CRIMES VIRTUAIS: O DESAFIO DO CÓDIGO PENAL NA ATUALIDADE E A IMPUNIDADE DOS AGENTES

Mário Vinicius de Azevedo NUNES [1]
Fernanda de Matos Lima MADRID [2]

RESUMO: O presente artigo tem como objetivo realizar uma análise a respeito do Direito Digital, com foco no aprofundamento do tema relacionado aos crimes na internet, vez que existiu modificações paradigmáticas na coletividade contemporânea em bem da globalização e dos avanços tecnológicos, especialmente no mundo da comunicação que evolucionou assustadoramente com o surgimento da rede mundial de computadores. Em decorrência disso a internet tornou-se um novo meio para a prática de diversos tipos de crimes que já eram praticados contra a sociedade, mas por outros meios. Esses novos meios estão sendo discutidos pois a nossa legislação atual não possui regulamentação para tais tipos de delitos, assim como a dificuldade para controlar esses delitos. O legislador pretendendo adaptar a nossa legislação aos novos avanços tecnológicos, editou a Lei nº 12.737/2012 que permitiu avanços no combate aos crimes virtuais. O foco principal deste artigo será tratar do crime estelionato e sequestro de dados, que vem acontecendo cada vez mais com muitas pessoas na nossa sociedade.

Palavras-chave: Direito Penal, Direito Digital, Crimes Virtuais, Estelionato, Sequestro de dados.

1 INTRODUÇÃO

O artigo a seguir exposto abordou o tema dos crimes praticados pela internet com enfoco especial no crime de estelionato e sequestro de dados. Abordando dados históricos sobre a respeito do surgimento da internet e o desenvolvimento de toda essa tecnologia.

Com todo esse avanço e o surgimento de novos dispositivos que facilitam ainda mais o acesso à internet, como por exemplo, os dispositivos móveis.

[1] Discente do 4º ano do curso de Direito do Centro Universitário "Antônio Eufrásio de Toledo" de Presidente Prudente. marionunes_azevedo@hotmail.com.
[2] Doutoranda pela Universidade estadual do Norte do Paraná – UENP. Mestre em Ciências Jurídicas pela Universidade Estadual do Norte do Paraná – UENP. Especialista em Direito Penal e Processo Penal pela Universidade Estadual de Londrina. Graduada em Direito pelas Faculdades Integradas '' Antônio Eufrásio de Toledo'' de Presidente Prudente. Professora de Direito Penal '' Centro Universitário Toledo'' de Presidente Prudente. Advogada Criminalista.fm.com@ig.com.br. Orientadora do Trabalho.

Consequentemente, a vulnerabilidade das informações de todas as pessoas que se utilizam de dispositivos eletrônicos para acessar a rede mundial de computadores com o objetivo de se utilizar das redes sociais, sites, ou até mesmo trabalhar, desenvolveu se dispositivos que facilitam o manejo de informações, e está buscando cada vez mais facilitar a vida da sociedade em geral.

O Estelionato já existia antes do surgimento da internet, segundo a nossa legislação e Estelionato é capitulado como crime contra o patrimônio.

A internet facilitou o acesso à informação e consequentemente a obtenção de informações, que atualmente são usadas para cometer delitos.

Ao longo do artigo, serão estudados: a origem da rede mundial de computadores, o crime de estelionato e sequestro de dados, a dificuldade na apuração da autoria e do momento e local da consumação, e os meios de prova e apuração do crime.

Toda a pesquisa e a metodologia foram embasadas em doutrinas a respeito do tema abordado, também foi levado com considerações artigos e pesquisas já existentes sobre o tema.

2 A ORIGEM DA REDE MUNDIAL DE COMPUTADORES E DADOS

Durante a Guerra fria o governo norte americano precisava que seus computadores trocassem informações para que facilitar o funcionamento das bases militares, o governo então desenvolveu um sistema que ligava dos computadores da base militar, e que funcionava de maneira segura.

Nas palavras de CASTELS (2001, p. 13,14):

> As origens da Internet podem ser encontradas na Arpanet, uma rede de computadores montada pela Advanced Research Projects Agency (ARPA) em setembro de 1969. A ARPA foi formada em 1958 pelo Departamento de Defesa dos Estados Unidos com a missão de mobilizar recursos de pesquisa, particularmente do mundo universitário, com o objetivo de alcançar superioridade tecnológica militar em relação à União Soviética na esteira do lançamento do primeiro Sputnik em 1957. A Arpanet não passava de um pequeno programa que surgiu de um dos departamentos da ARPA, o Information Processing Techniques Office (IPTO), fundado em 1962.

O projeto iniciado teve o nome de ARPANET, com existo o projeto se estendeu a área de pesquisas científicas para as universalidades.

O fluxo de informações aumentou demais, foi então que nessa época o governo dividiu a rede destinada aos militares das demais redes destinadas as universais.

O serviço militar utilizava o grupo chamado MILNET, somente para atividades militares, e os demais se utilizavam da ARPANET, que servia para atividades não militares.

Foi assim que se deu início a comunicação entre as pessoas físicas e jurídicas para facilitar o comercio por todo o mundo de maneiras mais fácil e rápida, interligados pelo Protocolo de internet.

Antigamente o uso da internet era restrito a casa das pessoas, a internet era utilizada de forma discada, em decorrência dos avanços tecnológicos a internet e os dispositivos ficaram bem melhores, permitindo o uso de maneira remota, como por exemplo os celulares, notebooks e tablets na atualidade.

De acordo com Comer (2016, p. 3):

> As redes de computadores têm crescido explosivamente. A partir dos anos 1970, a Comunicação via computador transformou-se em uma parte essencial de nossa infraestrutura. A ligação de computadores em rede é usada em cada aspecto dos negócios, incluindo propaganda, produção, transporte, planejamento, faturamento e contabilidade. Consequentemente, a maioria das corporações tem múltiplas redes. As instituições de ensino, em todos os níveis, do ensino fundamental à pós-graduação, estão utilizando redes de computadores para fornecer a estudantes e professores o acesso instantâneo a informações em bibliotecas online em todo o mundo. Órgãos governamentais em níveis federal, estadual e municipal utilizam redes, assim como as organizações militares. Em resumo, as redes de computadores estão em toda parte. O crescimento contínuo da Internet global é um dos fenômenos mais interessantes e empolgantes em redes. Em 1980, a Internet era um projeto de pesquisa que envolvia algumas dezenas de sites. Hoje, ela cresceu e se tornou um sistema de munição produtivo que alcança milhões de pessoas em todos os países povoados do mundo. Muitos usuários já tem acesso à Internet de alta velocidade por meio das conexões a cabo (cable modem), DSL, fibra óptica e tecnologias sem fio.

A internet se torna mais eficaz a cada dia que passa, o seu desenvolvimento colaborou para todas a áreas em geral, e o acesso está cada vez

mais fácil para todas as pessoas, pois todos nós temos o direito a internet que a nossa CF garante a todas as pessoas.

O rápido desenvolvimento, entretanto, se tornou um perigo para as leis, pois elas não se desenvolvem de maneira rápida igual a internet.

3 A CRIMINALIDADE DENTRO DA REDE MUNDIAL DE COMPUTADORES

A nossa CF traz a internet como direito fundamental de todas a pessoas e esta prevista no seu artigo 7º da lei 12.965 de abril de 2014.

De acordo com este dispositivo, este artigo apresenta o Rol de direitos dos usuários de Internet no Brasil, expondo que o acesso à internet passa a ser condição para a cidadania; que a proteção a intimidade e à vida privada, que também é prevista no artigo 5, inciso X da CF de 1988, é cabível de indenização por dano moral ou material decorrente da violação da mesma.

De acordo com a Lei nº 12.965/2014 - Marco Civil da Internet de 23 de abril de 2014 (2016, p. 1975):

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - Inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - Inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> IV - Não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
> V - Manutenção da qualidade contratada da conexão à internet;
> VI - Informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

Embora o acesso seja para todas as pessoas, nem todas elas utilizam a internet de maneira segura e bem-intencionadas, ao mesmo tempo que existem pessoas que se utilizam da internet para realizar trabalhos, estudos, comercio etc.

Também existem pessoas que perdem o seu tempo procurando vulnerabilidades na rede, ou até mesmo através de softwares maliciosos buscando maneiras de invadir os dispositivos de pessoas inocentes e realizar o furto de dados,

com a intenção de obter vantagem sobre esta pessoa, e mediante ameaça o hacker tenta obter dinheiro da pessoa para devolver os dados que foram furtados.

De acordo com o livro Direito e Internet: Liberdade de Informação, Privacidade e Responsabilidade Civil, 7ª edição. Existem dois tipos de hackers, são chamados de hackers éticos e hackers não éticos.

Nas Palavras de Paesani (2000, p. 22). O hacker ético:

> São especialistas, os denominados hackers éticos, que invadem sistemas, corrigem falhas de segurança e instalam uma porta única e controlada, com o propósito de garantir a exclusividade no acesso. Alguns arriscam falar sobre suas proezas, mas a maioria prefere a segurança do anonimato. Normalmente, um hacker entra num computador e sai sem ser percebido. Nem sempre está mal-intencionado, mas utiliza seus conhecimentos, para obter mais conhecimentos e avisa que ainda vai demorar muito até que as transações eletrônicas sejam totalmente seguras. Cita como exemplo uma companhia cujo site recebe pedidos por meio de uma conexão criptografada na Internet e então os envia para seu centro de processamento via e-mail. A primeira etapa é segura. A segunda, não. As mensagens eletrônicas corporativas são uma das primeiras coisas que um invasor procura. A maior preocupação do chamado hacker ético é com a implantação do sistema de segurança e sua tarefa é a de tentar invadir os sistemas das companhias com o objetivo de detectar os pontos vulneráveis à ação de outros hackers. Trabalha para gigantes do ramo dos computadores e para empresas que precisam defender informações confidenciais de seus clientes.

Conforme o entendimento do autor o hacker ético se utiliza de sua inteligência e conhecimento avançado em computação para ajudar as pessoas. Ele cria maneiras de evitar que as pessoas sejam prejudicadas por hackers mal-intencionados, eles trabalham para solucionar os problemas e ajuda a evitar problemas na nossa rede mundial de computadores.

Nas Palavras de Paesani (2000, p. 23) O Hacker não ético:

> O hacker não ético (cracker) é o invasor destrutivo que tenta invadir na surdina os portões de entrada dos servidores Internet, que são a melhor forma de disseminar informações. É forçoso admitir que até o momento são os grandes vitoriosos nessa batalha informática. No Brasil, um exemplo de invasão agressiva ocorreu no dia 6 de junho de 1999, quando as páginas da Presidência na Internet foram invadidas por hackers e os textos com ataques ao governo também ocuparam o site do Supremo Tribunal Federal. No mesmo dia, houve uma tentativa frustrada de entrar no site da Secretaria da Receita Federal. Conforme comunicado do Computer Security Institute (CSI), os prejuízos financeiros atribuídos a crimes de computador podem ultrapassar US$ 10 bilhões por ano, em parte por causa da crescente expansão da Internet. Especialistas dizem que os crimes de computador ocorrem o tempo todo. A causa deve-se ao fato de os hackers terem desenvolvido programas automatizados que investigam os alvos a serem atingidos, como computadores conectados a uma rede pública, em busca de pontos vulneráveis. A proliferação de conexões de alta velocidade à Internet, por linhas telefônicas ou modems a cabo permanentemente conectados, aumentou muito o número de alvos disponíveis. Portanto, qualquer PC que não tenha um sistema de segurança, como o firewall, corretamente configurado será acessível a hackers sempre que o

> computador estiver ligado. O rápido desenvolvimento de novas tecnologias para a Internet também abre canais para o cibercrime, e é impossível para qualquer grupo corporativo de segurança manter-se atualizado em relação a essas mudanças, com possibilidade de até 75% dos servidores da Web se tornarem vulneráveis a ataques por hackers.

O hacker não ético tem o objetivo de causar mal as pessoas se utilizando do amplo conhecimento que ele possui na área de informática, para realizar sequestro de dados, retirar dinheiro das pessoas, fazer ameaças e até mesmo roubar dados e expor na internet, com o simples objetivo de fazer a sociedade.

No tópico a seguir iremos tratar do crime de estelionato e sequestro de dados que é uma modalidade muito utilizada pelos hackers para conseguir ganhar dinheiro de pessoas inocentes.

4 CRIME DE ESTELIONATO E O SEQUESTRO DE DADOS

O crime de estelionato está disciplinado no nosso ordenamento jurídico no CP Artigo 171, que diz o seguinte: 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.

Consiste basicamente em obter uma vantagem considerada ilícita que traz prejuízo a algum individuo, mediante algum meio fraudulento e induzindo a pessoa a errar de maneira proposital.

O estelionatário usa essa vantagem para forçar essa pessoa a oferecer determinada coisa de seu interesse, o mais comum a ser pedido é dinheiro em troca.

Com o surgimento da internet ficou totalmente mais fácil para quem tem conhecimento técnico na área e está mal-intencionado e quer obter vantagem (informação, dados, fotos, vídeos etc.), de pessoas que estão vulneráveis nada rede. Neste caso vamos tratar do estelionato com foco maior no sequestro de dados.

O sequestro de dados já é conhecido pelas autoridades de todos os países, tais ataques estão voltando a aumentar, trazendo muitas vítimas.

O meio utilizado para fazer essas vítimas é a utilização de Ransomwares que são códigos maliciosos que empregados para criptografar

qualquer tipo de dados da vítima. É exigido em troca dos dados um pagamento de um resgate. O resgate normalmente é pago em criptomoedas, que são mais conhecidas como bitcoins, e isso é um grande problema, porque os bitcoins são moedas arrastráveis, portanto não é possível saber para onde o dinheiro foi, deixando impossível a identificação do estelionatário.

De acordo com o livro de Ulrich (2017, p. 27), os bitcoins podem ser utilizados para lavar dinheiro sujo.

> Outra preocupação é que o Bitcoin seja usado para a lavagem de dinheiro para o financiamento do terrorismo e tráfico de produtos ilegais. Apesar de essas inquietações serem, neste momento, mais teóricas do que empíricas, o Bitcoin poderia de fato ser uma opção àqueles que desejam mover dinheiro sujo discretamente. Preocupações com o potencial de o Bitcoin ser usado para lavagem de dinheiro foram atiçadas após o Liberty Reserve, um serviço privado e centralizado de moeda digital com sede na Costa Rica, ter sido encerrado pelas autoridades sob alegações de lavagem de dinheiro.

Portanto este meio de pagamento do Estelionato é sempre utilizado para que os estelionatários saiam impunes do crime.

Existem inúmeras versões deste Ransomware que tem o nome de FBI MoneyPak ou o vírus FBI os hackers se utilizam deste logo para dar mais credibilidade a estes golpes.

Atualmente surgiu um novo Ransomware que foi apelidado de Wannacry já fez inúmeras vítimas em todo o mundo, criptografando os arquivos dos dispositivos de muitos usuários, ele surgiu através de uma falha que foi explorada no sistema operacional do Windows.

5 MEIOS DE PROTEÇÃO CONTRA OS CRIMES

O meio tradicional para evitar esse tipo de invasão é utilização de Antivírus em todos os tipos de dispositivos para que evite o sequestro dos dados. No caso de grandes empresas, elas devem contar com profissionais da área de TI especializados em segurança para que ajudem na proteção dos dados.

O acesso a sites maliciosos pode comprometer a segurança do dispositivo, tentando fazer o download de programas sem que o usuário saiba.

Devemos tomar cuidado com E-mail, que quase sempre é a porta de entrada para os Ransomwares, e até mesmo outros tipos de vírus que podem afetar

os dispositivos. Os arquivos maliciosos sempre vêm em anexo nos e-mails. Devemos também tomar cuidado com arquivos executáveis que podem ser enviados através dos e-mails, que podem vir nas extensões como: zip, Dll, Pif, Js, Exe, entre outros.

Para manter se seguro, é importante realizar backups dos arquivos importantes, para que não venha ocorra o perigo de perder os dados.

Em alguns órgãos públicos como os cartórios já é obrigatório a utilização de diversos meios para se proteger dos ataques contra a Serventia, tal exigência esta positivada no Provimento CNJ 74/2018, que trouxeram os padrões mínimos de segurança dos cartórios, estabelecendo exigências mínimas de T.I. para garantir a segurança, integridade e disponibilidade dos dados, e para a continuidade da atividade pelos serviços notariais e de registro.

De acordo com SILVA (1995, p.55)

> a) Software, dados e informações.
> Exigências de proteção para software, dados e informações estão baseadas na necessidade de preservar a confidência, integridade e disponibilidade. A confidência pode ser requerida, porque o sistema contém dados pessoais, informações de uma organização ou até dados relacionados a segurança nacional. A integridade de dados é exigência de todo sistema de computador. Usuários do sistema exigem garantias de que mudanças sem autorização, deliberada ou acidentalmente, não aconteçam. A preocupação da disponibilidade é importante a curto e em longo prazo.
> b) Serviços de processamento de dados.
> Serviço de processamento pode ser o recurso mais importante para requerer proteção em casos onde a segurança nacional, a segurança ou sustento de cidadãos individuais ou serviços essenciais, são dependentes dos sistemas de computador, p.ex., controle de tráfego aéreo, informações policiais, sistemas de monitoramento médico, fundos eletrônicos de transferência, etc.
> c) Equipamento de processamento de dados eletrônicos e instalação
> Esta categoria envolve a propriedade tangível. O próprio computador e materiais, as instalações físicas, bibliotecas de mídia, áreas de preparação de dados e áreas terminais, como também os serviços ambientais.

Existem três classificações que estão relacionadas a segurança na internet.

Trata da utilização de senhas e forma de autenticação para limitar o uso de softwares, dados e informações, se você controlar o acesso já dificulta e reduz o número de pessoas que teriam acesso a tais informações, podendo reduzir muito a chance de ocorrer o crime.

Também é importante o armazenamento das senhas, as mesmas não devem ser anotadas e qualquer lugar, portanto, não adianta nada se proteger com

uma senha se o acesso a senha estiver relativamente fácil ao alcance que quem quer realizar o ato ilícito.

Também existem formas de se denunciar estes abusos na internet, em sites como a SaferNet Brasil que é uma entidade que trabalha com o Ministério Público Federal. Eles recebem denúncias anônimas de vítimas dos crimes virtuais, a denúncia é feita de maneira fácil. Se for provada que a denuncia é pertinente será solicitado ao provedor que retire o conteúdo do ar o mais rápido possível.

6 SUJEITOS ATIVOS DO DELITO

Usuários Normais: Existem vários tipos de sujeitos ativos nestes crimes, podendo ser o usuário, que incide em erro e acaba praticando algum tipo de conduta ilícita na Internet, geralmente ocorre em redes sociais aonde os usuários expõem fotos intimas de alguém, ou ate mesmo cria perfil falso ‘’fake’’ na internet para se passarem por alguma pessoa, podendo difamar e sujar a imagem de alguém.

A maioria dos que utilizam a internet são os usuários normais, que estão limitados, detém somente conhecimentos básicos da rede, são pessoas que usam para trabalhar de forma normal no seu dia a dia, ou te mesmo pessoas que usam casualmente em casa ou em qualquer lugar, para ter acesso a fotos, redes socias, jogos, filmes, livros, informações em geral.

Lembrando que estes usuários se utilizam de vários dispositivos, estamos abordando todos os tipos de mídia eletrônica, como por exemplo, celular, notebook, Pc de mesa, tablet etc.

Todos estes usuários estão sujeitos a serem vítimas ou a cometerem crimes, mesmo que de forma inocente, sem perceber.

Existem também outros tipos de usuários que são pessoas com alto conhecimento na área te T.I, conhecidos como Hackers, que podem agir como hackers éticos e hackers não éticos como ante exposto. Eles podem tanto trabalhar para o bem, como também para o mal.

São pessoas com conhecimento avançado na área de tecnologia e que facilmente conseguem trabalhar para ajuda ou para cometer atos ilícitos, pois tem

enorme facilidade em acessar dados pessoais de outras pessoas, banco de dados, redes sociais, e qualquer outro tipo de área que esteja restrita a um usuário normal.

Os hackers também trabalham para o bem em alguns casos, como por exemplo detectando falhas em sistemas ou em qualquer dispositivo eletrônico e expondo está a falha ao seu criador, para que o mesmo faça os devidos reparos no dispositivo para que o mesmo não venha trazer prejuízos aos usuários que estão utilizando o dispositivo.

Crackers são os indivíduos que praticam a quebra de um sistema de segurança de forma ilegal ou sem ética, tem foco específico em descobrir senhas, dados privados, invasão de sistemas de empresas, governos etc., para se utilizaram das informações furtadas. A maioria dos ataques acontecem em grupo, aonde vários crackers trabalham para invadir determinado sistema.

Existem vários grupos na internet que estão destinados a prática desses atos ilícitos, os mesmos têm foco específico em roubar dados, derrubar sites e expor informações importantes sobre o governo ou algo que venha a trazer grande impacto as pessoas que ficarem sabendo.

Em alguns casos são pessoas que fazem a justiça com a própria mão em casos de grande repercussão nacional, eles agem de maneira autônoma para descobrir informações e as tornarem públicas.

7 LEGISLAÇÃO ESPECÍFICA

Existem duas leis que foram sancionadas no ano de 2012 para alterar i código penal e instituir os crimes cometidos pela internet.

A primeira lei foi a de crimes cibernéticos (Lei 12.737/2012), conhecida como Lei Carolina Dieckmann, que trata de invasão a dispositivos eletrônicos, furto de senhas, violação de dados e divulgação de dados pessoais.

Os crimes incluídos no código foram os do artigo 154-A e o Art. 298.

De acordo com o Artigo 154 da Lei 12.737, de 30 de novembro de 2012. Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de

função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem.[3]

Se trata de um artigo para proteger as pessoas de alguém em que se utilizando de seu cargo, função, ou profissão revela segredo que pode trazer prejuízo a outrem.

> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
> Pena - reclusão, de um a cinco anos, e multa.
> Falsificação de cartão (Incluído pela Lei nº 12.737, de 2012) Vigência
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. Lei n. 12.737, de 30/11/2012

Artigo 298 que trata dos crimes cometidos na falsificação de cartões de crédito ou débito.

A Lei seguinte é a 12.735/12 que determina a instalação de órgãos públicos especializados no combate dos crimes digitais.

> Art. 1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal , o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar , e a Lei nº 7.716, de 5 de janeiro de 1989 , para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Lei n. 12.737, de 30/11/2012.

A Lei tipifica as condutas realizadas através de dispositivos eletrônicos de todas as naturezas, para prática de crimes.

O artigo 4º desta lei se trata da criação de delegacias especificas para investigação de crimes cometidos através dos dispositivos de comunicação. A delegacia deve conter setores específicos e profissionais especializados para combater a ação ilícita na rede de computadores.

A lei que alterou o CP tem ainda o objetivo de proibir a produção, qualquer ação que propague o uso de softwares ou dispositivos que servem para invadir dispositivos de outros usuários. Foi então que no ano de 2014 foi sancionada a lei n. 12.965/014.

De acordo com KAMINSKI (2002, p.202)

> Entre as inovações tecnológicas que se estendem incrivelmente, a internet acaba apresentando claros desafios á aplicação de regras jurídicas (nacionais) no seu espaço (global). Essas dificuldades, no entanto, não

[3] Lei n. 12.737, de 30/11/2012. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 17/05/2019.

> podem servir de justificativa para que os Estados deixem de tentar intervir naquela dinâmica, regulamentando objetos e condutas de interesse público.

Esta lei foi criada para tentar suprir as lacunas existentes no sistema jurídico em relação aos crimes virtuais, abordando primeiramente e enumerando todos os direitos do usuário, tratando de todos os tipos de assuntos como solicitar os arquivos pessoais de navegação, bem como solicitar a atuação do pode público perante estes crimes, garantindo ao cidadão o direito de usar a internet de maneira autônoma sem ter nenhum tipo de prejuízo estando protegido a todo tempo.

As informações solicitadas são privadas e só poderão ocorrer mediante ordem judicial, como por exemplo, o provedor, senhas, IP, isso dificulta a ação da polícia no trabalho de investigação, pois os dados dos criminosos são protegidos por estas leis, pois todos são considerados usuários e este direito vale para todos.

8 COMPETÊNCIA PARA JULGAMENTO

A princípio para a definição correta da competência para julgar estes crimes, é necessária que saibamos determinar o tempo e lugar do crime. O lugar é considerado para fins jurídicos, muito importante porque pode facilmente se estender a limites territoriais fora de nosso alcance jurídico, em decorrência disso é de suma importância definir o tempo em que o crime foi realizado.

De acordo com MORENO, (2010, p. 95)

> O aumento das redes de computadores, possuindo como grande representante a internet, permitiu que se ultrapasse os limites fixados pelos critérios da territorialidade e da nacionalidade na prática de certos crimes.

Para que ocorra a aplicação da Lei penal no espaço devemos nos atentarmos ao princípio previsto no artigo da lei penal, do artigo 5º, do Código Penal brasileiro.

De acordo com o Artigo 5º do CP (2016, p. 527). - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.

Este artigo nos traz o princípio da territorialidade para aplicação da lei penal. Portanto para que os hackers sejam punidos o crime deve ser cometido dentro do nosso país. Seria interessante se houvesse um tratado internacional que

permitisse a perseguição destes criminosos partindo dos seus países de origem para que possam ser punidos da forma efetiva.

Portanto, para analisar a competência territorial devemos fazer uma verificação de onde foi consumado ou o lugar de onde partiu o derradeiro ato de execução. Precisamos ter em mente que os crimes digitais causam efeitos exteriores e poderão afetar outros países.

O nosso código de Processo penal no traz o Art. 70, que disciplina a competência para julgamento. (2016, p. 618)

> Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.
> § 1o Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução.
> § 2o Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.
> § 3o Quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção.

A determinação da competência se dá em razão do lugar aonde a conduta foi consumada, e quando falamos de tentativa, o lugar é determinado pelo último ato de execução. Analisando desta forma, quando for localizado o dispositivo usado pelo criminoso, estará determinada a competência do local para o julgamento da lide.

Podemos assentar que no Brasil os crimes cometidos por dispositivos eletrônicos, utilizamos a teoria da ubiquidade, não somente para determinar o tempo e lugar do ocorrido, mas sim fazer a preservação de provas que surgem, deliberando como o local aonde se encontra o provedor de acesso, e também aonde se consuma o crime.

9 CONCLUSÃO

De acordo com o que foi aludido, a internet surgiu para facilitar a vida de toda a nossa sociedade, foi criada com uma finalidade de facilitar a comunicação a distância de maneira efetiva, troca de informações, e consequentemente

melhorando a vida de todos. Porem a internet não é utilizada de maneira correta por todos os usuários, algumas pessoas se utilizaram do alto conhecimento em tecnologia e se aproveitando do anonimato que a internet fornece, para cometer crimes contra pessoas inocentes, trazendo prejuízo a elas.

O crime em específico que foi tratado neste artigo foi o de estelionato em forma de sequestro de dados através de Ransomwares, que são um perigo na atualidade, vírus silenciosos que podem afetar inúmeras pessoas em muito pouco tempo, que podem causar um estrago enorme e um grande prejuízo a sociedade. Estes crimes podem ser praticados por qualquer pessoa porque todos nos somos criminosos em potencial, e é muito difícil responsabilizar os agentes nestas condutas cometidas através da internet.

Também foi discutida algumas formas dos usuários se protegerem destes ataques tomando algumas medidas para manterem seus dispositivos seguros para tentar evitar a contaminação de seus arquivos, consequentemente fechando a porta de vulnerabilidade de seus dispositivos para se resguardarem deste mal que está à solta na rede.

Tratamos também da competência para julgamento dos crimes virtuais, aonde se faz necessário determinar o tempo e local do crime, que pode se estender facilmente para outros países, ou ate mesmo serem cometidos de fora do país e afetar usuários aqui dos brasil.

A nossa lei não consegue acompanhar o desenvolvimento da internet que é muito mais rápido que a criação de leis.

Todo dia surge um dispositivo novo, uma possibilidade nova de crime a ser cometido através da internet, e isso é um grande problema, pois não se pode punir alguém sem lei anterior que defina o crime que foi praticado, portanto, se for uma conduta nova o usuário se torna impune, pois não existe regulamentação sobre o ocorrido.

REFERÊNCIAS BIBLIOGRÁFICAS

COMER, E., D. **Redes de Computadores e Internet**. [Minha Biblioteca]. Retirado de https://integrada.minhabiblioteca.com.br/#/books/9788582603734/ Acesso em 15/05/2019.

CASTELS, M. (2001, p. 13,14). **A Galáxia da Internet**. Disponível em: https://zahar.com.br/sites/default/files/arquivos/trecho_-_a_galaxia_da_internet.pdf - Acesso 02/06/2019.

KAMINSKI, Omar. **Internet Legal: O direito na tecnologia da informação**. 1ed. Curitiba: Juruá, 2003.

Lei n. 12.737, de 30/11/2012. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 17/05/2019.

MORENO HERNÁNDES apud COLLI, (2010, p. 95). **Direito e Crime Cibernético**. Disponível em: https://play.google.com/books/reader?id=EQj1BgAAQBAJ&hl=pt_BR&pg=GBS.PP1 - Acesso em 18/05/2019.

Paesani, , L.M. **Direito e Internet: Liberdade de Informação, Privacidade e Responsabilidade Civil, 7ª edição**. [Minha Biblioteca]. Retirado de https://integrada.minhabiblioteca.com.br/#/books/9788522493623/ acesso em 15/05/2019.

SARAIVA. Vade Mecum Saraiva. 21. ed. São Paulo: Saraiva, 2016. Lei nº 12.965/2014 - **Marco Civil da Internet** de 23 de abril de 2014. (2016, p. 1975).

SARAIVA. Vade Mecum Saraiva. 21. ed. São Paulo: Saraiva, 2016. Código Penal Brasileiro. (2016, p. 527).

SARAIVA. Vade Mecum Saraiva. 21. ed. São Paulo: Saraiva, 2016. Código Penal Brasileiro. (2016, p. 618).

SILVA, Jorge Vicente. Estelionato e outras fraudes. 1. ed. Curitiba: Juruá, 1995, p. 55.

Ulrich, F. **Bitcoin A moeda na Era Digital**. (2017, p. 27). Disponível em: http://empreendernaeradigital.com/wp-content/uploads/2018/09/Bitcoin-A-Moeda-na-Era-Digital-Fernando-Ulrich.pdf. Acesso em 17/05/2019.