CENTRO UNIVERSITÁRIO PRESIDENTE
TANCREDO DE ALMEIDA NEVES

GUSTAVO HENRIQUE R. RESENDE

CRIMES CIBERNÉTICOS E SEU IMPACTO NA ATUALIDADE

SÃO JOÃO DEL REI
2021

SUMÁRIO

RESUMO

Este estudo tem como objetivo realizar uma breve analise didática a respeito dos tão famoso e comuns nos dias atuais, os crimes cibernéticos e seu impacto na vida do cidadão Brasileiro. A criação de leis para suprir o vazio presente na constituição para esses novos delitos praticado com advento da tecnologia com a Lei Karolina Dieckmann, o Marco Civil e a LGP além de destacar certos crimes praticados nas redes socias.

INTRODUÇÃO

Nos últimos anos a utilização da internet e dos recursos tecnológicos se tornou algo essencial na vida cotidiana das pessoas, seja essa para fazer amizades, na busca de conhecimento, promover relações comerciais ou mesmo em investimentos. No Brasil cerca de 134 milhões de brasileiros tem acesso à internet como aponta estudos do Comitê Gestor da Internet no Brasil (CGI.br), entretanto mesmo inúmeros benefícios proporcionados pela tecnologia, esse mesmo recurso muitas vezes indispensável, apresentam diversos riscos que podem proporcionar transtornos ou prejuízos graves para a vítima. Nessas situações e existindo uma previsão penal, surgem os tão famosos crimes cibernéticos, os quais se caracterizam pela prática de delitos no ambiente cibernético, no caso a internet.

O meio virtual vem se apresentando cada dia mais um local com grandes taxas de incidência de criminalidade, de modo em que o anonimato de alguns se torna a poder e lucro para outros. Como já dizia o autor Moisés de Oliveira “A internet é uma grande praça pública, o maior espaço coletivo do planeta”.

Apesar dos inúmeros benefícios surgindo das evoluções tecnológicas, abriu-se uma grande oportunidade também para atos criminosos, e com a mundialização se tornou algo prático e rápido.

Diante desse cenário, o presente estudo tem como intuito de realizar uma breve analise a respeito dos crimes cibernéticos tecendo breves comentários acerca do surgimento das novas condutas criminosas, diante da maciça utilização da informática no dia-a-dia da população, abordando a problemática da aplicação do Código Penal frente a essas novas infrações, analisando-se as tipificações de tais comportamentos e a utilização da analogia em determinadas situações.

O presente trabalho se deu através do método dedutivo além da pesquisa bibliográfica de renomados autores sobre o assunto, análise das leis pertinentes ao tema trazendo atona os crimes cibernéticos praticados na atualidade no Brasil.

OS RISCOS E PERIGOS DO MUNDO DIGITAL

O mundo digital embora seja extremamente fascinante, ainda se mostra enigmático e perigoso ao homem comum o que pode gerar grandes riscos para o mesmo. Através da popularização do uso internet veio também a preocupação em relação a segurança dos dados que eram compartilhados online, não somente de uso para os governos e sim a todos que fazem uso dela.

O conceito de crime cibernético (cybercrime em inglês) surgiu na década de 90, através de uma reunião do G-8 (grupo formado pelos sete países mais ricos do mundo e a Rússia) no qual tinha como objetivo a discussão do combate a práticas ilícitas na internet de forma punitiva e preventiva. (D'URSO, 2017)

Através dos inúmeros avanços que a tecnologia vem sofrendo se torna cada vez mais difícil o combate a esses crimes, que se mantêm alinhado a esses avanços. Através do uso indiscriminado da internet, alguns indivíduos que tem pouco conhecimento de informática passou a se aprimorar e utilizar seus conhecimentos para praticar crimes como roubo de informações criptografadas, com intuito de ganho próprio (econômico ou no caso por mera diversão). (JESUS e MILAGRE DE OLIVEIRA, 2016)

Esses indivíduos mais conhecidos como *¨hackers"*[1], um termo importado da língua inglesa utilizado para denominar programadores muito habilidosos, que de forma secreta consegue obter informações do sistema informático de outra pessoa para vasculhar, usar ou troca de informação pelos mais variados motivos, tornando o cibercrime uma grande mazela que assola os dias de hoje.

[1](Definição retirado do dicionário online https://dictionary.cambridge.org/pt/dicionario/ingles/hacker)

CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Com fins didáticos, os estudiosos do ramo como a autora Rita de Cássia Lopes existem diversas classificações normativas para os crimes cibernéticos.

Entre as várias classificações adotadas na literatura para esse delito, duas se destacam-se sendo está uma que faz referência aos crimes cibernéticos puro, mistos e comuns e outra que classifica tais infração como impróprios e próprios.

Para o autor Rossini os crimes cibernéticos puro está ligado a comportamentos ilícitos com o intuito de atacar sistema computacional e seus componentes, tanto o hardware[1] ou software[2], englobando tanto os dados quanto o sistema em si. Nessa modalidade, o hacker tem como objetivo atingir o equipamento físico, o sistema informático e as informações dos bancos de dados. Simplificando, nessa modalidade temos a invasão dos sites e servidores.

Os crimes cibernéticos mistos a ação do delito está ligada essencialmente condicionado ao uso da internet para a pratica criminosa ser efetiva, onde o infrator visa bem jurídico distinto do informático. O agente não se dirige diretamente sua conduta ao sistema computacional ou no caso seus componentes, mas sim o uso da tecnologia, de modo que, como ferramenta primordial para a concretude da ação criminosa. Pode se utilizar como exemplo a retirada ilícita de valores monetários de contas bancarias através do ***homebanking***[3].

E por último porem não menos importante temos a conduta de agentes no qual se vale da rede mundial de computadores especificamente como um instrumento para a efetivação de um crime que já foi devidamente tipificado no Código Penal, caracterizando assim na modalidade de crime cibernéticos comuns.

Entretanto pode se perceber uma certa dificuldade em se reconhecer crimes cibernéticos impróprios praticados a patrimônios, já que estes não se conhecem nas informações armazenadas de um bem material, mas sim imaterial, incapaz da apreensão como objeto.

A estudiosa Rita de Cássia Lopes da Silva chega a conclusão de que:

> [...] *"*a informação neste caso, por se tratar de patrimônio, refere-se a bem material, apenas grafado por meio de bits, suscetível, portanto, de subtração. Assim, ações como alterações de dados referentes ao patrimônio, como a supressão de quantia de uma

> conta bancária, pertencem à esfera dos crimes contra o patrimônio”

CRIMES CIBERNÉTICOS PRÓPIOS E IMPRÓPIOS

Segundo o pesquisador Anderson Soares Furtado Oliveira, os crimes cibernéticos próprios seriam aqueles:

> [...] só pode ser cometido no ciberespaço, ou seja, necessariamente, deve ser realizado no ambiente do ciberespaço, para que a conduta seja concretizada, tendo um tipo penal distinto do tradicional. Ademais, tanto a ação quanto o resultado da conduta ilícita consumam-se no ciberespaço. (OLIVEIRA, 2009, p.33)

Pode se perceber que a discussão na aplicação das normas penais aos crimes cibernéticos está ligada diretamente aos crimes cibernéticos próprios.

Essa conduta denominada crimes cibernéticos próprios, tem como característica pela sua autonomia e distinção das infrações positivadas no Código Penal. Dessa forma torna um trabalho difícil para se criminalizar tais ações, pela falta da tipificação legal, já que o ordenamento penal brasileiro se pauta pela estrita legalidade, de modo a não punir infrações nas quais não estão previstas em lei.

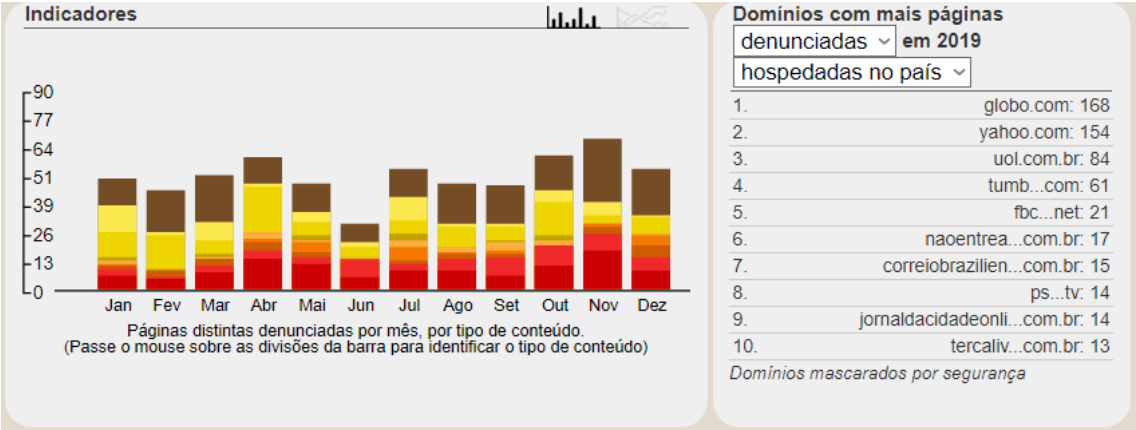
Sobre os crimes cibernéticos impróprios na visão do autor Aires José Rover, temos:

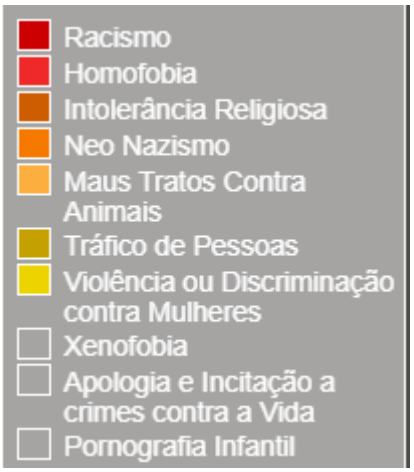
¨São todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta para a perpetração de crime comum, tipificável na lei penal. Dessa forma, o sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta. ¨ (ROVER, 2009, p.3)

Os crimes cibernéticos impróprios, considera-se possível a aplicação da norma penal para essa conduta, de modo que o indivíduo se utiliza de recursos informáticos como mero instrumento para a pratica de crimes previstos no Código Penal.

Vale a se ressaltar que a aplicação não se dá de forma sumária, devendo a conduta se amoldar a descrição do tipo penal.

Podemos observar através do gráfico os crimes cibernéticos mais praticados no Brasil em 2019 pelas denúncias online:





O gráfico acima retirado do site safernet representa os crimes com a maior taxa de denúncias praticadas pela internet no Brasil, onde será abordado alguns deles sendo esses:

CYBERBULLYING

O cyberbullying nada mais é que uma condição onde um determinado grupo ou um indivíduo pratica violência contra alguém através da internet ou também através de outras tecnologias relacionadas ao meio virtual. Sendo uma ação com a finalidade de agredir, perseguir, ridicularizar ou assediar determinada pessoa.

O foco do Bullying é aproveitar de uma suposta ¨superioridade¨ e anonimato presente nas redes para dirigir ataques contra a honra e a imagem de outrem. Os maiores alvos desses ataques são jovens e estudantes tendo uma relação conflituosa.

O caráter de interconexão presente nas redes sociais, possibilita com que vários indivíduos de grupos diferenciados tenham acesso, sendo fácil e suscetível a invasão e a intimidade com o objetivo da criação de um elo de poder, sendo o cyberbullying, necessitar de uma motivação, o qual deve ser analisada caso por caso, podendo ser a impopularidade nas redes sociais ou outros motivos, sempre existe uma exclusão interpretada por uma suposta inferioridade e o agressor por uma suposta superioridade.

Através desse sentido o art. 5 º inciso XXXIX da Constituição da República (1988):

> "não haverá crime sem lei anterior que o defina, nem pena sem prévia cominação legal" (princípio da legalidade e princípio da anterioridade).

Partir disso os crimes existentes no cyberbullying, seriam as condutas praticadas como a injúria, difamação, calúnia, constrangimento ilegal, ameaça, falsa identidade e extorsão, os meios de ação são feitos mediante ao ambiente virtual, principalmente ligado a troca de mensagens em redes sociais, diante dessas formas penais dos cyberbullying são elencadas.

A Constituição Federal tem um art. que demonstra a valorização do ser humano e a proteção da dignidade humana, como se observa a seguir:

> Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
>
> III - a dignidade da pessoa humana; também devemos tomar nota dessa dignidade que deve ser posta esse valor como objetivo da República Federativa do Brasil.

Sendo assim podemos observar que temos um rol de proteção do direito, porem nada de uma legislação especifica para tratar dos crimes cyberbullying, sendo uma conduta ligada ao ataque contra a honra e a imagem.

RACISMO VIRTUAL

A grande diferença consiste que no crime de racismo em ofensa a toda coletividade indeterminada, sendo esta considerada inafiançável e imprescindível prevista na lei 7.716/89, onde o crime de injúria racial prevista no Código Penal através do parágrafo §3 do art. 140, o qual consiste na utilização dos elementos sendo cor, etnia, religião, origem ou condição de deficiência física tendo pena de um a três anos mais multa.

> Conforme prevista a Constituição Federal (1988) termos tipificados pelo inciso XLII sobre o crime de racismo:
>
> 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:
>
> XLII - a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei.

A internet proporciona varias possibilidades aos crimes, uma manifestação racista verbal na maioria das vezes nem é compartilhada por muitas pessoas mas em razão disso quando a mesma ocorre na internet a repercussão e bem maior, deve-se investigar caso o criminoso está ou não agindo de forma individual ou junto a um grupo organizado, esse tipo de crime muitas vezes envolve imagens , comentários ou até mesmo vídeos que atingem a cor, religião e raça conforme prevista na lei 9.459/1997, o crime de racismo é inafiançável, imprescritível e sujeito a reclusão. Essas discriminações são previstas tanto em redes sociais, blogs, sites ficando bem mais fácil a identificação e a localização dos computadores destes criminosos.

Infelizmente o racismo está disseminado em nossa sociedade, alastrando a cada dia mais, sendo uma pratica de menosprezar, de denegrir a imagem alheia, pela sua cor, opção religiosa e cultural, sendo de extrema importância fazer a denúncia pertinentes a esses atos, para que assim possa penalizar as pessoas praticantes desse tipo de crime.

CLASSIFICAÇÃO DOUTRINÁRIA DOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos são classificados pela doutrina brasileira como delitos de cunho formal, uma vez que a mesma se consuma no momento que venha a ser praticado a conduta delitiva, mesmo sem a ocorrência do resultado naturalístico.

O Jurista Vicente de Paula por sua vez classificou os crimes cibernéticos como:

[...]Trata-se de crime comum (aquele que pode ser praticado por qualquer pessoa), plurissubsistente (costuma se realizar por meio de vários atos), comissivo (decorre de uma atividade positiva do agente: "invadir", "instalar") e, excepcionalmente, comissivo por omissão (quando o resultado deveria ser impedido pelos garantes – art. 13, § 2º, do CP), de forma vinculada (somente pode ser cometido pelos meios de execução descritos no tipo penal) ou de forma livre (pode ser cometido por qualquer meio de execução), conforme o caso, formal (se consuma sem a produção do resultado naturalístico, embora ele possa ocorrer), instantâneo (a consumação não se prolonga no tempo), monossubjetivo (pode ser praticado por um único agente), simples (atinge um único bem jurídico, a inviolabilidade da intimidade e da vida privada da vítima).

CONTEÚDO DA LEI E AS CONDUTAS PUNÍVEIS

A Lei nº 12.737/2012 –Lei dos Crimes Cibernético, ou também conhecida como Lei "Caroline Dickmann¨ trouxe um importante alterações ao Decreto-lei 2.848/40-Código Penal brasileiro de maneira a realizar a formalização e a tipificação das condutas delituosas na área da informático, constituindo os chamados "crimes cibernéticos". Vale se ressaltar algumas considerações sobre a lei mencionada.

A tipificação dos crimes informáticos já havia sido prevista no primeiro artigo do referido diploma legal, porém, baseando-se na hermenêutica jurídica, onde for citado os "crimes informáticos", devem ser interpretados como "crimes cibernéticos".

Enquanto o seu segundo artigo, havia realizado algumas alterações na seção IV do Código Penal brasileiro, no qual trata de crime contra inviolabilidade dos segredos, posto o qual acrescentou ao compêndio penal os dois artigos 154-A e 154-B.

Estes dois artigos buscam a proteção de qualquer violação nos dispositivos informáticos, como pode se observar:

> 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.
>
> § 1º 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.
>
> § 2ºAumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3ºSe 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 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4ºNa hipótese do § 3o, 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.
>
> § 5ºAumenta-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.

O caput descrito acima (art. 154-A do CP) representa um dos maiores avanços proporcionado por essa norma. Tendo como finalidade principal a de realizar o combate a principais práticas criminosas, mais conhecidas por trazer transtorno para quem a utiliza ou necessita de tais tecnologias.

Os novos artigos que foram inseridos no Código Penal brasileiro pela lei 12.737/2012 tem como objetivo de combater a invasão dos dispositivos informáticos alheios, que esteja conectado ou não a rede de computadores.

O tipo penal indica a necessidade do dispositivo informático tenha algum tipo de proteção ou mecanismo de segurança, sob pena de ser considerado desprotegido penalmente. (SANTOS, 2015)

Dessa forma para se enquadrar na conduta tipificada no regido artigo o sujeito teria que invadir, pra ser mais exato violar o dispositivo alheio, sem precisar necessariamente que o aparelho esteja conectado a internet, com a simples finalidade de obter, adulterar ou no caso destruir dados importantes de informação.

Previsto no § 1º, no qual está elenca como condutas normativas produzir, vender, distribuir ou difundir material alheio, constitui práticas que dependem das condutas típicas no caput art. 154-A, dessa forma, para cometer a conduta tipificada em questão, o criminoso deverá reunir tanto os elementos objetivos quanto subjetivos do tipo.

Entre as demais, os parágrafos 2º até o 5º do artigo mencionado, preveem qualificados pelo resultado, nos quais, serão configurados caso a invasão tiver como desfecho a aquisição de informações de comunicação privada, algum segredo comercial ou industrial ou sigiloso ou controle remoto não aprovado de algum dispositivo invadido, nessa hipótese, a pena poderá chegar de seis meses a dois anos de reclusão além da multa. Caso venha a ser comercializado ou a transmissão dos dados a terceiros obtidos através da invasão a pena aumentara a de um a dois terços. Caso essa invasão venha a ser praticado contra o Presidente da República, prefeitos e governadores, Presidente do STF, o da câmara Legislativa do Distrito Federal e Municipal ou com qualquer ¨cargos máximos¨ a pena irá aumentar um terço ou até mesmo a metade.

MARCO CIVIL NA INTERNET

Os direitos de cada usuário têm sua origem através da lei 12.965/2014, mais conhecida como Marco Civil da Internet onde a sociedade tem a necessidade de entender o que se caracteriza como um crime informático. Após os 15 anos de inúmeras discussões foi promulgado as determinadas leis 12.735/ e a 12.737/12, os quais passa a expor determinadas condutas no âmbito cibernético, o qual é necessário cautela por entendimento por ser uma legislação nova, necessitando o esclarecimento de quais condutas podem ou não ser punidas. A lei 12.735/2012 surgiu prevendo que os determinados órgãos de polícia judiciário poderão estruturar em termos de regulamentação, equipes e setores especializados no combate de sistemas de informatização.

Já a Lei 12.737/12 por sua vez esta longe de ser uma legislação capaz de resolver todos os problemas relativos aos crimes cibernéticos, a solução não seria apenas a criação e edição de leis mas também uma educação digital, politicas criminais e uma base investigativa mais eficaz. O Marco Civil pode ser considerado como a Constituição da Internet, garantindo assim os direitos e deveres inerentes a todos os usuários que utiliza a internet no Brasil.

No que tange os princípios do Marco Civil são especificados no art. 3º de sua lei, como podemos observar a seguir:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> I – Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
>
> II – Proteção da privacidade;
>
> III – proteção dos dados pessoais, na forma da lei;
>
> IV – Preservação e garantia da neutralidade de rede;

> V – Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI – Responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
>
> VII – preservação da natureza participativa da rede; VIII – liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

O Marco Civil da internet apresenta a possibilidade tanto as autoridades policiais quanto o Ministério Público possam fazer o requerimento de preservação dos registros de conexão, além do acesso a aplicações da internet, sendo no caso mantido por um ano ou até mesmo prorrogado caso seja devidamente solicitado pelas autoridades mencionadas, já no caso dos registros estes devem ser feitos a manutenção por seis meses, podendo haver prorrogação caso necessário, caso não houver o protocolo de representante judicial no prazo a preservação do registro em sessenta dias perderá a eficácia, o delegado tendo a evidencia deverá expedir o ofício ao provedor de conexão ou da internet, indicando assim a localização do suposto perfil ilícito e de seus dados.

O Marco Civil tem a capacidade de diferenciar o registro de conexão do registro de aplicação na internet, sendo o primeiro se tratar de informações referentes a hora e a data, o início e o termino de uma conexão de internet de um determinado endereço de IP. O segundo por sua vez seria o conjunto de funcionalidade no qual se referem a data e a hora, com tudo de uma forma determinada a aplicação da internet, partindo-se de um determinado endereço de IP. Ressaltando que tudo deve ocorrer com total sigilo sob um ambiente controlado e seguro, os registros dos provedores de conexão não podem ser passados a terceiros. Sendo estes dois elencados no art. 5 º do Marco Civil.

O inciso I do art. 7 º da lei do Marco Civil passa a tratar a inviolabilidade e o sigilo das comunicações da internet, salve regra caso venha a ser necessário por ordem judicial, para ser utilizado a fins de investigações criminais, no inciso V, o usuário não fornecerá a nenhum terceiro os seus registros de conexão e acesso a determinados aplicações na internet, salvo se a mesma tenha consentido ou em hipótese previstas em lei.

Podemos também a observa a neutralidade da rede prevista no art. 9 º da lei, tendo um acesso de forma igualitária na internet:

> Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

Entende-se que qualquer conteúdo que venha ser vinculado será removido via meio judicial, sendo os provedores obrigados a disponibilizar os registros e as informações da identidade do suposto usuário, sendo fornecido por um mandado, excluindo caso venha a ser conteúdo de nudez em que a notificação extrajudicial deverá ser atendida pelos provedores. Os provedores de conexão com internet, não serão responsabilizados civilmente pelos danos que possam ser gerados dos conteúdos de terceiros, poderá ser responsabilizado caso após ordem judicial especifica o mesmo não venha a tomar as providências no determinado prazo, através da remoção dos conteúdos infringentes e violadores como visto no Artigo 18 º.

Como se observa a lei Marco Civil tem como a finalidade de remoção de conteúdo, mantendo a proteção dos dados e criando um ambiente mais seguro para os usuários.

LGPD- LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS EM TECNOLOGIA DA INFORMAÇÃO

A lei de Proteção de Dados Pessoais 13.709/18, ou mais conhecida como LGPD, promulgada pelo ex-presidente Michel Temer no dia 14/08/18, sendo está uma legislação técnica com o intuito de assegurar uma gama de garantias previstas nos direitos fundamentais, a proteção dos direitos humanos de liberdade e privacidade, é um grande marco para a nossa legislação atual, impactando de forma geral tanto as instituições privadas quanto as públicas, sendo qualquer relação que envolva o tratamento de informações nos quais utilizem os dados pessoais, sendo este por qualquer meio, regulando princípios, direitos e garantias para uma sociedade digital firmada pelos dados pessoais.

A LGPD por ser uma legislação bem recente, que veio passando por várias atualizações, foi essencialmente inspirada pela Autoridade Nacional de Proteção de Dados (ANDP), uma representação da garantia da aplicação das normas trazidas com sua regulamentação, trazendo assim a regulação da proteção de dados para o Brasil, sem contar a ampliação do prazo para a sua entrada em vigor. A criação da ANDP foi criada com o intuito de trazer uma maior segurança e instabilidade.

> [...] O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização (PINHEIRO, 2020, p. 14).

A proteção de dados inspirada na Lei Europeia, bem conhecida também como General Data Protection Regulation (GDPR), a LGPD tem como finalidade geral de proteger os dados pessoais das pessoas tanto naturais quanto físicas, sendo as pessoas físicas o foco principal.

A proteção de dados vai ser garantida pelas plataformas e aplicativos, porem que exista muitas violações pertinentes ao uso indevido de tais dados pessoais, entretanto a lei 13.709/18, vem para proteção e sigilo dos dados em todo o território nacional, regulamentando o direito a privacidade e a proteção de dados, assegurando a todos os direitos fundamentais, inclusive no ambiente digital, tanto pessoa física quanto jurídico, sendo indevido, no caso sem a permissão da pessoa a publicação dos dados a terceiros, infringindo assim a nova lei.

A LGPD veio num momento crucial e importante no qual estamos vivendo, de forma promissora, tendo em vista a necessidade da proteção dos direitos pessoais dos cidadãos, em uma época onde o vazamento de dados está a cada dia mais comum e a exposição no âmbito virtual. A fiscalização e a proteção de tais dados são primordiais sendo uma lei complementar do Marco Civil da Internet.

CONCLUSÃO

Pode se concluir com tudo abordado nesse trabalho que apesar da evolução da tecnologia, os crimes vêm evoluindo na mesma proporção, contudo o Brasil infelizmente demorou para transpor essas leis para o papel e não só isso nosso código Penal não conseguiu acompanhar essa evolução. Os crimes sendo algo bem recorrentes em nossa sociedade, por ser bem mais lucrativos, tonando-se realmente algo bem critico com a facilidade do acesso da tecnologia à disposição de uma boa parcela da população, onde muitos acabam migrando para esse tipo de criminalidade, por acreditarem que o anonimato os protege de qualquer punição, consequentemente não temos de fato uma eficácia de nossa legislação pertinente a esses determinados crimes, estamos de fato vulneráveis aos delitos cibernéticos.

Os crimes por sua vez se tornam algo comum e cada vez mais prejudicial no Brasil, deve-se o legislador dar a real importância a essa temática, pois os infratores a cada dia que passa continuam cometendo crimes em escala cada vez maior.

Diante da lei 12.737/12 denominada como Lei Carolina Dieckmann, de fato houve uma significativa mudança, onde anteriormente os crimes informáticos não estava tipificado em nossa legislação, agora mostra um grande passo para o combate aos crimes cibernéticos.

Um outro meio de suma importância seria a investigação e os meios de provas para a identificação dos criminosos e as práticas delituosas cometidas no ambiente digital, um dos grandes problemas enfrentados por esse meio seria é que alguns servidores se encontram fora do país fazendo com que esses fatos demorem mais tempo para a obtenção de provas, precisando de ter a existência de uma cooperação internacional eficiente, ressaltando que o Brasil não faz parte da convenção de Budapeste que daria uma celeridade ao processo.

Para concluir se deve existir uma educação digital além de uma legislação especifica para a tipificação dos crimes cibernéticos, conscientizar as pessoas dos riscos presentes nessa ¨terra de ninguém¨, para que assim efetivamente venha a se reduzir os casos de pessoas infectadas por vírus e vítimas de golpes de estelionatários e crimes digitais, em geral.

BIBLIOGRAFIA

AFFONSO, Julia; COUTINHO, Mateus; MACEDO, Fausto. Para Janot, direito ao esquecimento não pode limitar liberdade de expressão. Publicado em 2016.

Link: https://politica.estadao.com.br/blogs/fausto-macedo/cibercrime-perigo-na-internet/

D'URSO, Luiz Augusto Filizzola. Cibercrime: perigo na internet. Publicado em 2017. Link: https://politica.estadao.com.br/blogs/fausto-macedo/para-janot-direito-ao-esquecimento-nao-pode-limitar-liberdade-de-expressao/

Michele, Berleze; Berlinda Silva, Pereira Publicado em 2017
Link: http://coral.ufsm.br/congressodireito/anais/2017/1-6.pdf

SANTOMAURO, Beatriz. Cyberbulling: a violência virtual. Publicado em 2010.
Link:https://novaescola.org.br/conteudo/1530/cyberbullying-a-violencia-virtual

Introdução à Computação Hardware, Software e Dados - 1ª Edição - André C. P. L. F. de Carvalho – 2017

JESUS ALMEIDA, BARBOSA MENDONÇA Crimes Cibernéticos-Publicado em 2013

Mapa site: https://indicadores.safernet.org.br