UNIVERSIDADE TIRADENTES

CURSO DE DIREITO

BRUNO LUIZ OLIVEIRA SANTOS

CRIMINALIDADE E AS NOVAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

Aracaju

2020

BRUNO LUIZ OLIVEIRA SANTOS

CRIMINALIDADE E AS NOVAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

Artigo apresentado como requisito parcial para obtenção do título de bacharel em Direito, pelo curso de Direito da Universidade Tiradentes (UNIT).

Orientador: Renato Carlos Cruz Meneses

Aprovado em___/__/__.

Banca Examinadora

_____

Professor Orientador
Universidade Tiradentes

_____

Professor Examinador
Universidade Tiradentes

_____

Professor Examinador
Universidade Tiradentes

RESUMO

O crescente número de crimes cibernéticos vem se alastrando e gerando impactos na sociedade brasileira, ou seja, crimes como: a injúria e a difamação, antes, praticadas de forma física e pessoal, hoje se repercutem de forma rápida e danosa, através da internet. Ainda que a identificação do sujeito agente seja de difícil acesso, novas medidas precisam ser tomadas para tentar minimizar tais condutas. Com isso, o presente artigo traz uma definição acerca dos crimes virtuais, assim, demonstrando o crescente número e os mecanismos utilizados para a prática ilícita dos mesmos, mencionando a insuficiência das leis do código penal nos diferentes tipos ilícitos desta mesma seara criminal. Este artigo também ressalta as mudanças obtidas através da lei 12.737/2012, além de outras medidas para combater este tipo de ilicitude e, ainda, a lei 12.965/2014, que trouxeram diversas transformações acerca dos assuntos relacionados à internet. Tais leis têm como objetivo a privacidade e a neutralidade da rede, garantindo, assim, a confiabilidade de proteção do acesso aos usuários, demonstrando, por fim, as mudanças que precisam ser feitas para combater essas ilicitudes.

Palavras-chaves: cibercrimes; internet; prática ilícita

ABSTRACT

The growing number of cyber crimes has been spreading and causing damage in Brazilian society, that is, crimes such as: an injury and defamation, previously practiced in a physical and personal way, today with repercussions in a fast and harmful way, through the Internet. Although the identification of the subject agent is difficult to access, the necessary new measures will be used to try to reduce these procedures. Thus, the present article provides a definition related to cyber crimes, thus demonstrating the increasing number and uses used for their illegal practice, referring to an insufficiency of penal code laws in the different illegal types of this same crime. This article also highlights the changes imposed by law 12.737 / 2012, in addition to other measures to combat this type of illegality and, also, a law 12.965 / 2014, which brings several changes related to Internet-related matters. Such laws

aim at the privacy and neutrality of the network, thus allowing the protection of access to users, finally demonstrating the changes that are necessary to avoid these illegality.

Keywords: cyber crimes; Internet; illicit practice

1 INTRODUÇÃO

Com a evolução da tecnologia o mundo vivencia uma difusão de recursos que facilitam a prática de atividades ilícitas. Informações que antes demoravam dias para chegarem aos seus destinos, hoje, com as transformações ocorridas, podem ser compartilhadas e apagadas em frações de segundos. Porém, por outro lado, esta mesma evolução dificulta o trabalho dos policiais, pois não se sabe ao certo de onde a informação foi compartilhada e para isso é necessário uma imensa análise.

Assim, revela-se importante a participação do direito penal na busca de soluções, já que este está longe de encontrar maneiras que possam enquadrar os sujeitos desses crimes. Ou seja, em se tratando desses assuntos, o código penal prevê a mesma punição dos crimes cometidos fisicamente para os cibernéticos, não encontrando nisso êxito, pois a materialidade da consumação não é a mesma.

O Brasil tem o objetivo de criar legislações para combater estes tipos de crimes, como a lei 12.965/14 conhecida como o marco civil da internet e a lei 12.737/12, que passou a ser chamada de “lei Carolina Dickmann”, após fotos da atriz serem expostas através da internet.

Como o foco do trabalho é apontar os mecanismos utilizados atualmente no Brasil para dar soluções mais eficazes ao combate dos cibercrimes, não serão aprofundados os estudos acerca de todas as legislações sobre o assunto.

Na linha do exposto, o presente artigo tem por objetivo analisar a cibercriminalidade, fazendo um breve apanhado histórico de sua origem. Em conjunto, revelar quais os grupos mais vulneráveis e como estas práticas se caracterizam. A demonstração da repercussão dos crimes formais e informais, mencionando, com isso, o grande aumento dos crimes cibernéticos e a dificuldade

para se obter informações, também é de suma importância, já que estes podem ser praticados a qualquer hora e lugar.

Com isso o presente artigo foi elaborado utilizando-se do método dedutivo, partindo de uma análise acerca dos impactos que a globalização causou ao direito penal, com o surgimento dos cibercrimes, demonstrando, para tanto, os meios de prevenção e as legislações aplicáveis para coibir a incidência desses crimes.

A pesquisa bibliográfica baseou-se no levantamento de artigos científicos e periódicos em acervos digitais na internet.

2- DEFINIÇÃO DE CIBERCRIMES.

O cibercrime consiste na prática de burlar a segurança de computadores, e com isso adquirir informações que se tornam relevantes para a prática de atividades ilícitas, sendo praticada de várias formas em qualquer hora e lugar, como: a falsificação, a fraude, o acesso não autorizado, a violação da propriedade intelectual, a distribuição de material pornográfico, entre outros. Independentemente de ainda não possuir legislação específica no Brasil, é possível que sejam tipificados alguns delitos no código penal vigente, para aqueles crimes que se assemelham aos praticados fisicamente, como é o caso da injúria e da difamação.

Em razão disso, já havia a existência desses crimes muito antes do surgimento da internet e dos sistemas computacionais, encontrando apenas maneiras que facilitaram a sua disseminação. Desse modo, pode-se dizer que a rede de computadores e os dispositivos de informática são apenas mais um meio para o cometimento de tais ações delitivas, não sendo necessária a utilização da esfera da informática para que elas existam, caracterizando esses crimes como impróprios. O que leva à disseminação dos cibercrimes é o modo com que eles podem ser praticados, ou seja, o uso de uma identidade falsa atenta para que essas condutas venham acontecer, uma vez que o infrator sente-se camuflado o que torna possível a prática de novos atos e assim gera um número maior de vítimas.

De acordo com a ONU, o cibercrime é uma das organizações criminosas transnacionais que mais crescem no mundo e que já afeta milhares de indivíduos em todo o mundo. Sua manifestação dá-se em diferentes formas, com transgressões relacionadas: à identidade, às violações de direitos autorais, à

pornografia infantil e aos abusos. Esta atividade ilegítima é uma das maiores ameaças para os 2 bilhões de usufrutuários da rede que, de forma escrupulosa ou não, armazenam informação online. Desta forma, até a fiscalização para conter esse tipo de propagação torna-se mais um grande desafio encontrado pelos agentes da lei, que acabam sendo impostos a barreiras tecnológicas cada vez mais avançadas. Sendo assim, países com baixos recursos, acabam tendo mais dificuldade na contenção e combate aos ataques virtuais, e por isso, contam com índices altíssimos de vítimas destas ações ilegais. Em um contexto assim, faz-se necessária a proteção cibernética de cidadãos em todo o mundo.

3- REPERCUSSÃO DOS CRIMES EM RAZÃO DA TECNOLOGIA

O acesso à internet, com o passar dos anos, está se tornando cada vez mais fácil, e muitas pessoas, até mesmo as que moram em zonas rurais, estão tendo essa garantia. Já os que não têm acesso a esses equipamentos eletrônicos, podem utilizar lugares públicos para o contato com esta ferramenta, como os cyber cafés e as *lan houses*. Estes espaços são estabelecimentos comerciais próprios para as pessoas que queiram pagar por um tempo determinado de acesso a um computador e a uma rede, estando assim ao alcance de várias pessoas e de informações.

A internet foi criada inicialmente com o objetivo de ser usada pelos militares e após a coexistência pacífica entre as duas maiores potências mundiais, EUA e URSS, através de um acordo que envolvia limitações armamentistas, passou-se a utilizar a internet nas universidades com fim educativo. A primeira troca de e-mail ocorreu em meados dos anos 70, logo depois, em meados anos 80. Quando os computadores já estavam com o poder de processamento mais avançado, houve a preocupação envolvendo o armazenamento de dados em decorrência do aumento das piratarias e das invasões de sistemas. No Brasil esses ataques cibernéticos surgiram no ano de 1996 com uma invasão ao site da universidade federal do Ceará, mas os danos maiores ocorreram em 2002. Hoje com várias inovações acerca de computadores, smartphones e tabletes, o acesso à internet está disponível, em grande massa, no mundo inteiro, surgindo assim várias práticas ilícitas em razão desses mecanismos que facilitaram a vida das pessoas. Ou seja,

hoje para fazer uma transferência bancaria ou compra na internet não é necessário sair de casa, o que deixou a população cada vez mais exposta.

Nesse sentido, o caos da nova sociedade se refletiu no surgimento da criminalidade complexa:

> "[...] estamos diante de uma transformação dos paradigmas criminológicos oriundos do positivismo. Isso quer dizer que os fenômenos criminais não podem mais ser enfocados exclusivamente do ponto de vista individual e local, pois tornaram-se fenômenos globais, sistêmicos e organizados em redes criminosas e legais que funcionam em permanente interação." (ANSELMO, 2012 apud Barboza e Gleber, 2016, p.5)

Mas com o passar dos anos esta realidade traçou novas perspectivas. Por um lado, hoje a internet pode ser usada para o bem, na busca mais célere de se obter informações necessárias, e até mesmo pela facilidade nas transações financeiras. Já por outro, o das mentes ruins, com o objetivo de atingir os cidadãos de forma ilícita, sendo este ato algo que preocupa e muito o Estado, atualmente. Além dos crimes que podem ser cometidos através da internet, têm aqueles que apresentam manifestação de maneira física, mas que acabam ganhando maior destaque com a tecnologia devido a sua rápida transmissão.

3.1 Disseminação Dos Crimes Cibernéticos

As práticas desses crimes vêm somando, a cada ano, grandes números de vítimas. Em face da modernização estes podem ser praticados em qualquer hora e lugar em questão de segundos, e na mesma proporcionalidade que são executados podem ser apagados, dificultando, com isso, o trabalho da polícia. O cibercrime é uma prática que consiste em burlar a segurança de computadores ou de redes empresariais, podendo assumir várias formas. Com tamanha versatilidade, os criminosos desenvolveram uma grande habilidade para a prática dessas transgressões, e assim, conseguem mudar a todo o instante a forma de se obter o esperado. Uma série de atividades ilícitas, como: a falsificação, a fraude, o acesso não autorizado, a violação da propriedade intelectual, a distribuição de material pornográfico, entre outros, acabam fazendo parte da variada possibilidade criminosa

dessa modalidade. Independentemente de ainda não possuir legislação específica no Brasil, alguns desses crimes por se assemelharem aos praticados fisicamente, como é o caso da injúria e da difamação, terão tipificação no código penal vigente.

O desenvolvimento tecnológico mostra-se instrumento de relevante valor para o crescimento das relações pessoais, econômicas, informacionais e, porque não se dizer também, criminosas. Em se tratando da chamada era informacional, o uso de diversos aplicativos que estão sempre conectados à rede facilitam tanto as vivências sociais quanto as vinculações relacionadas ao trabalho. O que deixa a população exposta a uma imensidão de situações e atividades que são desenvolvidas de forma mais célere através da internet, sendo possível: acompanhar em tempo real as principais notícias do mundo; realizar compras em sites; pagar contas; trabalhar em domicílio, *home Office*; pedir refeições por meio de aplicativos; conversar e interagir com pessoas localizadas em outros territórios, tudo isso feito de maneira prática, barata e rápida através da internet, porém não segura. Pois o usuário não está apenas diante de aspectos positivos, com a repercussão dos cibercrimes, muitos dados e informações ficaram desprotegidos deixando os usuários despreparados tecnicamente e assim se tornando alvos fáceis para a prática de diversos crimes, como por exemplo, a subtração dos dados pessoais e até mesmo de contas bancarias. No mundo atual, a criminalidade digital é fator crescente em consonância ao aumento no número de usuários nas redes de internet com frequente inabilidade ou negligência em seu uso. Desta forma, falhas na segurança e a expansão das infrações por diversas vias, como nos e-mails e nas redes sociais digitais, são ocasionadas.

Não se nega que muitos crimes só tiveram uma adaptação na sua forma de execução, agora utilizando a internet, em nada alterando a seleção previamente estabelecida pelo direito penal em relação às normas já tipificadas, citando-se como exemplos comuns, extorsões, crimes contra dignidade, subtração de bens e ameaças realizadas no ambiente virtual, dentre outros. (Brito, 2013 apud Rosa, 2018, p.6)

3.2 A Fragilidade No combate Aos Cibercrimes

De acordo com a ONG SaferNet Brasil em 2016 foram atendidas por chat ou e-mail 301 pessoas com essas denúncias. Em fevereiro de 2017 o STJ (superior tribunal de justiça) entendeu que o envio de fotos pornográficas de menores por e-mail era crime, chegando o assunto à corte, depois de uma decisão do tribunal de justiça do RJ, que assegurava que só existiria crime se houvesse publicação do material e não apenas a sua divulgação. Em pesquisas feitas pelo MP federal, entre os crimes cibernéticos mais praticados estão o estelionato e furtos eletrônicos, como: fraudes bancárias, invasão de dispositivos, armazenamento e publicações de imagem com pornografia infanto-juvenil, assedio e aliciamento de crianças, ameaças/*cyberbullying*, interrupção de serviços, crimes contra a propriedade intelectual e a venda ilegal de medicamentos.

Embora existam, no Brasil, vários problemas ligados à legislação, o que acaba dificultando o avanço de mecanismos que impeçam tais condutas são os problemas sociológicos, pelo fato da tecnologia ser recente e o judiciário não acompanhar tais avanços proporcionalmente. A falta de determinadas jurisprudências e, principalmente, a defasagem do código penal, dentre outros fatores, fazem com que, no Brasil, apenas sejam julgados como crimes, dessa natureza, aqueles que estiverem prescrito em lei, o que acaba dificultando a punição dos criminosos pelo fato de a nossa legislação não acompanhar tais avanços.

Em face das informações relatadas, demonstram-se as dificuldades para apuração do delito e a identificação de sua autoria, devido ao tempo que leva da consumação do crime até a fase investigativa. A fragilidade legislativa, seja ela em qual área for, acaba contribuindo para o aumento da criminalidade, sendo comum dizer que a prática de um crime digital acaba sendo mais difícil de ser punida. Tal informação leva em conta que a internet não para de crescer e, em consonância a isso, os crimes cibernéticos, também. Estão cada vez mais constantes e a situação tende a crescer pelo fato de a tecnologia dar saltos enormes o que faz com que o nosso código penal não consiga acompanhar, ou seja, para se criar uma lei demora-se anos, em exemplo disso a lei 12.787/12 que demorou 15 anos.

4- CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos se classificam de duas maneiras, crimes cibernéticos próprios e impróprios, ambos são praticados por meio da internet, mas o impróprio deriva de crimes praticados no mundo real. Crimes virtuais próprios ou puros são aqueles que o agente somente só se utiliza do computador para praticar a consumação de eventuais crimes, encontrando estes, tipificação legal nos artigos 154-A e 313-A da lei 12.737/12, que falam sobre a invasão de dispositivo informático e a inserção de dados falsos em sistema de informação, sendo o computador elemento essencial para a execução do crime. Crimes cibernéticos impróprios são aqueles que sua prática também é realizada por meio de um equipamento virtual, mas sua destinação não é atingir outro componente eletrônico, exemplo desses crimes são os delitos contidos no capítulo V do Código Penal brasileiro, como a injúria e a difamação. Sendo assim, temos os crimes cometidos com o computador e os cometidos contra o computador, isto é, contra as informações e programas nele contidos. Mas para a sua caracterização é preciso saber qual a finalidade da conduta do agente que o praticou, qual foi o meio usado, em razão de existirem crimes que necessitam de forma obrigatória do uso do computador, como é o caso dos crimes próprios. Já por outro viés, nos crimes impróprios o equipamento informático não é essencial para a configuração do tipo penal, pois pode ser realizado sem o uso deste.

5- MECANISMOS UTILIZADOS PARA A PRÁTICA

O meio virtual, o ciberespaço desde sua origem é um espaço de liberdade, sendo objeto de comunicação entre as pessoas e que de certa forma mudou o nosso mundo, não podendo o direito penal restringir esse acesso. Atualmente, novas práticas criminosas vêm acontecendo em um espaço curto de tempo e à medida que surgem equipamentos mais modernos estes acabam tornando-se vulneráveis, em razão dos criminosos manterem-se atualizados, ou seja, usam de programas para a sua anonimização e codificação. A repercussão das redes sociais torna para os *hackers* um cenário propício para a sua infiltração a grupos de *WhatsApp*, onde hoje ocorrem as maiores práticas delitivas por ser um ambiente de troca de informações pessoais. Através do uso de mecanismos fraudulentos acabam

conseguindo adentrar nos perfis dos usuários e, assim, passam a adquirir informações com as quais induzem as pessoas que têm proximidade com o usuário hackeado ao erro. Como exemplo desta modalidade, temos o pedido de transferências online que é um dos principais golpes.

Outro meio que torna fácil a prática dessas ilicitudes, são os sites de vendas através da internet, onde muitas das vendas acontecem por destinatários que se passam por outra pessoa, colocando a foto de perfil e cadastro das informações pessoais de outro indivíduo, com o objetivo de se camuflarem e assim simular a venda de um objeto. O intuito aqui é de receber a quantia referente ao produto, mas não enviá-lo ao seu destinatário. Outra atividade comum é através de uma pré-venda por sites de compra e venda, porém na hora da entrega ser feita pessoalmente, o criminoso rende a vítima e rouba seus pertences. Vários são os tipos de crimes que tem como base o acesso à rede, embora se repercutam no ambiente real, na internet os que são de maior destaque são os crimes contra a honra.

6- LEGISLAÇÃO APLICÁVEL

No Brasil antes da lei 12.737/12, a apuração de crimes virtuais tinha uma tarefa difícil, em razão da não existência de uma legislação específica, o que tornava a aplicabilidade da lei em relação aos crimes cibernéticos uma tarefa custosa, onde a maioria dos agentes que praticavam esses tipos de condutas não eram penalizados por não haver no nosso código penal legislação aplicável para determinados crime virtuais. Dessa forma, a criação da lei 12.737/12 teve como objetivo introduzir novos tipos penais referente ao mundo cibernético, buscando-se tutelar especificamente o crime de invasão a um sistema informático. Entretanto, a criação dessa lei se deu através da notícia na mídia com a divulgação de imagens íntimas da atriz Carolina Dieckmann em diversos sítios eletrônicos da rede mundial de computadores, o que causou uma grande repercussão social, gerando um campo para a edição da Lei nº. 12.737, de 30/11/2012, publicada no DOU de 03/12/2012, com *vacatio legis* de 120 (cento e vinte) dias, apelidada de “Lei Carolina Dieckmann”, que, dentre outras providências, dispôs sobre a tipificação criminal dos

delitos informáticos, introduzindo os Arts. 154-A, 154-B, e alterando os Arts. 266 e 298, todos do Código Penal.

O tipo penal de “Invasão de Dispositivo Informático”, previsto no art. 154-A do Código Penal, introduzido pelo art. 2º da Lei 12.737, de 30 de novembro de 2012, descreve como conduta ilícita:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com 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.

Em relação aos crimes cometidos de acordo com o art. 154-A, a pena de detenção é de 3 meses a um ano e multa, havendo, entretanto, a previsão das formas qualificadas e causas de aumento de pena, resguardando o bem jurídico tutelado em relação a liberdade individual, a privacidade e a intimidade das pessoas, como um todo. Sendo este crime configurado comum, o sujeito ativo pode ser qualquer pessoa. De certa forma esta mesma menção se dá para os sujeitos passivos, ou seja, todos nós estamos sujeitos a sofrer qualquer um destes tipos de danos, seja ele moral ou material.

Quanto à culpabilidade esta se caracteriza somente pelo dolo, não havendo a previsão legal na forma culposa, estando a consumação e tentativa do crime previstas no caput do art. 154-A, que se consuma apenas com a simples invasão ou instalação de vulnerabilidade, não sendo importante para a consumação a vantagem ilícita ou não por parte do agente. Já na forma qualificada (art. 154, § 3º, do CP), referida abaixo, o crime é material, pois exige para a consumação a obtenção efetiva de conteúdo.

O art. 154-A, § 1º, do CP, prevê a equiparação do crime cibernético, acusando o agente com a mesma pena do “caput” ao modo de quem “produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput”, sendo tipificado também como um crime de ação múltipla que exige dolo específico, tal qual o caput do art. 154-A do CP.

O art. 154-A, § 2º, do CP antecipa a causa de aumento de pena de um sexto a um terço, no caso de prejuízo ligado ao caráter econômico/financeiro da vítima, sendo aplicável o aumento de pena somente para os delitos de forma simples, e não para os de forma qualificada, prevista no parágrafo seguinte, em razão da topografia do dispositivo em comento.

O art. 154-A, § 3º, do CP prediz a pena e regime prisional diferenciado (seis meses a dois anos de reclusão e multa) para as seguintes hipóteses: 1) quando a invasão possibilitar a obtenção de conteúdo de comunicações eletrônicas privadas; 2) quando for obtido conteúdo de segredos comerciais ou industriais; 3) quando proporcionar a obtenção de informações sigilosas, assim definidas em lei; e 4) quando proporcionar o acesso não autorizado do controle remoto de dispositivo invadido. Destaca-se por tanto que as figuras acima qualificadas e descritas configuram crime subsidiário de forma expressa, pois é previsto que as normas somente serão aplicadas “se a conduta não constitui crime mais grave”.

Por fim, os parágrafos 4º e 5º, I a IV, do CP, antecipam as causas de aumento de pena, aplicando somente na forma qualificada do delito o § 3º, do art. 154-A, do CP.

A lei 12.965/14 também conhecida como Marco civil da internet, traz a definição para internet como sendo está um sistema constituído de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre redes por diferentes terminais (Art. 5°, I). O próprio texto da lei prevê uma argumentação feita através da plataforma digital, em que após as discussões feitas pela população em âmbito nacional, haverá um decreto presidencial para tratar dos casos que passaram a surgir

O marco civil da internet é uma legislação de 2014 que teve como objetivo trazer algumas transformações acerca dos assuntos relacionados à internet, e dentre as principais inovações está a preservação e a privacidade dos usuários da internet, bem como, a regulação em relação a garantia da liberdade de expressão na utilização da rede mundial e a chamada: neutralidade da rede. Sendo hoje um instituto com grande discussão, pois antes da referida lei quando se acessava a diferentes tipos de páginas na internet os provedores decodificavam as informações e geravam um direcionamento às publicidades que envolviam o assunto pesquisado. Como consequência, tal ação ocasionava o envio destes anúncios às páginas de e-

mail, e das redes sociais. Mas com o surgimento da lei 12.965/14 estes anúncios só serão enviados desde que aja manifestação do sujeito passivo.

Quanto à neutralidade de rede, hoje esta se refere tanto à privacidade dos usuários, quanto aos dados que estão circulando na rede mundial, sendo assim, não pode o provedor, nem quem está usando a internet, fazer distinção dos dados que estão circulando. Ou seja, pouco importa a origem, o conteúdo, o fim ou o serviço que está sendo prestado, sendo está uma novidade em relação aos dados pessoais que estão protegidos na internet através da garantia de privacidade. Seu sigilo quando quebrado será analisado por um juiz que vai verificar o procedimento e autorizar a quebra desses dados. Mas nos casos em que a intimidade pessoal for lesada, como no caso de fotos íntimas, pode a vitima procurar diretamente o site ou o serviço que hospeda a sua imagem e requerer a retirada.

Em relação à liberdade de expressão, a nova lei garante, no ambiente da rede mundial, a mesma garantia que se tem em qualquer meio de comunicação tradicional, sendo a internet um meio democrático e livre, embora todos possam se manifestar, haverá limitações em relação à privacidade que deverá ser preservada.

Nos últimos dias, o celular do atual presidente da república foi invadido por um grupo de *hackers* de nome *Anonymous*. O grupo vazou criminosamente supostos dados pessoais do presidente, de seus filhos, de ministros, de empresários e de políticos bolsonoristas. No vazamento, dados cadastrais como telefones pessoais foram subtraídos, além de atingirem informações acerca de supostos patrimônios.

Em razão do exposto, O Ministério da Mulher, da Família e dos Direitos Humanos escreveu nota de repúdio à divulgação repudia a divulgação delituosa de dados, em claro atentado aos direitos fundamentais à intimidade, à vida privada, à honra e à imagem. A nota diz, ainda, que as dissensões ideológicas jamais deveriam ser motivação para a prática de ação despótica e antidemocrática como esta. Falou também, que os responsáveis devem ser devidamente identificados e processados, nos termos da lei.

A legislação brasileira deixa espaço para qualquer pessoa acessar diferentes tipos de sites, sem analisar idade ou perfil real dos cidadãos. Afinal, em relação a esses crimes, não se pode quebrar o sigilo das contas utilizadas já que houve decisões acerca deste assunto:

“Ementa: HABEAS CORPUS SUBSTITUTIVO DE RECURSO PRÓPRIO. NÃO CONHECIMENTO. CRIMES CIBERNÉTICOS ASSOCIADOS A FRAUDES BANCÁRIAS E INVASÃO DO APLICATIVO TELEGRAM. VINCULADO A AUTORIDADES PÚBLICAS. PRISÃO PREVENTIVA. GARANTIA DA ORDEM PÚBLICA. MODUS OPERANDI. GRAVIDADE CONCRETA DO CRIME. PRESENTESOS REQUISITOS. FUNDAMENTAÇÃO IDÔNEA. CONSTRANGIMENTO ILEGAL NÃO CONFIGURADO.

O habeas corpus não merece ser conhecido, uma vez que impetrado contra acórdão que denegou ordem de habeas corpus, em indevida substituição ao recurso ordinário próprio, o que vem sendo rechaçado pelos Tribunais Superiores. - Trata-se da Operação *Spoofing*, que visa a apurar condutas praticadas por organização criminosa responsável pelas invasões na conta do aplicativo *Telegram*, vinculada a diversas autoridades públicas, com indícios de materialidade e autoria dos crimes previstos no art. 154-A e 171 do Código Penal; art. 10 da Lei 9.296/96, além do previsto no art. 13, parágrafo único, inciso I. da Lei 7.170 e art. 1º da Lei 9.613/98. - A prisão cautelar foi fundamentada em elementos concretos, uma vez que foi decretada a prisão preventiva do paciente por fazer parte de uma estruturada organização criminosa e com divisão de tarefas, especializada na prática de crimes cibernéticos. - Evidenciada a gravidade em concreto das condutas de "hackeamento" de aparelhos telefônicos de autoridades públicas, com o propósito de subtrair informações, uma vez que se tem noticia da invasão de celulares das autoridades de maior escalão dos Poderes da República Federativa do Brasil, em que a divulgação de informações sensíveis é apta a colocar em risco a segurança nacional e a estabilidade do país como um todo. - O Colendo Supremo Tribunal Federal possui o entendimento firme de que: "A necessidade de se interromper ou diminuir a atuação de integrantes de organização criminosa enquadra-se no conceito de garantia da ordem pública, constituindo fundamentação cautelar idônea e suficiente para a prisão preventiva" (HC n. 95.024/SP, Primeira Turma, Rela. Ministra Cármen Lúcia, DJe de 20/2/2009), o que se aplica à presente hipótese. - Parecer pelo não conhecimento do habeas corpus. É o relatório. Decido. Consoante informações prestadas pelo juízo de origem, a prisão preventiva do paciente foi revogada em 19/12/2019. Confira-se (e-STJ fl. 218, grifei): Posteriormente, GUSTAVO HENRIQUE ELIAS SANTOS celebrou termo de colaboração premiada

com o Ministério Público Federal e a Polícia Federal, homologada pelo Juiz Titular desta 10ª Vara Federal, em 19/12/2019, ocasião cm que foi revogada sua prisão preventiva, mediante o cumprimento de medidas cautelares diversas da prisão. Ante o exposto, com fundamento no art. 34, XX, do RISTJ, julgo prejudicado o presente habeas corpus. Intimem-se. Brasília (DF), 26 de fevereiro de 2020. Ministro REYNALDO SOARES DA FONSECA Relator

(STJ - HC: 540307 DF 2019/0312263-2, Relator: Ministro REYNALDO SOARES DA FONSECA, Data de Publicação: DJ 28/02/2020)

Nos últimos meses em razão do período de isolamento social a incidência de golpes na internet vem crescendo, pelo fato de que as pessoas estão usando cada vez mais as redes sociais. Em uma avaliação feita pela coordenadoria de análise e estatística criminal da Secretaria de Segurança do Estado de Sergipe, foi registrado um aumento de 63,6% nos registros de crimes de estelionato através da internet, no período entre os dias 21 de março e 17 de abril, em comparação ao mesmo período no ano passado.

CONSIDERAÇOES FINAIS

Se pensando na tecnologia, pela forma que as atividades ilícitas vêm se desenvolvendo a legislação brasileira não consegue acompanhar as mudanças ocorridas nos últimos anos pelo fato de que a internet se tornou uma ferramenta imprescindível nos dias de hoje, pois é indispensável para o mercado de negócios e da comunicação.

Com o surgimento das novas tecnologias, novas ameaças passaram a surgir, como: a negociação de serviços fictícios, o roubo de informações e outros tipos de ataque. Por tal motivo surge a necessidade de se realizar investigações mais detalhadas acerca dos diferentes tipos de crimes, com o intuito de encontrar respostas para combater estas ilicitudes.

Acerca dos problemas cibernéticos no Brasil, para uma melhor cooperação se faz necessário a aderência a convenção de Budapeste, uma vez que permitirá uma

harmonização entre as legislações e assim conseguir maior eficácia ao combate dos cibercrimes.

De acordo com a SaferNet, no Brasil, dos 27 estados, apenas 15 têm delegacias especializadas no combate aos cibercrimes o que torna a investigação e a busca de infratores uma tarefa difícil. O sistema brasileiro deve melhorar neste aspecto e, assim, criar leis que consigam acompanhar a interpretação deste tipo de crime pelo julgador.

Nesse sentido, com base no estudo apresentado, demonstra-se necessária a criação de novos centros especializados, na redução da criminalidade digital, por parte do estado, com o objetivo de estudar novas técnicas para aprimorar os órgãos públicos e, assim, tornar possível a implementação de políticas públicas com a finalidade de conscientizar e alertar o povo sobre os riscos, além de elaborar uma legislação que aborde estes tipos criminais de forma clara e objetiva.

REFERÊNCIAS BIBLÍOGRAFICAS

ALVES, Matheus de A. **Crimes digitais**: análise da criminalidade digital sob a perspectiva do direito processual penal e do instituto da prova. 2018. 97f. Dissertação (Pós-Graduação *stricto sensu* em Direito) - Faculdade de Ciências Humanas, Sociais e da Saúde, Universidade FUMEC, Belo Horizonte.

BARBOSA, A. S. Os crimes cibernéticos e a Lei nº 12.737/2012 (“Lei Carolina Dieckmann”). Disponível em: <https://jus.com.br/artigos/35796/os-crimes-ciberneticos-e-a-lei-n-12-737-2012-lei-carolina-dieckmann>. Acesso em: 20 maio de 2020

SILVA, K. B; CAVALCANTI, G. H. L. Criminalidade na era da informação: definições sobre criminalidade complexa. **Revista de Direito, Governança e Novas Tecnologias**. Curitiba, v. 2, n. 2, p. 75-93, Jul/Dez, 2016.

BRITO, Auriney. Direito Penal Informático. São Paulo: Saraiva, 2013.

FILGUEIRAS, Isadora. C. A; LIMA, Thais. S. Cibercrime. In: ETIC, 2015, Presidente Prudente. **Anais do Encontro Toledo de Iniciação Científica Prof. Dr. Sebastião**

Jorge Chammé. Intertemas Toledo Prudente, Presidente Prudente, v. 11, n. 11, 2015.

SILVA, Ana Laura R. **Cibercrimes**: uma análise sob a perspectiva da aplicação do direito internacional. 30f. UFU, Minas Geras. 2019.

ANTONELLI, Humberto Lídio; ALMEIDA, Emerson Gervásio. A Internet e o Direito: uma abordagem sobre cibercrimes. In: ENACOMP, 2011, Catalão – GO, **IX Encontro Anual de Computação**. ENACOMP, Catalão, 2011

ROSA, F. A. Crimes digitais: uma necessária releitura do direito penal à luz das novas tecnologias. **Interdisciplinary Scientific Journal**. Campos dos Goytacazes, v. 5, n. 5, p.199-220, dez, 2018.

Grupo de hackers vaza em rede social supostos dados pessoais de Bolsonaro, filhos e ministros, **G1,** Brasília, 02 de jun. de 2020. Disponível em: https://g1.globo.com/politica/noticia/2020/06/02/grupo-de-hackers-vaza-em-rede-social-supostos-dados-pessoais-de-bolsonaro-filhos-e-apoiadores.ghtml. Acesso em: 03 de junho 2020.

Período de isolamento social gera aumento de 63,6% na incidência de golpes na internet em Sergipe, **G1,** Sergipe, 14 de maio de 2020. Disponível em: https://g1.globo.com/se/sergipe/noticia/2020/05/14/periodo-de-isolamento-social-registra-alta-de-636percent-na-incidencia-de-golpes-na-internet-em-sergipe.ghtml. Acesso em: 03 de junho 2020.

BARRETO, Erick Teixeira. Crimes cibernéticos sob a égide da Lei 12.737/2012. **Revista Âmbito Jurídico**, São Paulo, revista nº 159, Abril, 2017.

Tribunal. S. J. Superior Tribunal de Justiça STJ - HABEAS CORPUS: HC 540307 DF 2019/0312263-2. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/815568442/habeas-corpus-hc-540307-df-2019-0312263-2?ref=serp. Acesso em: 02 junho de 2020.