MILAGRE, 2016, pág. 46).

Na mesma criação e inclusão de novos textos legais em nossa legislação vigente, com o intuito de conseguir proteger ainda mais os dados interligados a rede de Internet, a mencionada lei também trouxe em sua sanção uma breve alteração no artigo 298 de nosso Código Penal ao tratar da falsificação de documento particular, considerando como documento o cartão de crédito e débito. Por isso, pontua precisamente JESUS e MILAGRE (2016, p. 48) que:

“A falsificação de documento particular ou alteração de documento particular verdadeiro já era considerada crime pelo art. 298 do Código Penal, prevendo pena de reclusão de um a cinco anos e multa. O que a Lei n. 12.737/2012 fez foi inserir um parágrafo onde equipara ao documento particular o cartão de crédito ou débito.”

Com isso, podemos concluir que anteriormente à criação da Lei Carolina Dieckmann, nossa legislação vigente não possuía uma definição que enquadrasse e punisse os crimes cibernéticos advindos da Internet. Entretanto, ao criminalizar as condutas descritas em seu texto de lei, como o crime de invasão de dispositivos eletrônicos, obtenção ilícita de senhas de acesso, adquirir conteúdos, e-mails ou até mesmo pretender abalar sites de maneira intencional, mais do que a presença de críticas referentes às punições que estão previstas demasiadamente brandas, tendo em vista que no Brasil as penas que empregam até quatro anos de reclusão em face de crimes sem emprego de violência acaba por transformar-se em restrição de direitos, por isso, aquele que comete um crime de invasão de dados não perderá sua liberdade, logo que a nova lei dispõe de cumprimento de pena no máximo a um ano de detenção. (CASSANTI, 2014, p. 177).

Contudo, indica JESUS e MILAGRE que:

A Lei n. 12.737/2012 longe está de solucionar todos os problemas relativos ao crime cibernético no Brasil. A solução não é fácil de ser encontrada, mas com certeza não resolve tão somente com a edição de leis e mais leis criminais. Envolve educação digital, políticas criminais e estrutura investigativa. (2016, Pág. 71).

Desse modo, no tocante ao desenvolvimento de novas legislações disciplinadoras que abrangem a tecnologia da informação, que por sua vez continuou expandindo suas ferramentas, foi necessária uma nova regulamentação que definisse os limites permitidos para o uso da Internet. A Lei nº 12.965 de 2014 conhecida como Marco Civil da Internet. A mesma passará a vigorar com a objetividade de agregar definições a tudo que compõe a rede mundial de computadores, e por isso, foi considerada a “Constituição da Internet”. Esta referida lei vem para garantir os direitos e deveres pertinentes a todos que constituem a Internet Brasileira, sendo eles: os usuários da rede, os provedores de acesso e conexão e demais serviços em geral. (JESUS; MILAGRE, 2016, p. 71).

Este aumento na junção de comunicação e tecnologia da informação, realizou com eficiência mais domínios no que diz respeito às necessidades que a sociedade trouxe, fazendo assim com que mais pessoas acessassem a rede de internet. As pessoas passaram a necessitar de mais agilidade na busca por resultado e a Internet oferece esta solução para todo aquele que dela se beneficia, seja para resolver assuntos pertinentes a seu trabalho ou para realizar uma ligação em tempo real com alguém que mora distante.

A fim de promover uma exímia normatização no que diz respeito a utilização da Internet, o Direito veio buscando melhor forma de adaptação no tocante ao cenário contemporâneo, tendo em vista que novas atividades merecem uma nova regulamentação terminantemente eficaz ao que diz respeito ao desenvolvimento do Direito Digital. Para a sociedade é muito positivo os métodos fornecidos pelo espaço digital, porém, requer mais atenção na execução de suas funções mediante a falta de educação cibernética que muitas pessoas necessitam.

Esta lei regulamentadora vem para preparar a comunidade cibernética a fim de fazer com que grande parte de seus usuários possam compreender de maneira efetiva o que pode ou não caracterizar um crime de natureza cibernética. Por isso, a Lei 12.965/14 no caput do artigo 1º especifica que estabelecerá os mediante princípios, as determinadas garantias, quais os direitos e deveres das pessoas no que diz respeito ao uso da internet no Brasil. Diante do exposto, a criação do Marco Civil da Internet vem para complementar o que já foi publicado por meio da Lei Carolina Dieckmann, sendo uma lei nova para suprir e auxiliar a outra. Contudo, essa forma de garantia tem o intuito de estabelecer a proteção de direitos ora anteriormente não protegidos.

Por isso, segundo BARRETO e BRASIL (2016, p. 28):

“É válido destacar que o Marco Civil, apesar de visar primordialmente a tutela dos direitos civis na internet, também tem aplicação no Direito Penal e Processual, uma vez que estabelece conceitos fundamentais, bem como disciplina formas de obtenção de provas quanto à materialidade e à identificação da autoria delitiva.”

Acerca do que pretende a lei do Marco Civil, chama a atenção a perspectiva que ela tem quando traz em sua objetividade jurídica a vontade e o desejo de conseguir garantir a privacidade daquele que utiliza a internet bem como proteger os dados particulares dessas pessoas. A mencionada lei demonstra que uma de suas várias funções é acarretar proteção jurídica e oferecer uma base legal para o Poder Judiciário sempre que se deparar com problemas que abarcam questões referentes a internet e tecnologia da informação, bem como evitar decisões propriamente contraditórias relativas a temas idênticos (JESUS; MILAGRE; 2014, p. 18).

Sua criação deu-se após um extenso debate, diante disso em abril do ano de 2014 foi promulgada a Lei do Marco Civil da internet a fim de disponibilizar normas eficazes para conter e controlar questões referentes à vida particular das pessoas na rede, sendo esta legislação uma base para o mundo da sociedade digital. (LIMA, 2016, p. 168).

Com a publicação e vigência da mencionada lei, a fim de que todos tomassem conhecimento de sua pretensão rumo a uma eficácia, a estrutura de seus artigos é capaz de classificar e elencar tudo que vem a constituir a Internet, bem como cada conceito de todas as partes que agregam no desenvolvimento da Internet. Por essa razão, esta lei acaba por dispor em seu texto de lei conceitos que formam a rede mundial de computadores, pois, cada lei em sua especificidade vem para moldar e regular a utilização de determinado tipo de serviço.

A fundamentação do Marco Civil da Internet é baseada em formar normas específicas com o propósito de regular todas as movimentações que uma pessoa realiza no ambiente virtual, trazendo em sua base os referidos fundamentos da norma disciplinadora que rege o uso da Internet no Brasil. Sua respectiva fundamentação vem baseada em nossa Constituição Federal, tendo como ideologias a preservação e o respeito à liberdade de expressão, fundamentado em nosso artigo 5º e artigo 220º da referida Carta Magna de 1988. Tais direitos fundamentais dizem respeito ao “reconhecimento da escala mundial da rede; os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; a pluralidade e a diversidade; a abertura e a colaboração;

a livre iniciativa, a livre concorrência e a defesa do consumidor; e a finalidade social da rede”. (BARRETO; BRASIL, 2016, pág. 33).

Podemos afirmar que em razão de tal benevolência promovida em prol do respeito e da proteção civil de toda sociedade cibernética, evidencia-se que o legislador ao descrever a fundamentação da nova lei regulamentadora, vem com firmeza querer dispor e promover uma base para a indispensável educação digital que todos que compõem a comunidade digital merecem ter.

No que diz respeito ao Princípios do Marco Civil da Internet, salienta BARRETO e BRASIL (2016, p. 35) que:

“Os princípios estão expressos no Art. 3º do Marco Civil da Internet, não excluindo outros princípios decorrentes do regime democrático:

- Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal.
- Proteção da privacidade.
- Proteção dos dados pessoais, na forma da lei.
- Preservação e garantia da neutralidade de rede ¹⁰.
- Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas.
- Responsabilização dos agentes de acordo com suas atividades, nos termos da lei.
- Preservação da natureza participativa da rede.
- Liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.”

Ao passo que a rede cibernética expande seus horizontes, trazendo mais funcionalidade para o seu meio, cabe para as pessoas que utilizam a rede de dados, de forma precisa e indispensável, saber quais são os seus respectivos limites no que diz respeito ao que fazer ou não fazer na utilização da Internet, tendo em vista sempre sua proteção. Por isso, assim como nas outras áreas do Direito, a Lei do Marco Civil conta com determinados Princípios Basilares que ajudam estão mencionados na legislação em sua estrutura.

Como outrora visto em nossa pesquisa, a Lei 12.965/2014 traz em sua formação os determinados conceitos que compõem a Internet com a finalidade de ajudar a sociedade na compreensão destes e sua respectiva proteção. Com isso, nos aprofundaremos nesta formação dos devidos membros que ajudam no desenrolar da internet, a fim de entendermos como funciona cada parte que ajuda em sua construção.

Na análise voltada a este inciso presente no artigo 5º da presente Constituição da Internet, entende-se que de maneira generalizada, a Internet cuida de um aparato de informações que conseguem comunicar-se entre si, de forma mundial. Sendo permitido o tráfego de variados dados, concernentes às características públicas ou privadas. (BARRETO; BRASIL. 2016, pág. 37).

Contudo, no tocante à conceituação técnica de cada parte que assim formam nossa rede mundial de computadores, ressalta o descrito no artigo 5º e seus seguintes incisos da citada lei 12.965/2014 que:

I – Internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

II – Terminal: o computador ou qualquer dispositivo que se conecte à internet;

III – endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

IV – administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;

V – conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pelo internet, mediante a atribuição ou autenticação de um endereço IP;

VI – registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII – aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e

VIII – registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP."

Uma lei do porte em que se enquadra a Lei do Marco Civil da Internet tem a extrema necessidade de tratar os seus aspectos técnicos, logo que a indicada legislação vigente entende que seria arriscado uma lei deste porte não trazer em seu texto os conceitos que são relativos aos termos que a constitui, logo que poderiam ter interpretações diferentes e entendimentos posteriormente distintos ao disposto no artigo e seus incisos (JESUS; MILAGRE; 2014, pág. 26).

A fim de continuar no desenvolvimento de nossa pesquisa, é importante pontuar a relevância que o Marco Civil da Internet deu ao tratar também do rol de direitos dos usuários

que utilizam a internet no Brasil. Uma vez que a lei tem sua importância voltada a poder assegurar o usufruto de determinada ferramenta, proporcionando a todos os usuários segurança para tal ao realizar alguma tarefa onde seja indispensável o uso da rede.

Portanto, entende-se que o acesso à rede mundial de computadores é uma espécie de condição para o exercício regular da cidadania e que mediante ao regulamento disposto é capaz de demandar uma quantidade de iniciativas referentes ao Poder Público e instituições privadas com determinada pauta voltada à responsabilidade social. Logo que, a proteção à intimidade e a vida privada são previstas em nossa Carta Magna no fundamental artigo 5º, inciso X. O Marco Civil da Internet é tachado como a primeira lei que veio para regulamentar o tema da cibernética e esclarece em seu texto legal que cabe indenização por dano moral ou material quando este provindo de uma violação à intimidade e vida privada no que toca ao espaço digital. (JESUS; MILAGRE; 2014, pág. 33).

Nesta mesma linhagem, também foi criada a lei 13.709/18, mais conhecida como a Lei Geral de Proteção de Dados. Como constatado em nossa pesquisa anteriormente, o crescimento do número de internautas, desde a utilização da rede pelas pessoas físicas ou jurídicas, causou maior procura também pela prevenção no estabelecimento de regulamentos para uma confiança cibernética aos usuários. Por esse motivo, a nova lei vem para proporcionar a todos que trafegam na rede de dados, maior segurança na hora de sua utilização, que conforme vimos passou a ser indispensável o seu uso, a fim de normatizar também quaisquer tipos de operações que utilizem dados pessoais.

Para PECK (2021, p. 169):

“Com a Lei n. 13.709/2018 inaugurou-se um novo marco legal brasileiro para as instituições privadas e públicas. Isso porque a Lei Geral de Proteção de Dados Pessoais, ou LGPD, discorre acerca da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações que possam ser enquadradas como dados pessoais, ou seja, que estejam relacionadas a uma pessoa natural identificada ou identificável e que sejam tratadas em qualquer meio ou suporte, seja por pessoa jurídica ou por pessoa física.”

A referida lei traz em seu fundamento a alteração na forma como cada empresa e órgão público mantém os dados pessoais das pessoas que estão ligadas no empreendimento. Dados estes relacionados a toda pessoa que compõe aquele determinado grupo de pessoas que prestam serviços nas empresas, bem como dos clientes etc. Por isso, a LGPD foi criada a fim de proporcionar mais livre arbítrio e fortificação na privacidade de dados do usuário, norteando o respeito, garantindo a segurança e a

transparência ao usuário. Sendo que “atribuir funções de monitoramento e fiscalização a profissionais que não levem em conta a perspectiva do indivíduo, pode acarretar decisões conflituosas e distantes do propósito da legislação”. (PECK, 2021, p. 170)

Como foi possível compreender cada lei que combate o crime cibernético veio para complementar a outra, a fim de promover a toda sociedade digital maior segurança na hora da utilização da rede. Nos dias atuais é muito comum notar que grande parte das atividades realizadas anteriormente em ambiente físico, passou para o espaço digital e com isso passou a requerer maior precaução no uso da rede mundial de computadores. Por isso, ao tratarmos da aplicação da LGPD, será possível entendermos com mais profundidade o porquê da necessidade de sua criação.

Segundo PECK (2021, p.169) ao tratar da LGPD:

“É uma regulamentação considerada bastante técnica e que traz mais do que regras e diretrizes: traz princípios, direitos e obrigações relacionados ao uso das bases de dados pessoais, um importante e relevante ativo na sociedade atual. Importante destacar que o objetivo da LGPD é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, por meio da premissa da boa-fé para todo o tipo de tratamento de dados pessoais.”

É dada a relevância de entendermos que a facilitação do uso de dispositivos móveis que conseguem estabelecer uma conexão à internet, bem como a utilização de aplicativos em smartphones, fazem com que nossos dados fiquem expostos, pois no uso dessas aplicações ficam registrados nossos dados pessoais. Sendo assim, a maneira que confiamos nossos dados aos aplicativos e referidos sites de cadastro precisamos ter um tratamento específico em caso de fraude e assim por diante.

A Lei 13.709/18 prescreve em seu artigo 2º que:

“Art. 2.º A disciplina da proteção de dados pessoais tem como fundamentos:

- I – o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV – a inviolabilidade da intimidade, da honra e da imagem;
- V – o desenvolvimento econômico e tecnológico e a inovação;
- VI – a livre-iniciativa, a livre concorrência e a defesa do consumidor; e
- VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.”

A Lei 13.709/18 classifica os direitos fundamentais que cada pessoa no uso de suas atribuições, ao passo que efetiva o emprego de seus dados pessoais, passa a ter assim que estes ficam dispostos na rede de internet, A validação da eficácia dessa lei vem para assegurar a qualquer pessoa uma proteção promovida pelo Estado de Direito que tem como objetividade garantir os direitos referentes ao bem-estar social de cada pessoa que o compõe.

Trata-se de mais um grande passo na busca incessante pelo avanço nas soluções de conflitos advindos do mau uso da rede de internet, logo que a LGPD surgiu como um marco promissor para a legislação brasileira em face de estabelecer limites para os usuários, promovendo uma navegação mais regrada e a seguridade dos dados pessoais. Tendo em vista que todo aquele que não seguir o que está disposto nesta norma vigente, passará por aplicações de sanções já previstas e executadas nesta referida lei.

Ainda assim, a presente lei é terminantemente mais breve e em algumas situações deixou sua interpretação mais complexa, ressaltando diversos pontos em que trata sobre a insegurança jurídica ao proporcionar lacunas para subjetividade onde seria correta haver uma afirmação. Logo que isso acontece quando se trata de prazos, tendo em vista que enquanto a GDPR (General Data Protection Regulation) prevê prazos mais exatos de 72 horas, a Lei Geral de Proteção de dados prevê um “prazo razoável”. (PECK, 2021, pág. 170).

A apontada lei de dados pessoais vem para mostrar sua eficácia em tempos que vivemos situações já vistas fora do ambiente cibernético, porém ao adentrarmos neste espaço eletrônico acabamos por ficarmos expostos, em consequência, promove a defesa e proteção dos direitos dos cidadãos no momento em que há muita clareza na exposição de dados em virtude do mal uso da sociedade digital, sendo assim, esta lei vem para ajudar a complementar o que já foi divulgado em nosso Marco Civil da Internet.

3. CASUÍSTICA- CASOS CONCRETOS DE CRIMES DIGITAIS

É indispensável que seja tratado em nossa pesquisa a causa de aumento de casos relacionados a crimes cibernéticos no Brasil, pois este assunto tem sido cada vez mais discutido em nossa sociedade e por isso, este aumento é bastante considerável por ocasionar problemas diversos não somente nas relações pessoais. Devendo de ser tratado como um grande desafio, logo que se trata de uma ampliação delituosa também ocasionada durante a pandemia do Covid-19 onde cresceram os números de pessoas que passaram a utilizar a internet.

No decorrer da pandemia, podemos notar que cresceram os números de casos de crimes cibernéticos, haja vista que precisamos pontuar precisamente o porquê desses aumentos, como também por que tem acontecido essas condutas delituosas de forma mais frequente em nosso país. Talvez a resposta que procuramos se encontre no motivo de que o isolamento social fez com que as pessoas utilizassem com mais frequência as ferramentas digitais que já lhe eram oferecidas anteriormente.

Segundo o portal de notícias G1:

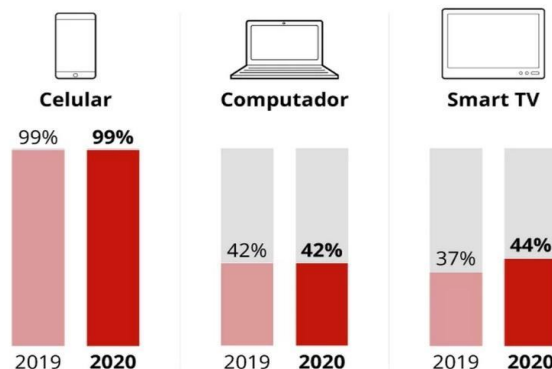
Acesso à internet no Brasil

Edição de 2020 da pesquisa TIC Domicílios indica aumento do uso da banda larga



Dispositivo de acesso

Celular segue como o principal meio para acesso à internet. Uso da televisão cresce e supera o computador



Como a internet foi usada

Com a pandemia, mais brasileiros recorreram à internet para realizar atividades à distância, como trabalhar e estudar



Fonte: Cetic.br



Infográfico elaborado em: 18/08/2021

FIGURA 1

<https://g1.globo.com/economia/tecnologia/noticia/2021/08/18/uso-da-internet-no-brasil-cresce-e-chega-a-81percent-da-populacao-diz-pesquisa.ghtml>

É importante ressaltar que ao passo que utilizamos estas ferramentas que nos são oferecidas para realizar determinadas atividades em nossos lares, mais tempos passamos conectados e com isso acabamos por nos sujeitarmos à exposição para a prática de determinados crimes. Dentre estes crimes podemos citar alguns crimes digitais comumente praticados, como por exemplo: fraude, roubo de dados e informações diversas dos indivíduos, pornografia infantil, cyberbullying, discurso de ódio e intolerância nos meios digitais.

Aponta o site de notícias Valor que:

“Segundo os dados da Coordenadoria de Estatística e Análise Criminal (CEACrim), da SSP, o ano de 2020 apresentou um crescimento de 265% nos crimes praticados no ambiente virtual no estado de São Paulo. Já no Rio de Janeiro, os casos de golpe na internet sofreram um aumento de 11,8% do total de crimes, de acordo com o ISP (Instituto de Segurança Pública), e Minas Gerais registrou alta de 50% no mesmo ano, segundo informações da polícia civil. Os ataques cibernéticos têm por objetivo principal se apropriar de informações e dados sigilosos, e estão se tornando cada vez mais comuns.” (DINO, 2022)

Talvez o motivo de acontecerem tantos fatos criminosos assim em nosso meio social seja a falta de conhecimento das pessoas em relação à segurança digital e seus modos de uso, logo que em nosso país podemos notar que as pessoas aumentaram a forma de acesso aos recursos tecnológicos e digitais, porém não tiveram um acompanhamento para

realização de tais atividades neste meio. Trata-se de recursos disponibilizados no espaço virtual que necessitam de uma orientação assídua, seja por intermédio de propagandas voltadas ao público adulto como também discussões a respeito deste tema nas escolas visando a educação digital de todas as crianças e adolescentes.

A sociedade precisava ter aprendido sobre a internet e seus recursos antes de manuseá-la, pois de nada adiantaria ter acesso ao recurso se não soubesse se prevenir de eventuais problemas que poderiam ser ocasionados com o mau uso dele. Como consequência deste constante mau uso, muitas pessoas passaram por situações negativas, sendo envolvidas em fraudes, vazamentos de dados e tantos outros problemas relevantes para nossa discussão.

Em 2021 houve um vazamento de dados de mais de 223 milhões de indivíduos em nosso País, sendo boa parte dessas pessoas já falecidas. Esse vazamento tinha como dados várias informações importantes das pessoas. Trata-se de um enorme problema voltado ao crime cibernético por envolver o vazamento de dados, por isso é relevante para nossa discussão notar que essa prática delituosa pode ocasionar situações criminosas a partir do uso desses dados expostos

De acordo com o site de notícias G1:

Quais dados vazaram?

Foram dois vazamentos:

Um deles tinha 223 milhões de números de CPF, acompanhado de informações como nome, sexo e data de nascimento, além de uma tabela com dados de veículos e uma lista com CNPJs (Cadastro Nacional de Pessoas Jurídicas). Essas informações circulam na internet de forma gratuita.

O outro incluía, além dos 223 milhões de CPFs, informações sobre escolaridade, benefícios do INSS e programas sociais (como o Bolsa Família), renda, entre outras informações. Esse está sendo vendido por criminosos.

Juntos, os dois vazamentos continham:

- Dados básicos relativos ao CPF (nome, data de nascimento e endereço).
- Endereços.
- Fotos de rosto.
- Score de crédito (que diz se é bom pagador), renda, cheques sem fundo e outras informações financeiras.
- Imposto de renda de pessoa física.
- Dados cadastrais de serviços de telefonia.
- Escolaridade.
- Benefícios do INSS.
- Dados relativos a servidores públicos.
- Informações do LinkedIn. (PORTAL G1, 2021)

Com essa falta de informação e conhecimento das pessoas referente as leis contra os crimes cibernéticos no Brasil, tendo em vista a pouca divulgação das respectivas leis, poucas discussões e poucas denúncias no que diz respeito a essas práticas delituosas, o crime cibernético acaba por continuar sendo executado em nossa sociedade e por isso continua a ser um grande problema para a população brasileira, ressaltando-se que essa prática de crime virtual não começou no ano de 2020 com a pandemia.

Embora existam leis que descrevem essas condutas criminosas, ainda existem muitas pessoas que nem se quer tem o conhecimento mínimo ou noção voltada ao funcionamento da lei em vigor que já está à disposição da comunidade brasileira no geral, por sua vez necessita de novas propostas que possuam em sua espécie a apresentação da importância da discussão sobre o crime cibernético e suas formas de prevenção.

De acordo com o site de notícias Exame:

A empresa de cibersegurança **Norton** divulgou recentemente os resultados de sua pesquisa, conduzida em parceria com o The Harris Poll, que destaca o **Brasil** como o terceiro país com mais dispositivos infectados por ameaças. De acordo com a análise, mais da metade (58%) dos brasileiros entrevistados afirma ter sofrido um **crime cibernético** em 2021. A pesquisa estima que cerca de 71 milhões de brasileiros sofreram ataques cibernéticos nos últimos 12 meses, e que mais de 828 milhões de horas foram gastas (uma média de 11,6 horas por pessoa) tentando resolver os problemas. Entre os entrevistados, 37% afirmam que detectaram software malicioso em um computador, rede Wi-Fi, smartphone, tablet, casa inteligente ou outro dispositivo conectado e 10% sabem que suas informações pessoais foram expostas em um vazamento de dados. A estimativa é que **32 bilhões de reais foram perdidos somente no ano passado**, já que mais da metade das vítimas de crimes cibernéticos do último ano foi impactada financeiramente. Dentre os 10 países entrevistados (Austrália, Brasil, França, Alemanha, Índia, Itália, Japão, Nova Zelândia, Reino Unido e Estados Unidos), o Brasil é o terceiro com mais aparelhos eletrônicos infectados por stalkerware, que são aplicativos de espionagem, e ficou atrás apenas da Índia e dos EUA. (PANCINI, 2022)

Tudo aquilo que pode ser cometido no real também pode ser realizado no virtual, por esse motivo é necessário a tipificação dos crimes realizados na internet, como outrora visto em nossa pesquisa, o nosso Código Penal Brasileiro já disciplina algumas condutas, por exemplo: ameaça, calúnia, difamação e injúria. Todos estes crimes são realizados também por intermédio da internet e na maioria das vezes o objetivo do criminoso ao realizar esta conduta punitiva é causar um prejuízo a imagem de alguém ou a uma empresa. Assim causando um transtorno ou até um considerável prejuízo financeiro, conseguindo vantagens ilícitas ou até mesmo um favorecimento sexual.

Tornou-se comum a quantidade de pessoas que passaram por um crime cibernético, logo que a maioria das atividades realizadas pela comunidade são executadas por intermédio da internet. Tudo precisa de um cadastro em site, seja voltado a compras online, consultar saldo bancário pelo aplicativo do banco, entre outras funções, nas quais todas necessitam do preenchimento de um cadastro onde ficam disponibilizados os dados pessoais dos indivíduos.

Ocorre que são variadas as formas de execução dos delitos cibernéticos, tendo sempre como objetivo principal invadir o dispositivo de outrem a fim de causar-lhe um dano e obter um benefício. São invasões a sites, invasão a sistemas de software, de dispositivos móveis, de computadores etc. Bem como a comercialização, produção, venda, compra, compartilhamento de sistemas e programas que são utilizados com finalidades criminosas como as fraudes bancárias com o intuito de furtar valores de contas correntes de bancos no Brasil.

Aponta uma reportagem do site Correio Braziliense que:

“O especialista em segurança pública e privada Leonardo Sant’Anna destaca que os brasileiros não têm muita cultura de cibersegurança. “O Brasil é um dos países em que mais se baixa aplicativos, além de aparecer entre os cinco que mais sofrem com golpes cibernéticos. Mas, quando a pessoa está baixando um aplicativo, esquece que, nele, vão todos os seus dados, todas as suas informações”, alerta. Ele acrescenta que, pelo gosto dos brasileiros pela tecnologia, o país é um mais afetados na internet em todos os aspectos. “O primeiro motivo para isso é a questão populacional, nós somos quase 220 milhões de habitantes, então, essa questão interfere muito”, explica.” (NUNES & STRICKLAND, 2022)

Também são inúmeros os casos de fake News e como elas trazem prejuízos para a imagem de uma pessoa, de uma empresa e do nosso governo brasileiro. Grandes foram as discussões relacionadas a cerca de empresas que são responsáveis por financiar sites, blogs, ou até mesmo perfis na internet que reproduzem notícias falsas para atacar aqueles que são contrários as opiniões do presidente da república Jair Bolsonaro.

Em notícia publicada pelo G1:

“O ministro do Supremo Tribunal Federal (STF) Alexandre de Moraes determinou nesta quarta-feira (4) a inclusão do presidente Jair Bolsonaro como investigado no inquérito que apura a divulgação de informações falsas. A decisão de Moraes atende ao pedido aprovado por unanimidade pelos ministros do TSE na sessão desta segunda (2). A apuração levará em conta os ataques, sem provas, feitos pelo presidente às urnas eletrônicas e ao sistema eleitoral do país. Mesmo após ser eleito, Bolsonaro tem feito nos últimos três anos reiteradas declarações colocando em dúvida a lisura do processo eleitoral. O inquérito das fake news foi aberto em março de 2019, por decisão do então presidente da Corte, ministro Dias Toffoli, para investigar notícias fraudulentas, ofensas e ameaças a ministros do Supremo Tribunal Federal. O ministro Alexandre de Moraes é o relator dessa investigação e,

por isso, coube a ele decidir sobre a inclusão do presidente Jair Bolsonaro.”
(PORTAL G1, 2021)

Tendo em vista que as causas dos aumentos de crimes cibernéticos se devem também ao fato do mal uso empregado pelos usuários, e por isso cabe a eles procurar por mais soluções passíveis de execução para sanar este tipo de ameaça que cerca a comunidade digital, sendo terminantemente importante para o Estado, as pessoas e empresas terem uma maior seguridade cibernética a fim de proteger seus dados disponibilizados na rede de internet.

As empresas que utilizam o espaço cibernético para realizar suas atividades rotineiras, bem como atender seus usuários, precisam de uma segurança virtual mais assídua. Logo que também todos os usuários que utilizam os bancos, as financeiras, os órgãos públicos, os restaurantes e os comércios online, precisam se conscientizar a respeito da realização do manuseio de determinadas funções oferecidas por esses grupos.

É necessário que não somente as empresas como também o Estado utilize de mecanismos eficazes para barrar organizações criminosas que utilizam os meios virtuais para concluir suas condutas ilícitas. Sendo assim, o Estado deve de especificar e detalhar como são aplicadas suas leis voltadas ao combate do crime cibernético, pois é importante que para que sejam evitadas essas condutas delituosas haja uma aplicação de penas mais graves a aqueles que praticarem crimes cibernéticos. Para a sociedade digital brasileira cabe dispor de uma maior fiscalização voltada a crime cibernético, bem como o Estado ser mais célere e eficaz no tocante ao procedimento da denúncia quando uma vítima procurar os agentes do próprio Estado para denunciar um crime realizado no ambiente virtual.

CONSIDERAÇÕES FINAIS

A internet foi criada com o propósito de guardar dados que pudessem ser restabelecidos independentemente do local onde o usuário estivesse, logo que se tratava de um período em que foi necessário à sua criação. Desde a sua construção, a internet passou por muitos ajustes a fim de sempre acompanhar as necessidades que seus internautas apresentavam conforme as mudanças que a sociedade vivia, ou seja, se a sociedade avançava a internet também precisaria avançar.

Com essas modificações foram permitidas que novas infrações fossem cometidas no ambiente digital, pois, tudo que anteriormente era realizado apenas no real passara a ser efetuado no virtual e assim criando formas de execução de crimes no ambiente cibernético. Essas atividades ilícitas mostraram que existira a necessidade de uma nova legislação que pudesse limitar o que o internauta poderia realizar ou não na plataforma digital, sendo suscetível de sanção descrita na lei vigente.

Por isso foi necessária a criação de leis específicas no decorrer de todo desenvolvimento cibernético, tendo em vista que ao passo que a comunidade digital disponibilizava suas novas funções, também eram criadas modalidades de execução de crimes que poderiam certamente trazer consequências mais graves e um número maior de vítimas. Todo o ambiente virtual pode guardar um aparato de informações pertinentes a toda e qualquer pessoa que o utiliza como uma base de dados, por isso é indispensável que existam legislações aplicáveis contra a prática do crime cibernético, sendo oferecida uma maior segurança cibernética a cada usuário digital.

Tomada a proporção nacional da invasão de dados sofrida pela atriz Carolina Dieckmann, nosso legislativo apresentou a lei nº 12.737/2012 com o intuito de que fossem resguardados os dados pessoais de cada pessoa. Sendo apresentada ao público esta nova lei, foi discorrido em seu texto de lei a objetividade jurídica que ela teria ao ser disponibilizada e aplicada pelo Estado em prol daquele que sofresse uma invasão de dados.

Como visto anteriormente, somente havendo sido criada a lei 12.737/2012 para regradar o uso indisciplinado do ambiente cibernético, não seria possível conseguir limitar todas as práticas abusivas realizadas por intermédio da rede de Internet. É de conhecimento geral que as condutas ilícitas efetuadas no ambiente eletrônico também passaram por aperfeiçoamento e por isso a lei precisou ter um desenvolvimento maior para

conseguir obter o resultado necessário capaz de barrar essas lacunas que poderiam ir surgindo no tocante a novas práticas delituosas, tendo cada vez mais leis disponíveis voltadas ao combate de crime cibernético.

Posteriormente foi desenvolvida a lei nº 12.965/2014 conhecida como o Marco Civil da Internet que disponibilizava em seu texto de lei a constituição da rede de internet. Ficando à disposição da comunidade quais fatores que compõem o ambiente cibernético, tendo em vista que a maioria dos usuários não sabiam como que funcionava o ambiente eletrônico que tanto usavam. Esta referida lei veio para complementar os espaços que outrora ficaram sem ser preenchidos pela Lei Carolina Dieckmann.

A partir do momento em que a lei fica disponível, ela precisa ter os mecanismos que facilitem o seu desenvolvimento ao ser empregado na sociedade, por isso, a lei do Marco Civil da Internet veio para complementar o que faltava e demonstrar em seu corpo de lei toda a sua fundamentação e base de princípios. Ao proporcionar benefícios para sociedade digital, aplicando os direitos e deveres de cada internauta, a nova legislação visava dispor mais respeito e proteção cibernética para todos os usuários.

A busca pela prevenção de dados entre pessoas físicas e pessoas jurídicas, fez com que uma nova lei pudesse ser disponibilizada aos brasileiros visando uma maior proteção jurídica na área da cibernética. A lei nº 13.709/2018 conhecida como Lei Geral de Proteção de Dados veio para dispor aos usuários da rede de internet uma maior seguridade voltada aos dados que trafegam na rede mundial de computadores, bem como estabelecer regras a respeito das operações que podem ser realizadas com a utilização de dados pessoas.

Com isso, a respectiva lei apresentou em seu fundamento geral quais as formas que as empresas ou até mesmo os órgãos públicos deveriam manter os dados pessoais de cada pessoa. Assim, promovendo a liberdade, privacidade e transparência sendo assegurado a qualquer pessoa física ou jurídica um tratamento jurídico amplo e específico a fim de que não haja uma disponibilização de dados privados sem a respectiva permissão de cada um.

Por fim, ao compreender quais os casos concretos referentes a prática de um crime digital, bem como entender mais sobre a realização de crimes anteriormente já citados, a Internet possui em seus respectivos sites de acesso um grande aparato de informações voltados a prática de crimes virtuais realizados no Brasil. Por isso é importante podermos conhecer cada prática delitiva que pode ser ministrada no ambiente virtual, como também

a forma que poderão ser denunciadas essas condutas meramente passíveis de punição por nossa legislação vigente.

A busca pela informação voltada a crimes virtuais no Brasil demonstra que muitas pessoas ainda não sabem como resolver este tipo de problema em caso de ataque cibernético. Contudo, é necessário entender quais passos são necessários dar quando tiver sofrido uma violação por intermédio da Internet, logo que ficou demonstrado em nossa pesquisa que os crimes cibernéticos são realizados de maneira rápida e eficaz, sendo que este método de realização de delito abrange um número maior de pessoas por tratar-se de uma forma mais célere em sua execução.

Conclui-se que a comunidade no geral precisa passar por uma educação digital, sendo necessário que cada pessoa entenda como poderá recorrer ao judiciário, logo que já existem leis vigentes que são aplicadas ao crime cibernético. Nosso ordenamento jurídico precisa ser acionado para que possa investigar e conseguir chegar a um culpado quando acontece uma ocorrência de crime digital. Por isso, para que uma lei tenha sua existência garantida, é primordial que ela seja conhecida por todos a fim de poderem usá-la como uma garantia quando seus direitos forem violados.

É de antemão indispensável que a publicação de sua vigência venha a ser conhecida pelo maior número de pessoas possíveis, tendo em vista que a lei também necessita de mecanismos que facilitem a sua vigência, não sendo ela de difícil interpretação e compreensão por parte daqueles que pretendem aplicá-la. Mas se as pessoas não denunciarem e não aprenderem também o que se pode ou não realizar na rede de internet, de nada adiantará uma lei voltada a esta prática delituosa.

REFERÊNCIA BIBLIOGRÁFICA

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. Manual de Investigação Cibernética à Luz do Marco Civil da Internet. Rio de Janeiro: Ed. Brasport, 2016.

BERTHOLDI, Juliana. Crimes Cibernéticos. Curitiba: Contentus, 2020.

Bolsonaro é incluído no inquérito das fake news: os principais pontos da decisão de Moraes. Portal G1. 4 de agosto de 2021. Disponível em: <https://g1.globo.com/politica/noticia/2021/08/04/bolsonaro-e-incluido-no-inquerito-das-fake-news-os-principais-pontos-da-decisao-de-moraes.ghtml>. Acesso em: 9 de junho de 2022.

BRASIL. Código Penal (1940). In. Vade Mecum Saraiva. 33. ed, atual. e ampl. São Paulo: Saraiva, 2022.

CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro: Brasport, 2014.

CORRÊA, Gustavo Testa. Aspectos Jurídicos da Internet. Saraiva. São Paulo, 2000.

DINO. Crimes digitais crescem pós-pandemia e provocam corrida por ciberseguros. 27 de junho de 2022. Disponível em: <https://valor.globo.com/patrocinado/dino/noticia/2022/06/27/crimes-digitais-crescem-pos-pandemia-e-provocam-corrída-por-ciberseguros.ghtml>. Acesso em: 12 de julho de 2022.

ESTEFAM, André; GONÇALVES, Victor Eduardo R. Esquematizado – Direito Penal – Parte Geral. 11. ed. São Paulo: SaraivaJur, 2022.

FERREIRA, Ivette Senise. *Direito & Internet: Aspectos Jurídicos Relevantes*. 2 ed. São Paulo: Quartier Latin, 2005.

Jesus, Damásio Evangelista, D. e José Antônio M. Milagre de Oliveira. *Marco Civil da Internet : comentários à Lei n. 12.965, de 23 de abril de 2014, 1ª Edição*, Editora Saraiva, 2014.

JESUS, Damásio Evangelista de; MILAGRE, José Antonio. *Manual de crimes informáticos*. São Paulo: Ed. Saraiva, 2016.

LIMA, Glaydson de Farias. **Manual de Direito Digital. Fundamentos, Legislação e Jurisprudência**. 1. ed. Curitiba: Appris, 2016.

Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. Portal G1. 28 de janeiro de 2021. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml>. Acesso em: 20 de julho de 2022.

NUNES, Vicente; STRICKLAND, Fernanda. **PCC e Comando Vermelho controlam crimes digitais; "phishing" aumenta**. Correio Braziliense. 9 de maio de 2022. Disponível em: <https://www.correiobraziliense.com.br/economia/2022/05/5006431-faccoes-criminosas-de-olho-nos-celulares.html>. Acesso em: 10 de agosto de 2022.

PANCINI, Laura. **58% dos brasileiros sofreram crimes cibernéticos, aponta estudo da Norton**. EXAME. 11 de março de 2022. Disponível em: <https://exame.com/tecnologia/58-dos-brasileiros-sofreram-crimes-ciberneticos-aponta-estudo-da-norton/> Acesso em: 3 de agosto de 2022.

PINHEIRO, Patrícia P. *Direito Digital*. Disponível em: Minha Biblioteca, (7th edição). Editora Saraiva, 2021.

Uso da internet no Brasil cresce, e chega a 81% da população, diz pesquisa. Portal G1. 18 de agosto de 2021. São Paulo. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/08/18/uso-da-internet-no-brasil-cresce-e-chega-a-81percent-da-populacao-diz-pesquisa.ghtml>. Acesso em: 01 de agosto de 2022.