

CRIMINOLOGIA RELACIONADA AOS CRIMES CIBERNÉTICOS E A FALTA DE PUNIBILIDADE

Alexandre Gomes Faria Coutinho¹

RESUMO

Pode-se observar que com o passar dos anos e com os avanços da tecnologia e da internet, os meios criminosos também se desenvolveram. Apesar do direito se atualizar e sofrer modificações a todo o momento percebe-se que ele não consegue acompanhar os avanços dos crimes cibernéticos, isso fez com que essa modalidade de crime crescer rapidamente. Embora o Brasil tenha algumas leis específicas sobre o assunto elas ainda não suprem de forma eficaz a quem sofre esse tipo de crime. Podemos citar como exemplo de uma lei específica sobre crimes cometidos na internet a lei 12.737/12, mais conhecida como lei Carolina Dieckmann, trata como condutas feitas em meios digitais podem ser consideradas crimes. Diante este contexto prático o presente artigo vai expor conceitos acerca dos crimes cibernéticos e o acesso a justiça, abordará como o judiciário está tentando elucidar os conflitos, isso será possível através do levantamento de dados, estatísticas e estudo.

PALAVRAS CHAVE: Crimes Cibernéticos, Acesso a justiça, Internet.

ABSTRACT

It can be observed that over the years and with the advances in technology and the internet, criminal means have also developed. Despite the fact that the law is constantly being updated and modified, one can see that it cannot keep up with the advances in cybercrime, which has caused this type of crime to grow rapidly. Although Brazil has some specific laws on the subject, they still do not effectively provide for those who suffer from this type of crime. We can cite as an example of a specific law about crimes committed on the internet the law 12.737/12, better known as Carolina Dieckmann law, deals with how conducts made in digital media can be considered crimes. Given this practical context, this article will expose concepts about cybercrime and access to justice, and will address how the judiciary is trying to resolve conflicts, which will be possible through data collection, statistics and study.

KEYWORDS: Cybercrime, Access to justice, Internet.

¹ Graduando do curso de Bachelarel de Direito da Universidade do Grande Rio José de Souza Herdy, orientado pela professora Ana Paula Lopes

INTRODUÇÃO

Nos últimos anos com o grande aumento de usuários da internet e de recursos tecnológicos que são utilizados no cotidiano das pessoas, seja para atividades financeiras com os bancos, procurarem amigos, ampliar seu conhecimento, relacionamentos comerciais como, por exemplo, divulgações de diversos ramos empresariais, fazer investimentos e et. Apesar desses diversos benefícios que a internet nos trouxe também podemos elencar diversos pontos negativos que serão retratados no decorrer do presente artigo.

Nesta perspectiva, no primeiro capítulo será tratado como foco os fatos históricos da internet no mundo, como o surgimento e o como era realmente utilizada e seu principal foco na década de 1950. Neste primeiro capítulo também será tratado como a internet se formou até chegar aos dias atuais, e como se tornou indispensável para as pessoas nos dias atuais.

No capítulo 2, serão abordadas as principais dificuldades do nosso ordenamento pátrio acerca dos dispositivos legais que existem no nosso país referente aos crimes cibernéticos, mostrando suas alterações e legislações que estão em vigor, neste capítulo também citará as espécies mais comuns de crimes digitais e mostrar a complexidade para o enfrentamento do poder judiciário.

O capítulo 3, pretende demonstrar as principais condutas praticadas no cyberspaço e elencar alguns exemplos de práticas criminosas e evidenciar como nosso ordenamento jurídico trata esses tipos penais.

O capítulo 4 discutirá sobre o contexto atual dos crimes cibernéticos, e abordará como o nosso judiciário apesar de trazer diversas normas é evidente que ainda existem lacunas a serem preenchidas. Também será trado neste capítulo as forma de solução e otimização para a solução de crimes cibernéticos e como funciona o processo e julgamento.

Por fim, o principal objetivo deste artigo é externar como está o nosso ordenamento jurídico diante as evoluções que a internet trouxe para o nosso cotidiano, mostrar as diversas alterações que os magistrados tiveram que fazer perante todas essas mudanças. Ao final, serão discutidas formas que podem levar de fato a uma resolução dos enfrentamentos que essas mudanças trouxeram para o ramo jurídico. Cabe ressaltar que os responsáveis por promover a investigação criminal são a Policia Civil e a Policia Federal, este são os principais órgãos que tentam de alguma forma elucidar atividades criminosas que ocorrem no ambiente cibernético. Diante isso, serão apresentados também informações e os principais aspectos que rodeiam a cibersegurança e a investigação de crimes cibernéticos, e mostrar como podemos ter uma maior eficiência na investigação deste tipo de delito, pois a ajuda da vítima nesse tipo de crime na investigação é de suma importância.

I.1 INTERNET E SUA ORIGEM

A internet surgiu num contexto totalmente diferente do qual utilizamos ela hoje em dia. A Internet surge no meio da Guerra Fria de (1947-1991), tendo como sua principal função um possível sistema de descentralização com o pentágono, que com isso poderia escapar de possíveis ataques de outros países e se proteger contra guerras, pode-se perceber que a maior parte da evolução da internet se dá na área militar dos Estados Unidos, e tem como principal objetivo a defesa de seu país.

No ano de 1946, foi construído o primeiro computador digital, que foi chamado de ENIAC, a principal função era automatizar o cálculo de balísticas. Em 1957 a União soviética lança seu primeiro satélite espacial, e os EUA de contrapartida prometeu enviar um satélite para Lua para poder acelerar o crescimento tecnológico do país.

Com o passar dos anos foi se tornando cada vez mais necessário a criação de uma rede capaz de integrar computadores que estivessem distantes um dos outros, a partir disso foi criada a ARPANET, que no início foi criada ligando as universidades da Califórnia (Los Angeles e Santa Bárbara) a Universidade de Stamford (Santa Cruz) e a Universidade de Utah (Salt Lake City).

No ano de 1973, foi o ano da primeira conexão internacional da ARPANET, ligando os países da Inglaterra e a Noruega. No final dessa década a ARPANET substituiu os protocolos de comutação de pacote que utilizavam para Transmission Control Protocol/Internet Protocol (TCP/IP), protocolo que é muito conhecido até hoje no ramo da informática.

Na década dos anos 80, a ARPANET foi crescendo cada vez mais nos Estados Unidos, através dela foi possível interligar Universidades, governo e militares. E apenas no ano de 1986 a ARPANET começou a ser chamada de internet. Para que a internet se consolidasse foi de grande importância a criação da “WWW” – Word Wide Web e também da criação dos browsers. A internet chegou a um sistema global e público de rede de computadores.

Resumidamente, a internet e seus avanços se devem muito a tentativa de vários países tentar evoluir tecnologicamente a fim de se fortalecer cada vez mais a fim de demonstrar poder e até fazendo parte da corrida armamentista, pois quem conseguisse criar algo revolucionário naquela época estaria a frente dos outros que dependeriam dela para se proteger também.

I.2 CONTEXTO HISTÓRICO BRASILEIRO

Apesar de a internet ser criada em meio a guerra fria, ela só foi ser conhecida e ter uma grande expansão de fato nos anos 90. O princípio básico do que se tornaria a internet foi em 7 de abril de 1969, os conceitos começaram a surgir em meados da década de 1950. Sob o contexto da guerra, os EUA criaram um sistema de descentralização de suas informações no pentágono para evitar que possíveis ataques causassem a perda irreparável de documentos do governo.

Nos anos de 1970-1980, surge de fato o termo internet, nessa época que nasce os protocolos que conhecemos mais atualmente, obviamente que com alguns avanços, porém o conceito ainda é bem parecido.

No Brasil, o Instituto Brasileiro de Geografia e Estatística (IBGE), começaram a utilizar o computador UNIVAC 1105, durante década de 60. No ano de 1972 foi criado no Brasil o primeiro computador de fato Brasileiro, foi chamado no momento de “Patinho feio”, pela Universidade de São Paulo (USP). E em 1974 é criado a Computadores Brasileiro S.A. E em 1979, é criada a Secretaria Especial de Informática.

A internet chega ao Brasil em 1981, ela chegava ao nosso país pela Bitnet, que era uma rede de Universidades Americanas, a conexão era feito por meio de fios de cobre submarino até a fundação de Amparo a pesquisa do estado de São Paulo (FAPESP). Somente em 1994, a internet começou a ser comercializada no país pela empresa Embratel, 5 mil usuários foram chamados para testar o serviço na época.

I.3. EVOLUÇÃO E ADAPTAÇÃO AO LONGO DA HISTÓRIA CONSTITUCIONAL BRASILEIRA

Nota-se que a internet ganhou de fato relevância com o passar do tempo, podemos ver que até mesmo no nosso ordenamento jurídico foi afetado e alterações foram feitas para se enquadrar melhor com a evolução da internet. Um dos exemplos que podemos citar é a mudança que entrou em pauta no congresso no que diz respeito, do acesso a internet ser incluído entre os/ direitos fundamentais descritos no artigo 5º da Constituição, através da (PEC) 8/2020. Um dos principais pontos debatidos foi que o acesso a internet é hoje, um elemento fundamental para o desenvolvimento pleno da cidadania e para o crescimento profissional de todos e que sem dúvidas, a falta de internet limita as pessoas seja nas oportunidades de aprendizado, crescimento, de educação e de emprego, o que compromete não apenas o futuro das pessoas individualmente, mas um progresso em âmbito nacional.

Os crimes cometidos em ambiente virtual, não afetam somente as pessoas eles também prejudicam empresas e os negócios que estão envolvidos, dificultam muito a credulidade. O ordenamento Brasileiro conta com um grupo bem pequeno de leis que criminalizam e somente para algumas ações específicas não enquadrando alguns tipos penais que possam ser utilizados ou até mesmo já utilizados. Temos como principais normas as leis ordinárias, 12.965/2014 (Marco Civil da Internet) e 12.735/2012 e a 12.737/2012.

A mais conhecida e que teve uma aceitação não tão fácil, ocorrendo vários debates e controvérsias ao longo da sua tramitação foram a aprovação do Marco Civil da internet. A grande questão de debates quanto a lei está ligado as questões da privacidade, pontos como os provedores de internet manter os registros das conexões pelo período de até 1 ano e o histórico entraram em pauta. Outro ponto para essa lei ter tanto questionamentos foi pelo fato de ter sua criação ligada no momento em que o governo sofria diversos ataques cibernéticos, sites oficiais do governo foram atacados diversas vezes em um curto período de tempo.

Com relação à lei Nº 12.737/2012, surgiu para criminalizar a invasão de privacidade, Lei Também conhecida por “Lei Carolina Dieckmann” pela repercussão do caso da atriz Ana Carolina Dieckmann, quando teve seu dispositivo celular invadido e fotos suas vazaram.

A lei 12.735/2012 alterou algumas disposições da lei de crimes raciais, através dessa lei o magistrado conseguiu mais discricionariedade, até mesmo durante o inquérito para que a exibição de imagens ou símbolos que façam menção a qualquer forma de discriminação seja combatida.

Capítulo II – ORGANIZAÇÃO DOS CRIMES VIRTUAIS

II.1 LGPD E SUAS ALTERAÇÕES

A Lei Geral de Proteção de Dados (LGPD) é um tema que entrou em voga principalmente nos últimos anos, e que de fato se tornou lei (lei Nº 13.709/2018), é uma lei que trata especificamente sobre o tratamento de dados pessoais, essa lei também nos trouxe alterações em outros dispositivos que tratam sobre a internet em nosso ordenamento jurídico pode-se se citar como o exemplo a alteração nos artigos 7º e 16º do Marco Civil da Internet. A LGPD, é uma norma criada no ano de 2018, porém entrou em vigor apenas no ano de 2020, o principal objetivo desta norma é proteger os direitos ligados a privacidade e liberdade, que deveram ser seguidas por empresas e o governo com relação a coleta de dados pessoais sejam eles CPF, nome, endereço e outros dados extremamente sensíveis como a biometria e informações sobre politica e religião de cada individuo coletado. De modo prático a lei visa como principal objetivo, fazer com que a empresa explique para cada individuo o motivo, consentimento e a finalidade da empresa coletar os referidos dados, e caso a empresa disponibilize esses dados sem o consentimento do usuário ela será responsabilizada e sofrerá as punições cabíveis.

O Marco Civil da internet é uma lei criada no ano de 2014 (lei 12.965/2014), esta lei estabelece o uso e alguns parâmetros relacionados à internet, e como ele é utilizada e oferecida no Brasil, um grande projeto que até recebeu o nome de “Constituição da Internet”. O projeto desta lei está estritamente ligado para justificar a demora ocorrida durante o trabalho processual envolvendo os crimes cibernéticos, a lei foi utilizada como um argumento para ela fosse aprovada e em seguida ocorrer a aprovação da lei que tratava de crimes cometidos por meios de computadores.

Importante também destacar alguns princípios inerentes ao Marco Civil da Internet, são eles a Neutralidade de rede que tem como objetivo dificultar com que os provedores de internet cobrem valores diferentes dos usuários de acordo com o conteúdo que acessam; a Liberdade de expressão que faz com que todas as pessoas tenham igual direito de externar informações e opiniões na rede; e a Privacidade que faz com que as empresas fornecedoras e provedoras de internet não possam usar dados dos usuários para fins de comércio.

II.2 A COMPLEXIDADE DOS CRIMES DIGITAIS E O ENFRENTAMENTO PELO PODER JUDICIÁRIO

É sabido que a lista de crimes que são realizados por meios eletrônicos/internet é muito extensa. Porém grande parte dos operadores do direito sejam eles magistrados, advogados e consultores jurídicos entendem que os crimes digitais estão quase todos catalogados no Código Penal. Uma grande barreira que deve ser mencionada neste capítulo com relação a complexidade desse tipo penal é a ausência de uma fronteira física que demarca o mundo virtual, pois a maioria dos crimes são cometidos por computadores que estão em outros países, mas suas vítimas se encontram no Brasil.

Embora os crimes cibernéticos não sejam totalmente tipificado pelos nosso ordenamento, isto não quer dizer que quando um criminoso cometer um delito e prejudicar alguém estará totalmente impune, pois quando há ausência de alguma norma específica é utilizado a analogia, e este modo acabou se tornando muito comum nesse tipo de crime.

No final do ano de 2020 foi criado um Comitê Cibernético pelo Conselho Nacional de Justiça (CNJ) para conseguir reprimir crimes virtuais. Isso foi uma forma de pronta resposta aos ataques que o Superior Tribunal de Justiça (STJ), estava sofrendo constantemente e acabava retardando ainda mais os andamentos nos tribunais. Este comitê era formado por, membros de tribunais estaduais, pelo conselho nacional da justiça federal e Conselho Nacional de Justiça

.Diante os fatos mencionados acima, é notório que o nosso ordenamento jurídico ainda se encontra muito longe do ideal no que diz respeito as normas referente ao crimes cometidos na internet, a todo o tempo é criada novas leis e analogias de acordo com jurisprudências são feitas, mas as lacunas a serem preenchidas não acabam.

A grande quantidade de crimes está ligada principalmente a esses fatores, a falta de leis específicas e a falta de leis própria para tratar cada assunto, além das poucas normas que já existem apresentar falhas ou interpretações obscuras. E com a grande quantidade de pessoas conseguindo ter cada vez mais acesso a internet normas específicas acerca do tema se torna muito mais necessário, pois com o crescimento do número de usuários e que em muitos casos não tem total domínio da internet as pessoas estarão muito vulneráveis e se tornarem vítimas de crimes virtuais.

II.3 ESPÉCIES MAIS COMUNS DE CRIMES DIGITAIS

De acordo com a empresa Kaspersky, uma empresa Russa que trabalha com softwares para segurança na internet. Os crimes cibernéticos em sua maioria se enquadram em duas categorias principais que são: a atividade criminosa que visa computadores e a atividade criminosa que usa computadores para cometer outros crimes. Pode-se dizer que os crimes que tem como o objetivo atingir os computadores muitas vezes envolvem vírus e outros tipos de malware. Os cibercriminosos ou também conhecidos como “atacantes” podem se utilizar de vírus e malware para danificar serviços ou impedi-los de funcionar. Eles também podem excluir ou roubar dados.

Os crimes cibernéticos que usam computadores para cometer outros crimes podem envolver o uso de computadores ou redes para disseminar malware, informações ilegais ou imagens ilegais. Há de se ressaltar que uma modalidade não exclui a outra, podendo ser utilizadas ao mesmo tempo ambas para fazer um ataque criminoso de uma só vez. Temos como uma das principais modalidades os ataque de malware, phishing, ataque DDoS.

Esses tipos de condutas praticadas no computador podem ser classificados de duas formas, a saber, “crimes cibernéticos” e “ações prejudiciais atípicas”. As ações prejudiciais são condutas que são praticadas na internet que causem algum tipo de dano ou prejuízo a outrem, mas não há uma previsão legal, um exemplo disso é um indivíduo que adentra um computador de outra pessoa sem objetivo de obter ou alterar os dados ou até mesmo sem violar algum tipo de mecanismo de segurança.

Já os crimes “cibernéticos abertos” eles podem ser praticados de uma forma tradicional ou com o auxílio de um computador que serve apenas para auxiliar a atividade criminosa. Os crimes exclusivamente cibernéticos é uma conduta que é realizada exclusivamente por computadores ou com algum outro tipo de ferramenta tecnológica que tenha acesso a internet.

Os crimes que são mais comuns atualmente estão ligados ao phishing, que está condicionado na maioria dos casos ao mercado financeiro, são furtos mediante fraude. Na maioria dos casos um indivíduo recebe uma mensagem falsa e acaba clicando no arquivo e neste arquivo contém um vírus que fixa na máquina a fim de coletar dados do usuário, o dado que geralmente é acessado é a conta bancária e em seguida o criminoso tenta retirar todo o dinheiro da conta.

Capítulo III – PRINCIPAIS CONDUTAS CRIMINOSAS ATRAVÉS DO CYBERESPAÇO

III.1 Estelionato e Fraudes

Esse é uma das modalidades mais recorrentes, o Código Penal no artigo 171, define o estelionato como “obter, para si ou para outrem vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante, artifício, ardil, ou qualquer outro meio fraudulento”. Podemos ter como principal atividade estelionatária em ambiente cibernético os e-commerce (comércio virtual), apesar de facilitar a vida das pessoas com compras mais rápidas a facilidade acabou gerando espaços também para a atuação de criminosos, e ainda não há uma ferramenta que assegure proteção aos consumidores no momento da compra online.

Destarte o entendimento trazido pelo Superior Tribunal de justiça (STJ), que diz que venda fraudulenta dentro do ciberespaço configura crime de fraude, ao passo que a compra e venda revestida de fraude caracteriza estelionato.

Podemos conceituar o estelionato sob a ótica cibernética quando o criminoso induzir ou manter a vítima em erro, obtendo vantagem ilícita. Geralmente, por e-mail falso para a vítima, contendo links maliciosos que poderá redirecionar para uma página de compra, mecanismo que é utilizado para obter dados bancários.

Com relação a fraude virtual, ela ocorre quando se dá a invasão, modificação ou qualquer outra forma de adulteração em sistemas de dados. Podemos ter como exemplo, o caso da atriz Carolina Dieckmann, ela teve o computador pessoal invadido e teve suas fotos íntimas divulgada na internet.

Ambas as modalidades com o passar do tempo vem crescendo, porém a que mais se destaca é o furto mediante fraude, artigo 155 do Código Penal. Segundo Antônio de Loureiro Gil, em sua obra Fraudes Informatizadas, ele entende que as fraudes informatizadas constituem:

“Ação intencional e prejudicial a um ativo intangível causada por procedimentos e informações (software e bancos de dados), de propriedade de pessoa física, ou jurídica, com o objetivo de alcançar benefício, ou satisfação psicológica, financeira e material.”²

² GIL, Antônio de Loureiro. Fraudes Informatizadas. 2ª edição, 1ª tiragem, 2000. p. 114.

III.2 Invasão de dispositivo eletrônico e Privacidade

Esse tipo de modalidade criminosa cresceu devido a intensa e crescente quantidade de acessos a internet por todo o mundo, pois o fluxo de informações e dados, sejam eles em redes sociais ou sites, mediante cadastro, que podem ser usurpados e utilizadas indevidamente por criminosos. No Brasil foi atribuído um tipo penal a essa situação com a lei 12.737/2012 que também é conhecida como a Lei Ana Carolina Dieckmann, a doutrina mais conservadora defende-a somente com base no artigo 154-A do Código Penal, o que contempla somente a invasão.

A lei Nº 12.737/2012 gerou um grande impacto na área penal, tendo em vista o acréscimo dos artigos 154-A e 154-B, trouxe também modificações quanto as redações os artigos 266 e 298. Com essas mudanças normativas trouxe uma nova tendência do direito que é a segurança virtual, com isso os crimes que decorrem do uso indevido de informações e materiais pessoais como fotos e vídeos, dizem respeito a privacidade de uma pessoa na internet.

Há de se ressaltar que a lei “Ana Carolina Dieckmann” foi apenas um marco inicial para a proteção de dados em nosso ordenamento jurídico ter um amparo legal, mas é possível perceber que a lei ainda precisa ser elucidada para poder eliminar as incertezas de sua interpretação. Um de seus principais pontos de debate é em relação ao aspecto do texto da lei parecer essencialmente vago e carecer de aspectos técnicos. Por exemplo, não há uma certeza quanto se a invasão de seu próprio dispositivo é considerada crime, podendo gerar conflitos entre interpretações de alguns juristas, e logo gerando conflitos na resolução de lides no caso concreto. Outro problema é a lei não especificar o tipo de crime que pode ser cometido, deixando então uma margem para interpretação por parte do poder judiciário e do Ministério Público.

Independentemente da ótica de posicionamento o necessário é assegurar a proteção de dados que os internautas disponibilizam na internet, e é necessário que o estado seja capaz de resguardar esses direitos, bem como a identidade de usuários.

III.3 Crimes contra a honra

A honra como conhecemos sobre a visão objetiva, é a imagem pela qual a pessoa é vista perante a sociedade. No que diz respeito a honra subjetiva é a imagem a ser entendida como o sentimento que a pessoa possui, ou seja a sua dignidade. Em âmbito geral, a honra é composta de aspectos físicos, morais e intelectivos, aspectos que determinam se um individuo vai ou não ser respeitado por uma sociedade.

Os crimes contra a Honra se encontram nos artigos 138,139 e 140 do Código Penal. Todos eles são aplicados tanto no ambiente real quanto no ambiente virtual. Com a entrada em vigor do pacote Anticrime (Lei 13.964/19) foi criado uma causa de aumento de pena que triplicou a pena para os crimes contra a honra que foram praticados nas redes sociais, sendo este aplicável a todas as modalidades dos crimes contra a honra, sejam eles simples ou qualificados.

A calúnia esta prevista no artigo 138 do Código Penal, que diz:

"Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa".

A injúria está prevista no artigo 140 do Código Penal, que diz:

"Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa."

A difamação está prevista no artigo 139 do Código Penal, que diz:

"Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa".

Diante os fatos caracterizados acima, é de suma importância saber distinguir um tipo penal do outro, a calúnia se trata de imputar um fato criminoso a alguém, por exemplo: um individuo "A" Roubou a Loja do individuo "B" ontem. A injúria acaba sendo mais simples de ser entendida é um crime que ofende a honra subjetiva da pessoa, ou seja, ela causa um sentimento de mal estar, e abaixa a autoestima, um

exemplo muito utilizado pelas doutrinas é o caso de uma pessoa xingar a outra, exemplo: um indivíduo “A” fala que o indivíduo “B” é um golpista está cometendo o crime de injúria.

Por fim, temos a difamação que é diferente da calúnia por se tratar de imputar fato ofensivo. No caso em específico da calúnia afirma-se que categoricamente cometeu um crime. É diferente também da injúria, pois a injúria atinge a honra objetiva, que é a imagem que a pessoa tem perante a sociedade. Na difamação, o autor do crime imputa o fato ofensivo. Por exemplo: um indivíduo “A” fala que o indivíduo “B” costuma aplicar golpes na vizinhança toda quarta-feira. É uma pequena diferença, mas é de grande importância, percebe-se que na difamação não há como afirmar que João cometeu um crime, mas ele possui esse hábito. Esse tipo de imputação ofende a sua reputação. Nas três modalidades acima citadas, podem ser cometidas tanto de forma falada ou até mesmo em postagens de redes sociais.

III.4 Principais alterações que foram feitas e acrescentadas ao Código Penal pela lei 14.155/21

Entrou em vigor no dia 28 de maio de 2021, a lei que amplia as penas por crimes praticados com o uso de aparelhos eletrônicos sejam eles celulares, computadores e tablets, estejam eles conectados ou não a internet. O principal motivo dessa alteração é poder punir com maior rigor as fraudes que vem se tornando cada vez mais comum durante a pandemia do Covid-19, as alterações afetam tanto o Código Penal e o Código de Processo Penal.

Com relação ao furto, a lei criou um agravante de reclusão de 4 a 8 anos, para o furto realizado com o uso de dispositivos eletrônicos, estando eles conectados ou não a internet, podendo ser por meio de programas invasores ou por meio de violação de senhas. Se o crime for praticado contra idoso ou vulnerável, a pena pode ser aumentada de 1/3 ao dobro, dependendo do resultado da ação. E se for praticado com o uso de servidor de informática que esteja mantido fora do país, a pena pode ser aumentada de 1/3 até 2/3.

Quanto ao estelionato, a lei trouxe como qualificadora o furto qualificado por meio eletrônico houve um incremento quanto a punição, com pena de reclusão de 4 a 8 anos e multa. Esse tipo de fraude é uma das mais utilizadas e que teve um grande aumento nos últimos anos não só durante a pandemia, tem como principal objetivo

enganar a vítima para obter informações da senha ou do número da conta. A pena pode ser aumentada de 1/3 a 2/3 se o crime for praticado mediante a utilização de servidor mantido fora do país, e de 1/3 ao dobro se praticado contra idoso ou vulnerável. Sendo que atualmente o aumento é somente em dobro e apenas quanto ao idoso.

Por fim, há ainda a invasão de aparelhos o crime já é existente no Código Penal que é invadir aparelhos de informática para obter dados, a lei aumenta a pena de detenção de 3 meses a 1 ano para reclusão de 1 a 4 anos. Caso a invasão provocar a obtenção de comunicações privadas, segredos comerciais ou industriais, informações sigilosas ou o controle remoto não autorizado do dispositivo que foi invadido, a pena será de 2 a 5 anos e multa. No Código Penal atual, ela é menor, que é 6 meses a 2 anos e multa. A pena também será aumentada, 1/3 a 2/3 da pena, se houver prejuízo econômico decorrente da invasão.

CAPÍTULO IV - O CONTEXTO ATUAL DOS CRIMES CIBERNÉTICOS

IV.1 ORDENAMENTO JURÍDICO PÁTRIO ACERCA DO TEMA E A INSUFICIÊNCIA DE NORMAS ESPECÍFICAS

No que se refere ao nosso ordenamento jurídico quanto as leis específicas para tentar de alguma forma “frear” o crescimento dessa modalidade criminosa, nos últimos anos o assunto já entrou em debate diversas vezes, porém apesar de diversas leis para tentar solucionar al lides que ocorrem envolvendo crimes cibernéticos podemos notar que existem ainda diversas lacunas a ser preenchidas.

Os crimes cometidos no ciberespaço afetam a todos, sejam elas empresas (PJ), as pessoas e os negócios, isso porque a credibilidade de todos os entes envolvidos no negócio é colocada em “cheque”. A internet muitas das vezes como dito popular é conhecido como “a terra de ninguém”. Podemos observar que, em alguns casos a legislação que está vigente engloba algumas situações que ocorrem no ambiente virtual, e então é aplicada a analogia. Todavia, podemos verificar o crescimento demasiado de atividades criminosas, o que torna cada vez mais necessário uma legislação mais específica, os avanços tecnológicos nos fazem ter de fazer alterações a todo o momento em relação a essas normas e mesmo com a analogia sendo utilizada para sanar essas condutas criminosas, por vezes vemos que aquela modalidade é totalmente “sui generis”.

Apesar da Legislação não conseguir acompanhar as mudanças que ocorrem, temos um ponto positivo que é a sistemática de inquéritos. Através do inquérito eletrônico, podemos simplificar e agilizar os cumprimentos de mandado, podemos encontrar o que de fato aconteceu e facilitar a instrução probatória.

No ambiente cibernético, poder identificar quem de fato cometeu o ilícito é a maior dificuldade durante as investigações, por causa da falta de um agente físico. A principal problemática relacionada aos crimes virtuais se dá por causa do anonimato, pois nesse ambiente possibilita que crie ou transforme sua identidade. No entanto, já há maneiras como a busca de IP (Internet Protocol), que é um endereço que é dado a cada um que acessa a internet, pode ser entendida como uma “identidade” de um computador e cada um possui um diferente do outro.

IV.2 POSSÍVEIS SOLUÇÕES E OTIMIZAÇÃO

Os crimes cibernéticos ocorrem de uma forma muito acelerada com a mesma rapidez da transmissão de dados. Para melhorar esse cenário é necessário maior rapidez na expedição e cumprimento de mandatos, celeridade por parte da perícia; união entre as forças da segurança pública; e o aperfeiçoamento da legislação.

Outro método que pode ser utilizado é utilizar programas que possam aperfeiçoar os mecanismos para o combate de crimes cibernéticos, com exemplo a IA (Inteligência Artificial) e Machine Learnig (Aprendizado de máquina), alguns desses mecanismos são utilizados já no ambiente bancário para simplificar as tarefas cotidianas. Porém, não basta somente programar essas novas tecnologias, devem ser escolhidos serviços de qualidades com segurança bem forte, eficaz e bem alinhados com a necessidade do órgão que se utilizará, podendo ser bancos, empresas públicas, escolas e etc.

Com esses mecanismos podemos colher muitos benefícios que podem ser desde a otimização da identificação de ameaças, mais agilidade na investigação de alertas e na correção de ameaças. A execução da IA como um recurso de cibersegurança pode ser desde, a análise de quantidade muito grande de dados; identificar desvio de padrões; análise de sentimento em textos, direcionando os esforços dos times de prevenção e a facilidade na correlação de dados.

IV.3 PROCESSO E JULGAMENTO

Com relação a parte processual e julgamento dos crimes cibernéticos há uma complexidade muito grande para a resolução das demandas, pois há muitos aspectos que devem ser levados em consideração no momento da verificação sobre qual competência deverá ser aplicada por exemplo, como o endereço eletrônico, o lugar onde a conduta foi consumada ou teve efeitos, o domicílio da vítima, domicílio do réu. Diante isso, a legislação brasileira, considera os artigos 5º e 6º do Código Penal, que rege a competência para processar e julgar os crimes praticados no ciberespaço.

Art. 5º – Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.

Art. 6º – Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.

Percebe-se que nosso ordenamento jurídico faz uma adaptação á teoria da ubiquidade, com o que está escrito no artigo 6º do Código Penal, pois na medida em que crimes cometidos por pessoas de nacionalidade brasileira, independente de terem ocorridos ou não em território brasileiro, será aplicada a legislação brasileira.

CONCLUSÃO

Com o grande avanço da globalização e evolução dos meios de comunicação a internet ganhou muita visibilidade e se difundiu rapidamente por todo o mundo. É notório que cada vez mais nos tornamos muito dependente dela, pois com a internet conseguimos resolver diversos assuntos do nosso dia a dia, seja no âmbito pessoal ou profissional. De início a internet tinha como objetivo guardar informações do governo no período de guerra, naquele momento a internet servia como um meio teoricamente mais seguro de manter as informações do governo americano durante a Guerra Fria.

Com o passar dos anos a internet e seus conceitos foram sendo aprimorados e consequentemente foi tendo mais visibilidade por outras pessoas não só do ambiente de militares. Diante todo este contexto, surgiram muitas evoluções tanto para o lado positivo e negativo, podemos ter como um dos principais pontos positivos que a internet nos trouxe que foi a comodidade de realizar diversas tarefas sem ao menos sair de casa, no atual momento pandêmico, por exemplo, as possibilidades que ela nos trouxe para continuar seja no ambiente de trabalho ou de estudo foram muito benéficas. Por outro lado, também há alguns pontos negativos como a grande quantidade de informações pessoais que depositamos nela, seja com cartões de crédito, informações pessoais e etc. Isso atraiu muitas pessoas maliciosas que buscam roubar dados para fazer eventuais atitudes criminosas.

Embora a internet tenha trazido a diversos benefícios, esses mesmo recursos que tratamos hoje em dia como indispensáveis apresentam um grande risco ao utilizá-lo se não souber utilizá-lo corretamente, e muitos deles podem causar diversos transtornos e muitos prejuízos para as vítimas. Pode-se afirmar que o crescimento acentuado dessa modalidade criminosa pode ter ocorrido principalmente pelo aumento dos usuários, pelas vulnerabilidades existentes nas redes ou até mesmo pela falta de atenção de quem a utiliza. No decorrer do presente artigo, deverá ser levado em conta crimes cibernético como sinônimo de crimes virtuais.

Com relação a pandemia, a partir de pesquisas realizadas é possível notar que antes mesmo dela o Brasil já sóbria bastante com os crimes em ambiente virtual, pois no ano de 2019 o Brasil já se encontrava como o terceiro país do mundo que sofre mais ataques cibernéticos, perdendo apenas para os EUA e a China, fonte retirada do relatório global que foi divulgado pela Symantec.

Pode-se perceber que no ano seguinte em 2020, os ciberataques aumentaram e o Brasil sofreu mais de 3 bilhões de tentativas de ataques na internet, considerando o período de janeiro a setembro de 2020, segundo a Fortinet Threat Intelligence Insider Latin America. A Interpol nos meses de janeiro a abril conseguiu detectar mais de 907 mil ataques Spams, e 737 incidentes que estariam relacionados a softwares maliciosos (malwares). Outro dado interessante que deve ser mencionado é que em 2019 foram registradas 57.428 denúncias de janeiro a dezembro, já no ano de 2020 foram registradas um total de 156.692 denúncias durante o mesmo período isso mostra um aumento de aproximadamente de 173%.

Diante todas as questões abordadas, as facilidades para o acesso a internet fez aumentar a grande quantidade de usuários o que causou uma grande incidência dos crimes cibernéticos, e com o Brasil figurando entre os 10 países que mais utilizam a internet é notório que o nosso ordenamento jurídico não se encontra evoluído a ponto de ser capaz de solucionar totalmente esse tipo penal. Sob esse contexto os cibercriminosos se aproveitam de diversos fatores, sejam ele a falta de habilidade na web por alguns usuários e a falta de leis específicas para se beneficiarem com essa modalidade de crime. Um dos pontos mais importantes para podermos nos desenvolver seria conseguir alinhar o aparato jurídico com a evolução da sociedade e meios de comunicação, tentando de alguma forma assegurar a proteção dos direitos fundamentais do povo.

Por fim, cabe aos internautas usarem medidas preventivas individualmente, tendo em vista que a legislação que temos não é suficiente para nos proteger do ambiente cibernético, devemos sempre procurar nos informar de novas praticas delituosas para que possamos ter medidas de segurança, seja por meio de antivírus, senhas mais complexas, programas para proteção de senhas e etc.

REFERÊNCIAS:

AMBITO JURIDICO, OS CRIMES VIRTUAIS E A IMPUNIDADE REAL

.Disponível em: <<https://ambitojuridico.com.br/edicoes/revista91/oscrimesvirtuaieaimpunidadereal/>>: acesso em 29/05/2021

CÂMARA DOS DEPUTADOS, ENTRA EM VIGOR LEI QUE AUMENTA PUNIÇÕES PARA FRAUDES ELETRÔNICAS Disponível em:<<https://www.camara.leg.br/noticias/765760-entra-em-vigor-lei-que-aumenta-de-punicoes-para-fraudes-eletronicas>>: Acesso em 14/10/2021

CRYPTOID, CRESCIMENTO DE CRIMES CIBERNÉTICOS NA PANDEMIA: COMO NÃO SER UMA VÍTIMA.

Disponível em:< <https://cryptoid.com.br/identidade-digital-destaques/crescimento-de-crimes-ciberneticos-na-pandemia-como-nao-ser-uma-vitima/>>:acesso em 15/10/2021

Emerson Wendt e Higor Vinicius Nogueira Jorge, **CRIMES CIBERNÉTICOS (2A. EDIÇÃO): AMEAÇAS E PROCEDIMENTOS DE INVESTIGAÇÃO**, Brasport, 2013.

FUNDAÇÃO ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO (FMP), LEI CAROLINA DIECKMANN: VOCÊ SABE O QUE ESSA LEI REPRESENTA? Disponível em:< <https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/>>: acesso em 17/09/2021

JUSBRASIL, CRIMES CONTRA A HONRA NAS REDES SOCIAIS. Disponível em:< <https://vieiravictor.jusbrasil.com.br/artigos/834161248/crimes-contr-a-honra-nas-redes-sociais>>: acesso em 15/09/2021

LGPD APLICADA / Ana Paula Moraes Canto de Lima ... [et al.]; coordenação Ana Paula Moraes Canto de Lima, Marcelo Crespo, Patrícia Peck Pinheiro; prefácio Arthur Pereira Sabbat. – São Paulo: Atlas, 2021.

ROSA, FABRIZIO. **CRIMES DE INFORMÁTICA**. 1. ed. Campinas: Bookseller, 2002

ROVER, Tadeu. **INTERNET FACILITA CRIMES E DIFICULTA INVESTIGAÇÃO, ESTIMULANDO A IMPUNIDADE**. 2017, Disponível em: Conjur<https://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialista-crimes-virtuais>> Acesso em: 01/11/2021.

SANTOMAURO, Beatriz. **VIOLÊNCIA VIRTUAL**. Revista Nova Escola, ano XXV, n. 233, junho/julho, 2010.

SCHIAVON, Fabiana. **CRIMES ELETRÔNICOS DEIXAM RASTROS QUE AJUDAM NA PUNIÇÃO**. 2009, Disponível em: <https://www.conjur.com.br/2009-jul-25/identificar-autores-crimes-eletronicos-cada-vez-possivel>> Acesso em: 02/11/2021.

SHARIFF, Shaheen. Ciberbullying: **QUESTÕES E SOLUÇÕES PARA A ESCOLA, A SALA DE AULA E A FAMÍLIA**. Porto Alegre: Artmed, 2011.

SENADO, **LEI COM PENAS MAIS DURAS CONTRA CRIMES CIBERNÉTICOS É SANCIONADA**. Disponível em:<<https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contr-crimes-ciberneticos-e-sancionada/>>: acesso em 18/09/2021

TJDFT, **MARCO CIVIL DA INTERNET**. Disponível em:< [https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet#:~:text=O%20Marco%20Civil%20da%20Internet,da%20internet%20no%20Brasil...](https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet#:~:text=O%20Marco%20Civil%20da%20Internet,da%20internet%20no%20Brasil...>)>: acesso em 18/10/2021.