UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CENTRO DE CIÊNCIAS JURÍDICAS E SOCIAIS
UNIDADE ACADÊMICA DE DIREITO

NATHALIA DE MORAIS NOGUEIRA

DELITOS INFORMÁTICOS NA ESFERA NACIONAL E A EFICÁCIA DA LEI 12.737/12

SOUSA
2015

NATHALIA DE MORAIS NOGUEIRA

DELITOS INFORMÁTICOS NA ESFERA NACIONAL E A EFICÁCIA DA LEI 12.737/12

Trabalho de Conclusão de Curso apresentado a Banca Examinadora da UNIVERSIDADE FEDERAL DE CAMPINA GRANDE como exigência parcial para obtenção do grau de Bacharel em Direito.

Área de concentração: Direito Penal

Linha de Pesquisa: Direito Cibernético

Orientador: Prof. Dr. Jardel de Freitas Soares

SOUSA

2015

NATHALIA DE MORAIS NOGUEIRA

DELITOS INFORMÁTICOS NA ESFERA NACIONAL E A EFICÁCIA DA LEI 12.737/12

Trabalho de conclusão de curso apresentado ao Curso de Direito do Centro de Ciências Jurídicas e Sociais da Universidade Federal de Campina Grande, em cumprimento dos requisitos necessários para obtenção do título de Bacharel em Ciências Jurídicas e Sociais.

Orientador (a): Prof. Dr. Jardel de Freitas Soares

Sousa-PB,_____de_____de 2015.

Banca Examinadora:

_____
Orientador: Prof.

_____
Examinador interno

_____
Examinador externo

Para Verônica, que além de todo amor inerente à condição de mãe, ensinou-me desde pequena a prezar por aquilo que seria futuramente a minha máxima, o alicerce no qual baseio todos os meus dias: a liberdade do ser.

AGRADECIMENTOS

Aos meus dois pais, Francisco e Admilson. Ambos me proporcionaram uma visão distinta do significa da palavra pai, contribuindo ao seu modo com a pessoa que sou hoje. Da calmaria, pés no chão e segurança de um, até a poesia, empatia e cultura do outro.

À Gabriela e Patrícia de Morais, as quais dividem a posição de irmãs dentro de meu coração. A despeito da ciência de que ambas não são dadas a demonstrações de afeto e gratidão pública, gostaria de deixar marcado como dou valor à companhia de pessoas distintas, que compartilham comigo os mesmos valores, vocês me veem pelo que sou e por isso sou grata.

Gratidão eterna para figuras femininas fortes, que representaram o carinho de mãe diversas vezes: minhas duas avós, Maria Teresa e Laura Lopes. Figuras antagônicas de vital importância na minha criação.

À minha querida “Tia Nene”, por me acolher diversas vezes e fazer-me sentir amada sem pedir nada em troca que não fosse o meu sucesso. Ainda “Tia Jane”, pela qual gostaria de agradecer pelo suporte emocional em diversas situações.

Aos meus primos, que tenho por amigos. Grandes amigos. Independente da idade, dos dez até os trinta. Cada um de vocês me forneceu suporte, carinho e atenção que sequer imaginam. E colocando vocês aqui, fica a garantia de que vão me amar e pagar passagem de férias com todo luxo e conforto que mereço.

Toda família Morais e Nogueira, pelo alicerce familiar. Pela força e incentivo.

À minha melhor amiga, Alanne Eugenia. Agradecer por tudo parece ainda pouco comparado com a experiência vivida numa terra distante de onde nasci. Experiência compartilhada com você, sua visão de mundo e força de vontade. Desculpe-me se em algum momento, roubei um pouco da sua garra, mas ela é grande demais para nela não me inspirar. Obrigada por me ensinar que existe sim um amigo capaz de tudo por você – te levarei por toda a vida, ainda que o mundo insista em separações geográficas.

Aos meus amigos membros de uma Sociedade Morta que foi unida pelo amor às letras e permanece em meu coração pelo amor a cada ser individual que a compõe. Isabella – meu diário predileto, de uma paciência reconfortante. Letícia – minha fonte diária de debates, da partilha de pensamentos e de infinita criatividade. Laís – a pessoa mais carinhosa que já conheci, que me apoia desde o primeiro instante. Ananda – por todo conhecimento e força passados. Taís – por sua leveza e humor, ainda que não acredite muito neles. Vocês me enxergam por quem verdadeiramente sou, e por isso, sou grata.

Para todos os meus amigos, em especial a Thaís Monteiro, que compartilhou comigo a vivência cotidiana e me ensinou a exercer o respeito pelas diferenças e a prontidão para ajudar. E todos os demais que se demonstraram aptos a ajudar, reconfortar ou simplesmente deram alguma palavra de incentivo nessa jornada.

Aos meus mestres e exemplos que encontrei na caminhada dentro da faculdade: o meu orientador, Jardel de Freitas e as professoras Jônica e Marília, por emanarem tanta força e tanto querer em tudo que ensinam aos seus. Ainda agradeço a solícita professora Janeide e o mestre Marcelo – pois o ensinar não se restringe a quem te ensina lições numa sala de aula, mas para aquele que nos ensina tantas outras coisas nos percalços da vida.

Por fim, obrigada para todos aqueles que me ajudaram nessa etapa de minha vida.

RESUMO

Aborda os delitos informáticos e as transformações advindas do mesmo. Descreve o histórico da Internet e da sociedade virtual no qual está inserida. Demonstra o desenvolvimento da tecnologia, junto com sua influência na sociedade contemporânea. Usa da metodologia dedutiva para alcançar seu mérito. Define a Sociedade em Rede e demonstra sua relevância no mundo atual. Conceitua a Internet, expõe seus benefícios e os reveses. Explica as terminologias informáticas básicas e sua importância para quem acessa a Internet. Analisa o funcionamento da esfera virtual, suas minúcias e questões técnicas. Pondera a influência da informática no nascimento de novos delitos no novo século. Classifica os delitos informáticos, conceitua estes em próprios e impróprios. Classifica os sujeitos ativos dos delitos informáticos. Relata as novas classificações de criminosos. Esclarece os conflitos de territorialidade e tempo do crime no espaço virtual. Diferencia o procedimento investigativo relacionado a crimes digitais. Mostra a guarda de prova no meio digital, que é diferente da comumente usada. Aponta as legislações nacionais que disciplinam sobre a matéria. Denuncia as brechas deixadas pelo legislador quando ele se refere aos delitos cibernéticos no país. Aborda a Lei 12.735/2012, uma das primeiras nesse campo. Destrincha a Lei 12.737/2012 e fala sobre as falhas em seu texto. Demonstra o oportunismo social rondando os textos jurídicos cibernéticos no Brasil. Reflete sobre o Direito Cibernético no país. Fala sobre o futuro do Direito e sua necessidade de acompanhar as transformações sociais. Mostra o novo mecanismo de investigação utilizado no Direito Digital, que se diferencia do procedimento padrão utilizado em qualquer outra área investigativa nacional. Preocupa-se com o Direito e a sociedade atual, prezando pela segurança da mesma. Assim sendo, a necessidade do investimento no Direito Digital em nosso país, ao passo em que ressalta ser necessário que o operador do Direito acompanhe as transformações do meio que lhe cerca.

Palavras-chave: Direito Digital. Informática. Delitos Informáticos.

ABSTRACT

This article covers computer crime – also known as cybercrime – and the changes that came with it. Describes the history of the Internet and virtual society in which its find out. Shows the way that this technology evolved, along with the influence it had in the contemporary society. Uses the deductive approach of methodology to reach it's profits. Defines the Web Society and its importance in the world today. Conceptualizes the Internet, showing its pros and cons. Explains the most basic internet terms and its value to who access the Internet. Analyzes how the virtual sphere works, with its details and technical issues. Questions the influence of information technology in the birth of new crimes in the new century. Classifies the virtual crimes, into proper and improper. Classifies the active criminals on the virtual crimes. Shows the new kinds of criminals. Clarifies the territorial conflicts and time of crime in the virtual space. Distinguishes the investigative process for these type of crimes. It shows the criminal proof around the digital world, which is different from the commonly used. Points the national laws about the matter. Shows the gaps left by the legislator when he is talking about cyber crimes that happens in the country. Covers the 12.735/2012 law, one of the firsts in this field. Unveils the law 12.737/2012 and talks about the problems in its text. It shows the social opportunism around the virtual juridical texts in Brazil. Reflects about the Cyber Law. Talks about the future of Law and its need to keep up with the social changes. Shows the new ways of investigations used in Digital Law, that its different from the usual procedure used in any other national investigational field. Concerns about the law and society, appreciating the safety of it. Thereby, there’s a need of investment in Virtual Law in the country, while it also highlights that one that operates the law also needs to keep up with all the changes in the means that surrounds oneself.

Keywords: Virtual Law. Information Technology. Virtual Crimes.

SUMÁRIO

INTRODUÇÃO

O advento da tecnologia não foi um acontecimento repentino, cuja aparição transformou toda a sociedade em apenas uma etapa. Pelo contrário: a invenção dos computadores precedeu a internet, que por sua vez aprimorou-se conforme os avanços em sua própria ciência forneceram permissão.

Relatos de que o primeiro computador digital foi desenvolvido em 1946, o ENIAC *(Eletronic Numerica Integrator and Calculator)* desenvolvido pelo exército norte americano. Enquanto a internet teve seu primeiro gancho na década de sessenta, representada pela ARPANET (*Advanced Research Projects Administration)*, um projeto também norte americano derivado das necessidades alarmantes na época da Guerra Fria.

A sociedade, portanto, vive numa constante mutação, e a evolução tecnológica vem consumar um novo método de interação entre as pessoas na interface mundial; a distância foi entrecortada, cedendo lugar para uma conexão mais abrangente. No entanto, apesar da consciência de estarem encarando um grande avanço em questões tecnológicas, jamais se foi possível mesurar as proporções que tais inventos poderiam tomar.

Na conformidade das décadas, incontáveis foram os benefícios alcançados por conta da tecnologia virtual, sendo possível afirmar que ela moldou a entrada do novo século, assim como os hábitos da sociedade nela inserida – como consequência, o direito e seu legislador devem acompanhar as principais mudanças da sociedade.

O desenvolvimento do ciberespaço e a população que dela tornou-se usuária passou não somente a extrair prós, mas também vivenciar os prejuízos que nasceram desse meio. A evolução do ser humano trouxe consigo uma adaptação da criminalidade para o espaço virtual, portanto, o Direito precisa acompanhar tais transformações de modo a amparar os cidadãos cujas informações e detalhes tanto da vida pessoal como de trabalho, encontram-se sob a falsa sensação de segurança em hardwares, softwares e demais dispositivos envolvendo a rede de computadores.

Levando tal problemática em consideração, que desde abril de 2013 vigora no Brasil a lei nº 12.737/12 "Lei Carolina Dieckmann", na tentativa de que haja uma legislação que coíba as práticas de delitos informáticos.

Supracitada lei flerta com o direito penal alterando o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Essa lei é o primeiro passo para a escassez legislativa brasileira no que condiz ao espaço cibernético, sendo que a mesma peca em seu texto trazendo abertura para diversas interpretações ao mesmo tempo onde trás mudanças para um cenário outrora sem posicionamento jurídico relevante.

Apresentada também será a modernização do Direito, que nesse trabalho pretende abordar a evolução dos crimes numa ótica do mundo globalizado, atingido pelos meios digitais de comunicação e criação que por muitas vezes apresentam um vértice prejudicial cujo amparo legal defasado na atual legislação brasileira encontra-se como seu principal problema.

O presente trabalho intenciona analisar o cenário de crimes informáticos no Brasil, assim como a Lei de número 12.737, conhecida por “Lei Carolina Dieckmann” sendo ela um dos pontos principais para os legisladores brasileiros trabalharem no campo da *ciberdemocracia*, traremos à luz a repercussão da mesma no âmbito jurídico, assim como sua importância na esfera social brasileira que outrora se via sob a tutela civil.

A pesquisa desse projeto reside na natureza descritiva, sendo visada etapa mais sólida da investigação, analisar os aspectos da criminalidade informática na esfera nacional através do recurso da narrativa cronológica dos fatos, seguindo adiante pelo estudo do cenário contemporâneo comparativo e referencial acerca do caso, envolvendo assim pesquisa bibliográfica de cunho dedutivo, indo do âmbito geral para cautelosamente, especificar nossas intenções, trazendo os delitos informáticos para a seara nacional como propósito de elucidar os conteúdos abordados.

O método histórico e comparativo de procedimento será encontrado no decorrer da pesquisa, isso porque de primeiro plano é visado analisar o quadro de evolução histórica dos aparatos tecnológicos, de tal sorte que seja criada uma base para introdução do conteúdo na contemporaneidade – e também considerado comparativo, pois em alguns momentos será relevante equiparar as conquistas

nacionais, com as de outras nações, visto que a temática de “Novo Mundo” ainda precisa de quadro comparativo.

A coleta de dados será atribuída à documentação indireta, celebrando a pesquisa bibliográfica multilíngue. Serão utilizados livros abordando o referido tema, simultaneamente utilizado em acréscimo aos artigos e publicações que sirvam de embasamento técnico para dar prosseguimento na linha de abordagem adotada.

De referência, teremos ainda informações das análises de argumentos jurisprudenciais usados para complementar o estudo da matéria considerada ainda moderna para os operadores do Direito.

No tocante aos meios, o método utilizado será o bibliográfico, isso porque foram usados diversos autores, a exploração de artigos científicos abordando a temática cibernética criminalística. Durante o processo também serão revistadas leis envolvendo o condão dos crimes virtuais, tais como a legislação comparada que abrange determinados aspectos expostos.

Nesse procedimento metodológico serão analisados, ainda, os dispositivos legais envolvendo o universo dessa pesquisa buscando fomentar o estudo dos delitos cibernéticos, tal como acompanhamento de cunho cronológico na pretensão de acompanhar o desenvolvimento do mesmo.

Sendo assim, mostra através da pesquisa bibliográfica os crimes na seara informática, explicando as suas diferentes categorias. Mostra o oportunismo social existente por trás da aprovação da Lei 12.737/2012, ao passo em que aponta a falta de estrutura nacional para lidar com os problemas do chamado mundo moderno tecnológico. Defende, ainda, o Direito Digital e seu valor para o sistema jurídico e ao Estado.

Esquadrinha a Lei 12.737/12, trazendo à luz a repercussão dela no âmbito jurídico, assim como sua importância na esfera social brasileira, que outrora se via sob a tutela civil. Defende a existência de um novo ramo do Direito. Aponta a escassez de recursos no espaço nacional para combater os delitos cibernéticos, apontando a imprescindível organização do combate aos avanços desse contingente informático.

Destarte, o trabalho é motivado na real necessidade de promover o estudo da criminalidade e das ameaças que transitam pelo meio cibernético,

aprimorando o Direito da Informática, matéria recente que abrange diversos conflitos do cotidiano contemporâneo.

O primeiro capítulo tem enfoque nos aspectos da Internet e da sociedade virtual, elaborando acerca do contexto histórico e social que fizeram-na relevante para o homem de hoje e suas necessidades. Ainda no primeiro capítulo, estudar-se-á toda Sociedade em Rede, esmiuçando em seguida o conceito de Internet, para em avanço compreender melhor o seu histórico e funcionamento.

O segundo capítulo discorre dos conflitos encontrados nos crimes cibernéticos, questões sobre territorialidade e classificação das condutas condenáveis ganham foco. O estudo dos principais delitos informáticos também ganha destaque, sendo um por um destrinchado e colocado em pauta. Igual valia tende aos sujeitos ativos nos delitos, para depois de explicar os crimes, estudar o processo investigativo diferenciado e a guarda de prova dos mesmos.

Os delitos informáticos no Brasil preenchem o terceiro capítulo desse trabalho. Soluciona a problemática territorial e de tempo do crime, para enfim esquadrinhar relevantes Projetos de Lei e dispositivos legislativos aprovados envolvendo o tema informático. Por fim, alerta para o necessário novo profissional do Direito.

Apresenta em conclusão a necessária e irrevogável mudança na abordagem do Direito em todo país – além disso, apela que os termos digitais sejam adotados pelos doutrinadores, educadores e profissionais da área que se preocupam com o bem estar do cidadão, pois o Direito é acima de tudo uma forma de garantir segurança aos componentes da sociedade.

CAPÍTULO 1 ASPECTOS DA INTERNET E SOCIEDADE VIRTUAL

Este primeiro segmento esclarece o novo conceito de sociedade encontrado no panorama progressista no qual se encontra o mundo globalizado. Contempla o tema enquanto conceitua a Internet, demonstrando os aspectos que constroem a coletividade virtual. Por consequência, relata ainda o histórico envolvendo o processo criacionista da rede tecnológica, para enfim destrinchar o funcionamento dos mecanismos digitais de navegação comum.

1.1. A SOCIEDADE EM REDE

Na história, certas revoluções foram primordiais para a transformação da mesma. A Revolução Francesa, Burguesa, Industrial, todas elas contêm extratos do homem que perpetuar-se-á na memória da humanidade. Atualmente, se vivencia o período onde a Revolução corrente pode ser considerada a Digital – e ela trás consigo mudanças na estrutura basilar da sociedade. A própria definição de sociedade acabou por se renovar em decorrência do progresso tecnológico.

Em sua obra literária clássica, Política, Aristóteles se antecipa ao nosso cenário contemporâneo quando definiu o homem como um animal cujo destino é viver integrado para seu melhor funcionamento. “*O homem é, por natureza, um animal destinado a viver em comunidade*”. Conforme os séculos vão sendo deixados para trás, a despeito da tendência individualista do homem nascituro do século XX, o mesmo encontra-se mais conectado ao restante do mundo que nunca antes.

A sociedade padece de uma postura narcisista paradoxalmente preenchida pela integração humana numa teia de informações, hábitos culturais, econômicos, dentre outros fatores que anteriormente não conseguiam ser plenamente estudados por conta da ruptura na Rede que os conecta.

O conceito de Rede aqui aplicado é defendido por Manuel Castells e Gustavo Cardoso, em sua obra conjunta A Sociedade em Rede (2005), Manuel é pioneiro nos estudos da sociedade moderna, onde ele explica que o homem não se

adequa à evolução tecnológica – mas sim o caminho reverso, onde a tecnologia surge por efeito colateral da necessidade momentânea do coletivo. A estrutura coletiva acaba sendo influenciada tanto pelas tecnologias recentes, quanto pelos paradigmas sociais amplificados pelo novo patamar de integração proporcionado pelos aparatos tecnológicos. Tal advento apresenta uma sociedade emergente, onde muitos estudiosos apontam-na por sociedade do conhecimento ou ainda a era da informação.

Contudo, seguindo o raciocínio do referido norte-americano, Castells (2005) aponta falhas nessa percepção de mundo. Isso porque informação e conhecimento integram a estrutura basilar não exclusivamente desse século, sendo o homem uma figura ímpar cuja sede pelo conhecimento o faz buscar sempre por novas teorias e hipóteses que auxiliam em sua evolução. Destarte, faz-se mister apontar a grande novidade, o diferencial para que subitamente a informação tenha tomado conta de todas as residências. Se vive a época virtual, onde os eletrônicos proporcionam uma comunicação em rede:

> A sociedade em rede, em termos simples, é uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microelectrónica e em redes digitais de computadores que geram, processa e distribui informação a partir de conhecimento acumulado nos nós dessas redes. (CASTELLS, 2005, p. 19).

As vantagens são incontáveis, visto a possibilidade exploradora de flexibilizar e descentralizar as informações, propagando-as em ambientes diversos. É crível visualizar a rede virtual não como uma variedade de pontos separados que quando unidos, formam um todo, mas a análise correta tomaria rumos na contramão, ao se afirmar que toda a Rede é um ambiente único capaz de se fragmentar. Ou seja, a internet proporciona uma autonomia de valor imensurável – não obstante, fica difícil apontar alguma outra convenção histórica que tenha colocado os países em maior alinhamento do que ela.

Analisa assim, o desenvolvimento tecnológico e a gradual evolução das máquinas, pode-se analisar um embate político e sociológico na esfera cibernética. Implícito debate seria o questionamento de como é dada a divisão de poder nesse ambiente supostamente "*livre*", que já faz parte do núcleo social e familiar do século XXI. Poderemos então analisar que o poderio do acesso é desfeito em duas

concepções que se antagonizam, igual disposto em matéria de Jean Lojkine em 1995, defensor em sua obra A Revolução Informacional. Mencionado autor divide essas visões antagônicas entre dois polos conhecidos pela história universal: a elitista e a revolucionária.

A princípio, a internet detinha certo caráter elitista, pois há de se convir que a mesma seja fruto de pesquisadores e cientistas que visualizavam uma maior rapidez na comunicação e transmissão de dados entre sua própria limitada rede. Sua procedência igualmente é creditada aos eventos decorrentes da Guerra Fria, onde os Estados Unidos da América precisavam de uma resposta para as conquistas feitas pela Rússia, sua declarada adversária.

Partindo desse ponto, acaba sendo fácil detectar sua origem para poucos. No entanto, conforme as décadas foram passando, a mesma caminhou para o conceito de autogoverno - ou seja, a Internet acabou nas mãos da população para ser utilizada como quisessem. O acesso de todos à informação declarou um marco na humanidade, consolidando a máxima de que o homem não permanece parado, ele se molda, adapta-se.

1.2. CONCEITO

No princípio dos anos 90 a percepção humana envolvendo a Internet era incapaz de antecipar o gigantesco avanço que a mesma teria e suas conquistas para a sociedade contemporânea. Existiam questionamentos levantados envolvendo a rede mundial de computadores, além de certa descrença em relação à funcionalidade do mesmo. Apenas em 1990 que o acesso, outrora restrito a um grupo de estudiosos e cientistas vindouros dos Estados Unidos, Europa e Japão, chegou a ser acessível para quaisquer pessoas tivessem a oportunidade de navegação e construção de websites.

Esse momento de transformação pode ser aqui classificado como período da comercialização da internet, onde ela alcançou o status de produto comercial e de fins informativos por agora se enquadrar na procura de milhões de usuários.

A internet contribuiu com a tomada do indivíduo particular no mercado de trabalho, assim como fincou sua afirmação em fator determinante no processo de

globalização mundial. Indubitavelmente uma das maiores conquistas da modernidade, possui inúmeras funções, que vão desde a simplória pesquisa individual, passando por um essencial instrumento de trabalho, indo para uma indubitável fonte de entretenimento:

> A internet é um sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina a qualquer outra máquina conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem a limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento. (CORREA, 2008, p. 08).

Outra definição curiosa seria uma de Eric Schmidt, executivo da Sun Mycrosystems e atual presidente da NOVEL. A internet é a primeira coisa que a humanidade criou e não entende a maior experiência de anarquia que jamais tivemos. (CORREA, 2008)

Nascitura dos anos sessenta, sua primeira formatação advém de um projeto militar essencial para a guerra fria. Ou seja, a princípio a internet foi um mecanismo fatidicamente bélico, sendo que seu funcionamento pode ser explicado da mesma forma naquele tempo até os dias de hoje: o mecanismo procura uma variedade de caminhos para chegar ao ponto procurado, na palavra-chave utilizada.

Um dos principais princípios é o de que independentemente de encontrar uma travessia onde não se exista saída, uma nova porta seja aberta, para que ela encontre finalmente uma saída: o resultado da sua pesquisa, ou o outro ponto da sua rede de comunicação.

O fluxo de usuários da internet passou a crescer de forma exponencial a partir de meados dos anos noventa, assim como foi aludido anteriormente. O crédito disso fica por conta do modo como ela se determina, sendo baseada na proposta de uma única grande rede conectada capaz de abranger todos os pontos do globo terrestre. Nela, se encontram arquivos que utilizam os mais variados recursos, tais como áudios, sons, vídeos - projeções audiovisuais e escritas solicitadas no intuito de facilitar a conexão com os demais. A transmissão de dados tornou-se um dos maiores adventos da comunicação, sendo considerado o mais importante evento tecnológico no marco histórico:

> Desde 2002 o termo social software é usado para se referir ao tipo de programa que produz ambientes de socialização pela internet, ele é o que está por trás da colaboração online. Sua aplicação funde a difusão (broadcasting) que transmite informação da comunicação de duas vias. Em outras palavras, a internet representa a união das possibilidades de interação do telefone com o alcance maciço da nossa TV. (SPYER, 2007. 21).

Na obra de Spyer, é abordado um importante conhecimento, o primeiro registro de uma máquina que aproxima indivíduos e fortalece as possibilidades de interação veio ser feita em 1945 num ensaio do engenheiro norte-americano Vannevar Bush. O mesmo escreveu sobre o memex, que pode ser equiparado ao computador pessoal.

> Memex é um equipamento no qual um indivíduo registra todos os seus livros, discos e mensagens, e que é automatizado de maneira a ser consultado com velocidade e flexibilidade extremas. É um suplemento íntimo e ampliado de sua memória. (SPYER, 2007, pg 27).

Bush, em um dos seus mais famosos artigos, conseguiu descrever a internet em semelhança com o nosso modelo atual, isso vários anos antes da mesma ser criada. Vannevar antecedeu a criação de uma ferramenta capaz de registrar experiências pessoais e igualmente partilhar conhecimento - consequentemente auxiliando no acesso à informação.

Se explica o conceito de memex como registros de livros, mensagens, discos e demais formas de manter o conhecimento indelével. Eles estariam interligados e poderiam ser consultados numa velocidade acessível, extrema. O engenheiro se antecipou quase duas décadas, quando sua teoria veio tornar-se crível após a ideia de utilizar computadores para a colaboração.

O surgimento dos computadores como uma grande rede conectada surgiu no despertar da década de sessenta, nos Estados Unidos sob o contexto da Guerra Fria. Houve o pensamento de utilizar tais aparatos como resposta ao lançamento da nave Sputnik feita pela União Soviética. O pontapé inicial veio da Agência de Projetos para Pesquisas (ARPA), sendo que a mesma foi responsável pelo financiamento e posterior desenvolvimento de uma rede de comunicações chamada Arpanet, onde entra o conceito de hipertexto.

De acordo com Juliano Spyer, nessa fase foram delineadas duas tendências para a utilização de computadores na comunicação: na primeira, a tecnologia serve para cooperação, na outra, objetiva a colaboração. A cooperação seria por natureza algo estático, propiciando discussões a respeito de um problema já definido e compartilhando tarefas que se relacionem com o mesmo.

Colaboração, por sua vez, seria o processo dinâmico cuja meta é chegar a um resultado novo partindo das competências diferentes dos indivíduos ou grupos envolvidos. Ou seja, a cooperação vai se relacionar com o resultado tal como na colaboração o ganho de um ao mesmo tempo vai depender e influenciar o do outro.

1.3. HISTÓRICO

Não se pode falar da Internet sem antes compreender suas peculiaridades, os mecanismos que facilitam o seu funcionamento. A princípio é necessário esclarecer o contexto de "world wide web", também conhecido como o "WWW" que permite a interface virtual ser de maior acesso aos seus usuários. Como esclarecido pelo doutrinador Correia, em 2008, ela pode ser responsabilizada pela popularização de tal mídia. Por conta dela, se está apto, em vez de apenas contentarmos com textos em sua forma pura e simples há também agora desfrutar imagens, áudios e toda uma programação que facilita o movimento de página.

Há uma concepção interessante de que a World Wide Web é uma "convergência de concepções relativas à Grande Rede" permitindo que qualquer computador tenha acesso ao hipertexto relacionado com ela. Contudo, o que seria o hipertexto?

> Hipertexto é uma forma de organizar material que procura superar as limitações inerentes ao texto tradicional, em particular à linearidade. O prefixo hiper (termo do grego moderno que indica acima de ou além) significa a superação dessas limitações. A forma mais discutida de documento de hipertexto contém referências cruzadas inseridas automaticamente para outros documentos chamadas hiperlinks. Selecionando o hiperlink o computador acessa e mostra o documento relacionado. (WIKIPEDIA, 2014).

Esse conceito de hipertexto teve sua origem na década de setenta, por Ted Nelson, um pesquisador do Instituto Tecnológico de Massachusetts (MIT). O ponto de partida foi partir do pensamento em cadeia de que quando uma palavra fosse selecionada, a mesma redirecionasse o usuário para outros documentos que correspondessem àquela sua pesquisa.

Ou seja, surge a partir daí a concepção de unir toda a rede virtual como uma só – que alguém seja capaz de acessar as informações de outra pessoa em determinado ponto do globo usando como ponto de convergência nada além de meros vocábulos, um método simplório que precisou ser refinado durante os anos seguintes para chegar à complexidade dos dias atuais.

Porém, a World Wide Web assim como é conhecida foi aprimorada em 1989, em Genebra. Seu propósito inicial era a comunicação entre alguns pesquisadores que se dispunham em localidades diferentes, e dentre as propostas reunidas poderíamos dizer que reuniam três: a utilização de uma interface amigável, a habilidade de incorporar uma vasta gama de tecnologias e tipos de documentos na transferência, e por fim, a capacidade de ser lida universalmente.

Essa última apresenta a mais importante de todas porque enfim viabilizaria a capacidade da Grande Rede ser de alcance universal. Quaisquer usuários poderiam, através do computador, acessar o documento em outros pontos da Rede espalhados pelo mundo.

A primeira vez que o navegador WWW foi usado como recurso de fato, saindo do campo das ideias e dos projetos, foi em 1991, pelo mesmo laboratório de física que protagonizou toda sua pesquisa. No ano posterior tal sistema passou para domínio publico, sendo assim apresentado para a grande massa.

A partir de então uma série de avanços foram feitos – e estes podem ser apontados como vitais para o aperfeiçoamento da Rede. Contudo, não restringindo tais consequências apenas ao refinamento que ocorreu, mas também é válido dizer que não fossem os esforços feitos pelos cientistas até a década de noventa, possivelmente haveria uma demora na conectividade proporcionada pela criação da rede virtual informática.

Adiante na linha do tempo, tem início o ano de 1992, onde o aprimoramento do browser deu sequência para a integração de gráficos nos hipertextos. A partir disso, o acréscimo de atributos como imagens, áudio e demais

contornos gráficos em suas páginas acabou possibilitando que a população e o mercado financeiro vagarosamente tomasse interesse pelo advento. Seguindo com a cronologia, a partir de 1993 teremos diversos avanços tecnológicos e que contribuíram para a Rede ser propagada e sair do apelo científico para ser acolhida pelo apoio popular.

O MOSAIC para windows (que data-se de fevereiro de 1993) foi apresentado para o mundo por meio do "*Centro Nacional para Aplicações em Supercomputação",* sendo que citado centro tem sede nos Estados Unidos, no Estado de Illinois. Esse modelo de computador trazia consigo todo o aparato do WWW numa linguagem simplória, de fácil acesso.

A partir de então, existe outro salto onde a World Wide Web consegue ganhar espaço dentro de um período semestral. Dados citados por Teslas em Aspectos Jurídicos da Internet mostram que em março de 1993 os usuários eram 0,1% da população norte americana para que nos seis meses seguintes fosse deflagrado o salto para 1%.

Em decorrência disso, plausível que sua repercussão ganhasse visibilidade: a WWW conquistou os jornais mais prestigiados da mídia do país percussor. Estamparam-se páginas do New York Times, The Guardian, dentre outros veículos de comunicação em massa que auxiliaram na propagação de um investimento que se demonstrava de potencial econômico promissor.

Ademais, esse mesmo ano trouxe uma nova conquista considerada um verdadeiro marco na história da informática. Foi lançado o primeiro browser próprio para o sistema operacional que atualmente predomina os usuários virtuais: a Universidade de Cornell desenvolveu a programação do WWW para o Windows. Outro fato relevante foi a primeira conferência internacional sobre a web, realizada em Genebra, mesmo território onde parte crucial da sua pesquisa e desenvolvimento foi realizada. O crescimento do recurso foi de tamanha ascensão que Tim Bernes-Lee (o considerado pai da Internet) decidiu reunir o Laboratório de Física de Genebra ao Instituto Tecnológico de Massachusetts, criando a W3 organization.

Essa atitude do precursor da cadeia digital mostra sua acuidade porque em meados da década de noventa, não havia mais capacidade para o Laboratório de Genebra, sozinho, dar conta dos recursos necessários para o desenvolvimento da WWW. A junção dos laboratórios em prol do avanço foi chamado de World Wide

Web Consortium. O direito da organização, atualmente, continua sendo o cientista do MIT – ele também foi um dos fundadores da World Web Foundation.

Ou seja, a repercussão midiática, junto com toda a promessa de conectar as pessoas, feita pelos computadores pessoais ligados à Internet deixou de ser uma ideia abraçada por um grupo de cientistas para tornar-se a nova realidade, entramos numa era de revolução informacional, conquistando um novo ambiente para os anseios de conquista do homem: o ciberespaço.

> Ciberespaço foi um termo criado por William Gibson em seu livro *Neuromancer* para a descrição do mundo dos computadores e da sociedade que os cerca. Trata-se de um espaço fruto da interligação de computadores, como, por exemplo, o ambiente no qual trafegam os dados da Internet. (CORREA, 2008, p. 09).

Dentro do ciberespaço, encontram-se os mesmos elementos vistos no ambiente físico e ainda mais, pois o dito tráfego de dados é conteúdo exclusivo desse espaço virtual. A interligação de computadores dá origem a uma nova percepção societária, que por sua vez constrói hábitos e vai adquirindo costumes nesse espaço fornecido. Portanto, o termo ciberespaço aqui engloba todo o conteúdo que percorre esse tráfego de dados, sendo eles mecânicos ou advindos de atividades sociais.

1.4. FUNCIONAMENTO

Talvez um dos maiores atrativos da internet seja o seu design simples e a facilidade com a qual o homem médio consegue manipular a mesma. Era de se esperar que o padrão de funcionamento não fosse dos mais fáceis, levando-se em consideração a gama de oportunidades e modos de uso que ela apresenta.

No entanto, caso fosse complicado o manuseio, dificilmente teria sido adotada pela sociedade como um advento transformador. A grande conexão de redes mantém-se em padrão simplório, e para compreender a mesma devemos entender a estrutura dela, visto que para uma discussão mais acertada é necessário compreender a espinha dorsal e a engrenagem que a permite funcionar.

Seguindo a lógica, a Internet é baseada no hipertexto, também conhecido por seu nome em idioma original como *hypertext transfer protocol*, popularmente reconhecido pelos usuários por um conjunto de siglas mundialmente famosas, o HTTP. Este último funcionará dependendo da fidelidade em seguir ao protocolo, sendo quatro as etapas a serem consideradas: conexão, requerimento, resposta e fechamento.

Na primeira delas o navegador tentará manter contato com o servidor requerido, enquanto na próxima, o navegador especificará o protocolo para fins de definição da espécie de servidor que for selecionado. Quando chega ao terceiro procedimento, a resposta, ela será o momento onde as informações caminham entre o navegador e o servidor, para que finalmente a conexão com ele seja feita, configurando o fechamento.

A compreensão desse sistema apresenta relevância para o posterior dilema jurídico apresentado – pois uma vez onde coloca-se um tema em debate, precisamos compreender sua natureza e pormenores, afim de um justo esclarecimento.

Gustavo Tesla Corrêa direciona ainda para a compreensão do HTML, parte da linguagem informática e sigla bastante recorrente quando analisamos o assunto. O HTML, por sua vez, nada mais é do que um código utilizado para tornar legíveis os documentos postados nas plataformas e programas que compõem a Grande Rede. Essa criptografia passará pelos navegadores, onde serão traduzidos no monitor do usuário, possibilitando assim a sua interação. Citando exemplos práticos do que tais códigos geram, teremos os links, as listas, imagens e demais formas de gráficos que variam de acordo com o site acessado:

> A revolução na linguagem de comunicação entre rede e usuário resultou no aparecimento de uma interface amigável, mais interativa, fazendo da Internet, sobretudo através da WWW, algo mais simples e claro. O que faz da linguagem HTML importante e diferente é a interpretação de seus códigos pelos navegadores, como o aparecimento de alguns itens em sublinhado ou em negrito, criando um link e trazendo vida ao hipertexto criado por Ted Nelson. (CORREA, 2008, p.15).

Tudo que se relaciona aos fatos tecnológicos acaba ganhando uma acelerada mutação, então no conceito de HTML não haverá diferença, pois sozinho ele não poderia nos proporcionar toda a complexidade para manter a Rede ativa.

Foram desenvolvidas várias outras formas de aprimoramento no intuito de impedir a estagnação da web.

Por fim, abre-se parênteses para explicar a questão do domínio ou endereço eletrônico, essa exemplificação é importante para os estudos jurídicos, pois a questão da localização na Internet é algo que sempre levanta duvidas. O endereço eletrônico pode ser considerado, em analogia simples, a localização do usuário na Internet, tais como os Correios retêm o seu endereço físico. O objetivo do mesmo pode ser resumido em conectar o usuário ao servidor que se responsabiliza pelo site.

Esses endereços eletrônicos deverão seguir o padrão exigido pelo protocolo DNS (domain name system); sendo que o Comitê Gestor da Internet no Brasil, fundado em 1995, determinou em 1998 o registro de nomes de domínio, assim como passou a coordenar os endereços de IP. A Resolução nº 1 de 15 de abril de 1998, aduz que:

> Art 2º - O nome escolhido para registro deve ter
>
> I – comprimento mínimo de 2 caracteres e máximo de 26 caracteres;
>
> II – uma combinação de letras e números, não podendo ser exclusivamente numérico. Como letras entende-se exclusivamente o conjunto de caracteres de a a z. O único caracter especial permitido além de letras será o hífen (-);
>
> III – o nome escolhido pelo requerente para registro, sob determinado DPN, deve estar disponível para registro neste DPN. (numero da lei,1998)

Vale salientar que os prévios dispositivos de lei expostos dissertam sobre o endereço digital que vem após o “www.” Ainda existe outro procedimento a ser adotado, onde será preciso fazer o registro dos Domínios de Primeiro Nível (DPNs). Outro detalhe cujo destaque pode ser feito, vem novamente da obra de Gustavo Tesla:

> Além do registro do núcleo e do domínio de primeiro nível, todos os endereços registrados no Brasil possuem o sufixo ‘br.’, pois este foi reservado pela InternetNic/IANA para nosso pais. A InternetNic, ou Internet Network Information Center, foi criada em 1993 pela Fundação Nacional de Ciência Norte-Americana, tendo por objetivo principal o desenvolvimento tecnológico da Internet, não só no âmbito daquele país mas mundialmente, sendo a responsável, portanto, por traçar princípios gerais do registro de domínios. (TESLA, 2008, p. 23).

Em suma, tanto o endereço eletrônico quanto o seu domínio pode transformar parte do estabelecimento comercial, sendo categorizado no rol dos bens incorpóreos. Isso reforça a teoria de que a Internet invadiu todos os espaços da nossa sociedade, ampliando tanto a cultura quanto o comércio – ela dominou o mercado, os lares, os estabelecimentos comerciais e financeiros.

A linguagem virtual é mutável, inconstante, que foge dos padrões – ela está sempre em meio a um processo acelerado, sendo preciso um refinamento constante da sua própria estrutura para adequar-se às necessidades do homem.

Vivencia-se numa época onde a paralisação implica na perda, ou seja, é preciso viver numa mudança constante. A rede virtual foi, sem sombra de duvidas, o invento mais importante para definir nossa geração como conectada, interligada, globalizada. Nada mais justo que o Direito, como matéria que serve ao homem, adapte-se aos novos tempos e a nova demanda problemática da sociedade originária da época pós-industrialista. O Direito advém de uma linha cronológica antiga, sendo sua função social e obrigação permanecer caminhando de acordo com as necessidades do homem, e não o contrário.

Outro fator determinante para chamar os estudiosos do Direito ao fenômeno virtual dar-se-á pela criminalidade alarmante no ciberespaço. Não somente as utilidades cotidianas foram aprimoradas e se adaptaram ao campo informático, como também, devido ao entrelace cada vez maior das funções humanas com a rede virtual, notório foi a migração dos atos ilícitos para esse mesmo espaço.

CAPÍTULO 2 OS DELITOS INFORMÁTICOS E SEUS CONFLITOS

Os delitos informáticos trazem consigo incontáveis problemáticas, desde a territorialidade conflituosa até a questão do tempo do crime. Classificar as condutas criminosas no âmbito cibernético faz-se imprescindível, tanto quanto demonstrar as principais categorias delituosas do gênero. Nesse tipo específico de contenda, faz-se necessário compreender os sujeitos ativos, tal como ter uma visão do processo investigativo diferenciado.

2.1. A TERRITORIALIDADE NOS CRIMES INFORMÁTICOS

A sociedade é versátil – ela não se define por um ponto fixo, mas sim pelas mudanças consecutivas, pelas variáveis, por todas as minucias e peculiaridades que coexistem dentro dela. Portanto, difícil pedir que algo imensamente complexo venha a fechar os olhos para as transformações. Como foi bastante reiterado nesse trabalho, o homem é feito de mudanças e cabe ao Direito acompanhar cada uma delas, de modo a amparar as necessidades e proteger os seus partícipes. Portanto, inconsequente deixar fora dessa questão o surgimento do direito digital e todas as consequências surgidas com ele no quadro jurídico nacional e internacional.

Questões como a territorialidade e o tempo nos quais os crimes cibernéticos são cometidos surgem constantemente, e a explicação para isso segue o pensamento de que o espaço informático é diferente de todos os outros. O sistema computacional, a internet e os aparelhos tecnológicos prezam pela conexão.

Eles tentam, cada vez mais, interligar toda sociedade e facilitar seu dia-a-dia. Todavia, junto com isso há o surgimento de certas dificuldades para as quais os juristas devem estar atentos: na internet a noção de espaço e tempo é diferente do mundo material.

O ciberespaço nunca foi um território propriamente dito, não possui fronteiras no seu ir e vir – estamos diante de um fluxo informacional que trafega pelos mais variados países, sendo que um dado transmitido no Japão poderá ser lido por um brasileiro na curta distância de um clique.

Isto posto, uma das primeiras medidas a serem tomadas é a da localização da informação. É preciso buscar a fonte, de onde ela veio, para que o território seja ligeiramente apontado, ainda que por muitas vezes se esteja diante do caráter transnacional informático.

O crime pode ser praticado simultaneamente em diversos países, sendo suas vítimas estrangeiras, como pode ser cometido por um conjunto de pessoas em territórios diferentes vitimando uma unidade de outro país. Ocorre uma notória fragmentação do *iter criminis.* Uma consequência importante disso está relacionada com a prova processual. Colocando sob ângulo simplista, imagine que uma pessoa aqui em território nacional consiga invadir, modificar ou acessar dados nos Estados Unidos.

Imagine ainda que ao acessar tais informações, o mesmo criminoso a envie para a França no intuito de obter certa vantagem em seu beneficio próprio. Ou seja, um vírus, *trojan, malware, adware* ou similar pode ser difundido pela rede ainda que criado num só país. Nesse ponto tornar-se importante estudar a postura adotada pelo Brasil em casos de crimes digitais disseminado mundo afora.

Estudiosos apontam as teorias do resultado, da atividade e ubiquidade. Na teoria da atividade o lugar do crime será aquele onde a ação ou desenvolvimento se desenrolou, a despeito do resultado ter decorrido noutro território.

A teoria do resultado faz jus ao seu nome, sendo de maior valia o local onde ocorre o resultado. Por ultimo, a teoria da ubiquidade é importante para a doutrina brasileira, visto que ela é a adotada em nosso território. Está protegida pelo artigo 6° do Código Penal, em destaque:

> 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. (Redação dada pela Lei nº 7.209, de 1984).

A adoção dessa teoria contribui com o Direito Penal Internacional, pois a lei brasileira poderá ser aplicada ainda nos crimes dispostos fora da nossa fronteira. Pois no artigo 7° do Código Penal reside a disposição sobre extraterritorialidade.

Por definição, os delitos praticados por brasileiros, apesar de envolverem uma vastidão de países envolvidos, podem ser acatados pela lei brasileira. Não obstante, aplica-se ainda a questão da interpretação, por isso o diálogo entre os países é primordial. A Convenção de Budapeste dialogou sobre cibercrimes:

> A Convenção de Budapeste sobre o Cibercrime dispõe que os países subscritores devem providenciar que sejam competentes para julgar as infrações previstas nos arts. 2° a 11°, sempre que a infração seja cometida no seu território, a bordo de um navio arvorando o pavilhão desse país, a bordo de uma aeronave matriculada nesse país e segundo as suas leis, ou, ainda, por um dos seus cidadãos nacionais, caso a infração seja punível criminalmente onde foi cometida ou se não for da competência territorial de nenhum Estado.
>
> Quanto a isso, a legislação brasileira já poderia ser considerada apta, não fosse a ausência da tipicidade das condutas relativas aos crimes digitais próprios, como o acesso não autorizado e dano informático. Dispõe a Convenção, ademais, que os países devem manter uma rede interligada 24 horas por dia, sete dias por semana, no intuito de facilitar a comunicação sobre os delitos (art. 35°), inclusive para o fornecimento de informações técnicas, conservação de dados e auxílio para a produção de provar em geral. (CRESPO, 2011, p. 245).

Ou seja, não se pode contar apenas com a abrangência física do território nas questões de crimes cibernéticos, pois eles estão ultrapassados pela tecnologia. O mundo virtual rompe essa barreira, sendo difícil a sua demarcação. Outra dificuldade é posta pela terminação *".com"*, indicando que supostamente deveriam ter sua base nos Estados Unidos da América.

Mas não acontece isso, sendo apenas o registro norte-americano e sua existência física não ocorre naquele lugar. Sendo assim, usando o registro *".com"* a pessoa jurídica ou não, dona desse domínio, está se sujeitando às leis de países diversos. Fortuitamente o Código Penal resolve problemas desse gênero tanto nos artigos sexto e sétimo já demonstrados, como ainda no artigo 5° do Código Penal.

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

Graças a esse dispositivo penal, podemos atribuir os crimes que aqui acontecem ao nosso próprio sistema judiciário, sem que existam sanções aplicadas em consequência disto.

2.2. CLASSIFICAÇÕES DAS CONDUTAS INCRIMINÁVEIS

Dentre os maiores desafios ao se estudar os crimes digitais, possível que o maior deles esteja relacionado com a classificação das suas condutas. Isso porque a maioria dos autores diverge sobre a matéria, sendo um dos principais motivos para tamanha diferenciação o fato de que seu conteúdo de estudo é mutável. A evolução das tecnologias faz com que as opiniões se renovem ano após ano, tornando a criminologia cibernética pautada no dinamismo - sendo assim, aqueles dispostos a estudá-la, precisam acompanhar as mudanças que lhe cercam.

Delinear os crimes informáticos contribui para melhor estudo e interpretação, sendo primordial esclarecer a ideia básica envolvendo essa divisão. Destarte, certas condutas delitivas que ocorrem no cenário informático, decorrem nesse meio por mera questão instrumental. No referido caso, não será absurdo dizer que o comportamento reprovável pode ser efetuado por diferentes *modi operandi.* Contudo, em outros casos o meio informático deixa de ser apenas meio de execução, como nos delitos que somente podem ser cometidos contra o ambiente virtual, ou os dados nele inseridos.

Assim, no trabalho é adotada a classificação do doutrinador brasileiro Greco, no intuito de facilitar o estudo. O autor representa os crimes digitais entre aqueles cuja conduta é feita contra o sistema informático, sendo a outra classificação dada àqueles cujo patrimônio ou objeto que se intenciona atingir é de outro bem jurídico. Em outras palavras, na primeira estão englobados os crimes de risco informático, enquanto na segunda são os delitos meramente interligados com o ambiente virtual.

Exemplos do que pode ser considerado um crime digital próprio pode ser o hacking, a obtenção e transferência ilegal de dados, o dado informático. Sem falar nos vírus e na sua disseminação, passando pela divulgação ou utilização indevida de informações, segue-se pelo embaraçamento ao funcionamento de sistemas, adiante em novo exemplo observa-se cautelosamente a engenharia social, também conhecida como pishing, para em seu oitavo demonstrativo termos a interceptação ilegal de dados.

No conceito de hacking, que envolve a maioria dos demais delitos informáticos, a porta de entrada para uma infinidade de diversos comportamentos maliciosos. A premissa basilar é a de que se invada sistema informático sem a devida autorização para isso.

Vale lembrar que a definição de sistema computacional ou informático aqui, são os dispositivos interligados que venham a processar todos esses dados de maneira automática. Automizado é aquele sistema que processa informações sem que o homem interfira diretamente. A rede informática funciona no princípio de comunicação entre dois, três ou mais aparatos que se interligam no intuito de trafegar dados:

> Para que as redes possam se comunicar, há regulamentação do tráfego de dados. Tais regras formam um conjunto denominado "protocolo". Na internet, cada computador que a integra recebe um número, denominado IP (internet protocol, ou protocolo de internet). Esse número, formado por quatro campos numéricos de bytes (um byte equivale a oito bits) é um endereço de 32 bits que identifica qual máquina componente de um sistema está acessando outra. Ex: 32.104.87.2. Todavia, como a manipulação dos números de IP é complexa, há um sistema (DNS - Domain Name System ou sistema de nomes de domínio) que faz a correspondência dos endereços de IP com nomes específicos. Assim, no exemplo anterior, em vez de o usuário da internet digitar 32.104.87.2, digitará www.stf.gov.br e terá acesso à página de nossa Suprema Corte. (CRESPO, 2011, p. 44).

De tal sorte que todos os computadores, pessoas ou não, recebem um determinado número que corresponde ao seu endereço eletrônico. Esse número será sua porta de entrada cibernética, pelo qual será reconhecido. No entanto, apesar do receberem tal numeração, a mesma dará lugar ao correspondente em domínio, no propósito de facilitar sua interface e aproximar-se do usuário comum.

2.2.1. Principais delitos informáticos próprios tipificados

Para a compreensão dos delitos informáticos, imprescindível fazer alusão a um conceito doutrinário europeu sobre os delitos informáticos, onde a classificação dual permite uma análise diferenciada. Estão eles divididos entre delitos de relacionamento e delitos de intervenção.

Por "delitos de relacionamento" são assimilados os crimes determinados pelos relacionamentos, havendo um contato real, direto. Ou seja, nesse grupo se aponta o estelionato, por tratar-se de um crime onde é necessário estabilizar contato com a vítima do caso. Em contrapartida, os "delitos de intervenção", descartam essa interação entre criminoso e vítima. Ele poderá ser efetuado por meio de ação unilateral. É de vital importância explicar as diferentes categorias dos crimes informáticos antes de aprofundar no estudo jurídico nacional sobre o Direito Digital.

Faz-se mister reforçar que os crimes digitais que serão apresentados, apesar de serem delitos corriqueiros, nem todos eles encontram-se amparados pela legislação brasileira. Não há, no Brasil, ordenamento penal que mantenha foco nas violações de bens jurídicos nascituros da revolução virtual. E isso está provado conforme observa-se o apelo do presente trabalho, também no que as mídias apelam por mudanças.

2.2.2. Intrusão informática

O artifício da intrusão informática define a invasão de terceiro a um sistema, independente aqui de ele obter ou não vantagem com sua atitude. Também há de se desconsiderar os métodos, sejam ardilosos ou não, tendo emprego de violência ou quaisquer outros métodos.

A princípio tal delito era conhecido como aquele onde os ataques ocorriam a sistemas fechados, quebrando suas defesas (*breakage*). No entanto, aprofundando o estudo da matéria, percebe-se que não necessariamente o invasor precisa usar de subterfúgios sórdidos para violar sistema que não seja o próprio, tampouco precisa deles no objetivo de conseguir acesso.

Em linhas gerais, boa parte da tecnologia lançada chega ao mercado com o que podemos chamar de bugs. Uma das interpretações de bugs é que eles são justamente isso: falhas no sistema, defeitos de programação. Por lógica, qualquer produto que possuímos e apresente defeitos em sua defesa, pode apresentar uma fraca resistência a corpos estranhos - muitas vezes, nenhuma.

Na verdade, acaba sendo fácil para os estudiosos da informática, obterem acesso a essas portas abertas. Ainda no conceito de intrusão, se observa outra forma criativa para subjugar o programa computacional de um usuário. Esse último

pode ser definido por programas que instalam arquivos silenciosos nos computadores, *tablets*, ou qualquer que seja o sistema virtual utilizado. Os arquivos citados, logo depois de instalados em sua rede informática, instalam códigos que facilitam o acesso do invasor.

Na grande maioria das vezes o usuário do sistema nem mesmo chega a perceber as alterações, isso porque o método de *backdoor* utilizado é aquele onde não há emprego algum da violência. Alguns estudiosos apontam o interesse na substituição do emprego "intrusão" informática por "introdução" mal intencionada. De acordo com Paulo Marcelo Ferreira, em sua obra criada em 2006, que fala sobre crimes de computador e segurança dos mesmos, pode ser feita a comparação entre a violação de domicílio e a intrusão informática. Isso no caso onde existam senhas ou sistema de segurança protegendo os arquivos.

A conduta é ilícita, pois todo o caráter privativo dos arquivos, documentos e programas, fazem com que apenas seu proprietário detenha o direito vinculado a sua divulgação. Mostra aqui a violação da confidencialidade, assim como da segurança telemática, sendo que a Lei nº 12.737/2012 foi a primeira lei a trazer certo amparo a este delito, ainda que ele não seja o mais apropriado. O objeto será bem tratado quando houver matéria certeira o envolvendo.

2.2.3. Furto de identidade

Uma característica assintomática da sociedade virtual é o grande evento das comunidades. Um grupo de determinadas pessoas, com interesses afins, acabam desenvolvendo laços sociais que quando acumulados e postos numa rotina cotidiana, acabam definindo-as. Sua imagem, após determinado tempo de uso, acaba definindo a sua identidade. No entanto, não se restringe apenas ao uso da imagem, mas sim de apelidos utilizados para determinados fins.

Uma vez onde sua identidade virtual é criada, ela ganha existência no meio ambiente virtual. Ganha corpo, vida. No entanto, infelizmente para o ordenamento jurídico brasileiro, é usado o trabalho com o sistema de teoria da inversão da posse, e ela se explica pela necessidade do bem ser móvel para que haja um furto. Contudo, no espaço virtual se lida com uma problemática diferente:

> Ocorre que, por conta dos bits que compõem os dados a serem intangíveis e somente representações de uma linguagem a ser interpretada pelo dispositivo, não existe a possibilidade de subtraí-los, mas tão somente de replicá-los (copiá-los) para outro dispositivo, havendo, então, pluralidade de originais idênticos. (SYDOW, 2013, p. 95).

Por consequência, ninguém vai demover alguém de um dado. Furtá-lo, ou o roubar em sua literalidade. Apenas destruir, duplicar ou manter uma posse silenciosa não autorizada. A confusão com a nomenclatura pode também ser creditada ao fato dela ter origem inglesa*, "identify theft".* No Brasil, haverá um distanciamento da legislação brasileira, porquanto ela compreende como furto apenas a subtração, baseada na ideia de unidade do bem. E isso, como é visto não se configura no universo informático onde os dados são constituídos por sua pluralidade. Essa mesma pluralidade mostra-se como característica singular e recorrente dos estudos informáticos, dado a sua natureza complexa.

2.2.4. Inserção de código malicioso

Popularmente conhecido como *malware,* entra no rol das sabotagens que podem ocorrer no ramo informático. Os arquivos podem conter códigos puramente maliciosos, cujo intuito é quebrar a confidencialidade, prejudicar, atrasar a velocidade, integridade e comprometer a segurança dos dados. Essa conduta isolada configura a inserção de código malicioso, sendo esse um crime melhor tipificado na legislação alienígena.

No direito comparado, é trago a tona o discernimento de alguns Códigos Penais envolvendo a matéria. Primeiro, cita-se o Código Penal Japonês, onde no seu artigo 234-2, disserta que uma pessoa que interfere a operação ou negócio de outrem, utilizando-se de computadores para o gesto criminoso, ou ainda que causa dano ao aparato eletrônico fazendo uso de dados falsos e atribuindo comandos não autorizados, deverá ser punida.

O ciberterrorismo é uma ameaça real nos dias de hoje, sendo ela um dos principais motivos que incentivam tais invasões de sistema, não podendo ser descartado também a tentativa de prejudicar o indivíduo em particular.

Em se tratando de ciberterrorismo estaremos diante de ação penal pública. Spencer Roth nos elenca os principais tipos de malwares que devem ser levados em consideração nessa espécie de crime: os vírus, os *rooktkis,* os *worms*, os *trojan horses,* os *keyloggers,* os *screenloggers,* os *spywares* e até algumas modalidades de *adwares*, entre tantos. A Lei n. 12.737/2012 também trouxe mudanças relevantes para esse tipo criminal em sua redação.

2.2.5. Scamming

A definição de *scamming* pode ser compreendida por meio da simples tradução. *Scamming* vem do inglês, sendo que *"scam"* é verbo originário de fraude. Ou seja, *scamming* englobam as fraudes virtuais. Existem diversos tipos de fraude pela internet, diversos pequenos gêneros utilizados via de regra para obter controle sobre as máquinas dos usuários com menor conhecimento de segurança na rede. Dois métodos são mais conhecidos nessa categoria, sendo o primeiro deles onde o delinquente se envolve no ato a título de engenharia social: ele de fato entra em contato com a suposta vítima, até que consiga sua confiança e possa induzir tal pessoa a realizar transferências de valor financeiro em seu favor.

Vale ressaltar que esse tipo de atividade não é exclusivo do ciberespaço, no entanto, quando nele ocorre acaba sendo nomeado de *scamming.* Ademais, outros subterfúgios para envolver os "navegantes" vão desde os *adds* (propaganda) até as mais amplas categorias. Eles vão do emprego da engenharia social para os esquemas envolvendo a crença do usuário em estar diante de uma propaganda séria.

2.2.6. Spamming

O doutrinador Spencer Roth traz a discussão de que na esfera penal, há certo debate envolvendo a relevância do *spamming.* Pode ser lido como as famosas

mensagens não solicitadas que invadem o e-mail, sendo considerado o “lixo eletrônico”.

Elas podem ser utilizadas desde no intuito de fraudar, se apossar da identidade, difundir vírus, invadir seu sistema operacional, etc. Infelizmente, a criminalização dos spams anda em passos lentos, ainda que alguns países tenham legislado nesse âmbito. Exemplo de países podem ser os Estados Unidos: *CAN-SpamAct.* Geograficamente perto da nação, há o exemplo da Argentina: *Ley de Protección de los Datos Personales.*

No Brasil, até o presente momento não há um posicionamento formal nesse sentido. A importância em se legislar deriva do spamming ser crime informático próprio, visando o congestionamento na rede que ele proporciona, a violação do bem jurídico, a violação da paz pública da privacidade.

2.2.7. Interceptação de e-mail

É o sequestro de e-mail, onde você impede que ele chegue ao destinatário. Para melhor entendimento da matéria, faz-se proveitoso ter uma visão melhor da estrutura por trás do sistema de mensagens eletrônicas:

> A mensagem enviada por um programa de envio de correio eletrônico tem um funcionamento bastante simples. Alguém digita em seu dispositivo telemático uma mensagem e especifica um endereço-destino representado pelo usuário, o símbolo da arroba e o provedor do serviço-destinatário. Este conteúdo é constituído por bits que são encaminhados ao provedor-remetente do serviço, que, por sua vez, conhecendo o provedor-destino, encaminha-o por meio da rede mundial de computadores. (SYDOW, 2013, p. 111).

Capturar, impedir o envio da mensagem ou do pacote de dados anexados nele, todas essas condutas configura interceptação de e-mail. Interceptar seria equiparado a colocar um empecilho no intuito de impedir qualquer espécie de desenvolvimento.

Contudo, na informação digital temos que os dados da mesma se dispersa através da rede, deixando consigo rastros que podem fazê-la ser lida ainda

que alcance seu local de envio e destino. Uma medida cabível contra possível ato é o de se criptografar ou ocultar conteúdos que peçam uma maior discrição.

2.3. DOS SUJEITOS ATIVOS DOS DELITOS

Uma vez estudados as espécies de crimes virtuais e classificando-as como próprias e impróprias, outra questão do direito digital precisa ser desmistificada: a dos sujeitos ativos. Quando se mencionam as práticas abusivas na esfera cibernética, costuma-se relacionar todas elas com os famosos "hackers".

Erro comum da sociedade acreditar que todos os crimes envolvendo o sistema informático são realizados por eles, acostumados a levar o título de vilões da internet. Muito embora seja isso que acontece no cotidiano, errôneo afirmar que os hackers são responsáveis por toda balbúrdia gerada pelas condutas ilícitas. A seguir, são tipificados os sujeitos ativos dos delitos virtuais, baseado no pensamento de um dos poucos doutrinadores sobre a matéria no Brasil, Marcelo Xavier de Freitas Crespo.

Plausível dividir tais sujeitos no seguinte rol: os *hackers, crackers, carders*, *lammers, wannabes, phreakers* e por último, os *white* e *blackhats.*

- *Os hackers:*

Nomenclatura nascida no *Massachusetts Institute of Technology* (MIT), de onde a internet é derivada. Os estudantes envolvidos no arcabouço computacional costumavam dedicar suas horas na pesquisa do computador e tudo que pode ser realizado com ele. Todo afinco depositado, remota para uma tradução bastante utilizada em doutrinas, que seria a de "fuçador". Hacker, aqui, seria a pessoa que se dedica a fuçar, investigar e vasculhar os sistemas operacionais para sua própria vantagem.

Ele extrai dados e informações, porém não danifica o sistema invadido. A categoria dos hackers não está apenas composta por invasores constituídos de intenções prejudiciais, havendo os famosos hackers que agem na internet afim de

invadir sistemas alheios para avisá-los de falhas e brechas em sua programação de segurança. Alguns outros hackers acabam sendo contratados por empresas interessadas em proteger seus dados com maior eficácia. Hacker, por definição, seria o princípio-base dos invasores. E o que eles farão ao invadir é que forma os subgêneros restantes.

- *Os crackers:*

São eles os responsáveis por diversos crimes atribuídos ingenuamente aos hackers. Essa categoria de sujeitos intenciona destruir e roubar informações, assim como podem se interessar por recompensar pecuniárias. Famosos por quebrarem sistemas (muitas vezes por mero capricho ou pela repercussão que sua ação terá), outro costume atribuído aos crackers são as invasões a sites no objetivo de propagar mensagens difamatórias e de cunho pejorativo.

Os hackers, portanto, seriam aqueles que se utilizam de computadores como instrumento de fim. Enquanto os crackers seriam os verdadeiros vândalos da esfera virtual.

- *Os carders:*

Uma grande preocupação do direito, visto que enquadram os criminosos que costumeiramente realizam compras de cartões de crédito pela rede. Tais números podem ser de terceiros, ou aqueles gerados por programas computacionais específicos. Os *carders* invadem computadores de administradoras de cartões de crédito para roubar seus números, distribuindo todos eles em seguida na preocupação de ocultar o traço de quem originalmente os roubou. Nessa empreitada eles precisam de IP's falsos e contas "piratas".

- *Os lammers:*

Constantemente depreciados pelos hackers, formam um grupo de pessoas que sequer detém conhecimento o bastante para realizar invasões e não

possuem nada além da própria lábia. Nessa categoria entram os mais delirantes, que afirmam poder invadir sistemas poderosos e detém apenas o conhecimento mais básico. São semelhantes aos *wannabes.*

- *Os wannabes*

Anseiam pelo título de hackers, no entanto ainda não possuam habilidade para grandes atos. Mas ao contrário dos *lammers,* estão aptos a operações menores por possuírem certa consciência da sua capacidade. Empenham-se no estudo cibernético por tratar-se de matéria interessante para eles, que os instiga a investigar cada vez mais.

- *Os phreakers:*

A especialidade dos *phreakers* é o grampo telefônico. Não estamos falando de escutas físicas, colocadas em aparelhos móveis ou similares. *Phreakers* utilizam programas computacionais que operam da seguinte forma: quando o telefone da pessoa invadida com seu programa toca, próprio telefone do *phreaker* espelha o gesto para que ele possa escutar toda a conversação. Outro costume desses criminosos é o de invadir operadoras de telefonia, para que as companhias tenham seus registros alterados. Dessa forma, alguma outra pessoa pagará pelas ligações feitas pelos *phreakers.*

- *Os white e blackhats:*

Outro termo utilizado para definir os hackers bons dos "ruins". Sua referência encontra-se nos filmes de western norte-americanos, pois neles os "mocinhos" heroicos tinham costume de usar os chapéus brancos enquanto os vilões usavam de chapéus pretos. Logo, *White hats* seriam "hackers do bem", onde *blackhats* seriam hackers "maus".

2.4. INVESTIGAÇÕES DOS CRIMES CIBERNÉTICOS

Nas investigações de crimes virtuais, vamos adotar a divisão elencada pelo Sydow Spencer, no qual repartem as fases da investigação em: fase técnica e fase de campo. Na primeira delas, o enfoque ficará na tentativa de localizar o computador através do qual o crime foi cometido. Nessa fase, ocorrerá a análise do relato e das informações que a vítima fornecer, onde o intuito é compreender melhor o fato que ocorreu na internet. Ainda aqui, de acordo com a compreensão dos autores, serão feitas orientações para a suposta vítima, para que o material da prova seja mantido intacto e a mesma angarie proteção virtual.

Há ainda a coleta das provas no ambiente virtual, passando para a formalização do fato criminoso – ele deve ser feito comumente através dos boletins de ocorrência, registro, boletim. A terminologia varia de acordo com o estado no qual se encontra e o costume empregado.

A investigação inicial dos dados disponíveis e o registro de possíveis autores, buscando encontrar a origem das correspondências eletrônicas, da hospedagem dos domínios, etc. Sua fase técnica passa ainda por três outros pontos, sendo a formalização do relatório das provas coletadas.

Finalmente haverá a representação diante do Poder Judiciário, para que seja feito expedição da autorização judicial para a quebra do sigilo dos dados, conexão ou acesso (aos provedores poderá ser solicitado dados cadastrais de usuários), para que enfim seja feita a análise das informações coletadas nos servidores.

Nessa etapa da investigação, após a devida e minuciosa análise, se abre os olhos para a necessidade de envio para o Poder Judiciário demais representações do mesmo provedor, ou mesmo que seja solicitado a esses provedores que contribuam mais uma vez com a investigação e permitam acesso a outros dados e registros que devem obrigatoriamente estar guardados sob sua tutela.

É função dos provedores resguardar os registros dos usuários, como seu endereço (identidade) virtual. Isso porque o endereço de IP (protocolo da internet) atribuído a cada pessoa que navega na internet é exclusivo durante sua navegação,

anulando a possibilidade de dois usuários utilizarem-se do mesmo endereço durante a utilização da internet.

Isso é aplicável não somente aos computadores pessoais, como aos tablets, celulares e demais dispositivos que se conectem com a internet. Isso independente do IP ser estático ou dinâmico, continuando a ser devido que os usuários possuam endereços diferentes caso acessem a internet no mesmo fuso horário e dia.

E o que seriam IP's estáticos e dinâmicos? No protocolo da internet dinâmico, cada vez onde ele reiniciar o modem ou liga-lo novamente (falando do modem, não sua conexão virtual), um novo endereço de IP será associado com um novo endereço eletrônico.

O uso dos protocolos estáticos é um costume mais utilizado como recurso empresarial, visto que ao fazê-lo poderá ter maior controle das pessoas que acessam, ou seja, dos seus funcionários – isso porque o endereço eletrônico continuará como sugere o nome, sendo fixo. Uma vez identificado esse endereço virtual na investigação, terá início a fase de campo.

Nela, surge a necessidade do deslocamento dos oficiais para cumprir com as diligências na intenção de reconhecer o local indicado no apontamento eletrônico. Essa fase pede discrição dos envolvidos caso haja necessidade da alguma medida processual penal cautelar, ou seja, a representação para mandado de busca e apreensão.

Esse tipo de procedimento ocorrerá prontamente se o endereço indicado tratar-se de residência domiciliar e não de espaço coorporativo. Os processos vão divergir dependendo de onde serão realizados, o procedimento investigativo será especializado. A seguir, divididos em tópicos:

Para registrar um domínio (site) na internet, o procedimento padrão é bastante simples. Via de regra, nos sítios internacionais, toda informação que basta é ceder o e-mail como cadastro, login e senha, além do pagamento para manter esse registro como seu – o valor do pagamento aqui pode variar. Contudo, no Brasil, faz-se mister apresentar o CPF ou Cadastro Nacional de Pessoa Jurídica (CNPJ), o valor atual do domínio nacional é de R$ 30,00, para que se use o ".br".

Ainda assim, em ambos o sítios (nacional e internacional) falta o pedido de documentos, o que facilita o aumento das informações inverossímeis na hora de

investigar o crime. Sendo assim, para obter os dados cadastrais da pessoa investigada, o perito precisará ir direto aos sites de registro. Nos sites cuja terminação é “br”, indica-se o acesso ao site dos Registros Nacionais

Dentro dele, o investigador seguirá com o procedimento padrão de busca e etapas encontradas no próprio site, sempre visando encontrar os dados cadastrais e quem é o responsável pelo serviço. Três elementos básicos devem ser encontrados na investigação de sites, ou pelo menos, algum deles: a identificação do responsável pelo site, a identificação dos servidores DNS, e a identificação da responsabilidade pela hospedagem e a identificação da responsabilidade pela hospedagem.

2.4.1. A guarda de prova no meio digital

No processo investigativo dos crimes virtuais, assim como de qualquer outro gênero investigativo, alguns cuidados são necessários para resguardar as provas encontradas. A internet pede que as provas sejam rapidamente salvas, antes que elas sejam alteradas ou excluídas do campo virtual. Primeiro temos a famosa impressão, feita usualmente. Além dela, temos diversas alternativas.

O recurso do *“printscreen”* copia a imagem que no momento encontra-se na sua tela e deverá colar essa imagem congelada em algum programa de edição da sua preferência, valendo lembrar que se ela for colada no Writer poderá compor o relatório da investigação inicial, ou da petição inicial caso seja o advogado.

Contudo, esse recurso do *printscreen* poderá ser refutado ou questionado no judiciário, sendo assim, não é recomendável que seja matéria de prova exclusiva – aqui é aberto o parêntese para as chances de a imagem ter sido alterada, algo bem recorrente no mundo virtual.

Mas como leciona Emerson Wendt (2013) existem outras opções viáveis. Um dos recursos para manter a prova é o salvamento de cópia das páginas, esse método se encontra nas próprias páginas de navegação, em seu menu de ferramentas. Via de regra, ao salvar uma página, dois arquivos nascem dela: um deles contém o nome da página, e o outro os arquivos vinculados com ela.

Infelizmente, os links não são salvos e há de se proceder manualmente para salvar cada um deles – outra observação interessante seria a recomendação de que os arquivos salvos por esse recurso sejam levados ao tabelionato para ser lavrado uma Ata Notarial.

Outra opção viável seria utilizar o conjunto dos programas HTTrack Website Copier e o MD5summer, sendo o website copiar um mecanismo bastante utilizado e de roupagem simples, no intuito de que a cópia salva contenha os links devidos que possam interessar ao processo de investigação. Esse software agracia o investigador com uma cópia dos logs e arquivo “index” para facilitar o salvamento dos arquivos em material de mídia portátil. Ou seja, poderá um CD ser anexado ao Inquérito ou Processo Judicial.

Emerson Wendt e Higor Vinicius Nogueira Jorge em Crimes Cibernéticos, apresentam ainda a possibilidade de ser usada a Ata Notarial. Ela detém capacidade de ser utilizada para meio de prova eletrônica, incluindo os documentos, páginas e demais elementos virtuais. Ela consegue guardar a data da existência desses arquivos, dentre outros. A Ata Notarial será feita no tabelionato, sendo usada no intuito de provar tanto nos processos cíveis como nos criminais.

Serve de instrumento de prova ainda a certidão da Polícia Civil, visto a falta da razoabilidade no delegado de policia ter de ir ao tabelionato para manter seu registro em Ata Notarial. O escrivão tem pleno gozo da fé pública depositada em si para acessar os arquivos necessários e fazer sua impressão, sendo que o certificado dado por ele pode constar como meio de prova.

Em auxílio da investigação criminal, colocam-se as evidências deixadas por registro de acesso. A grande maioria dos usuários, leigos na navegação online, sequer imagina que estão deixando rastros por onde quer que passem na internet. Igualmente, cabe ao investigador e aos especialistas na área fazer a leitura desse caminho em casos investigativos – veja bem, a compreensão dessa matéria é devida aos estudiosos do caso e interessados, sendo que usuários não precisam dessa preocupação nas costas.

No entanto, esquadrinhar as evidências eletrônicas faz parte do procedimento de investigação, sendo esse o motivo pelo qual vamos tentar explicar certos conceitos básicos. Cabe a alguns programas tecnológicos o gerenciamento dos programas da rede, havendo duas formas de averiguar o registro realizado. Do

modo rudimentar, que seria o texto ou as imagens salvas e acessadas em site qualquer, ou pelo registro dos logs. Nestes últimos as informações contidas nos logs seriam a hora, data, de onde, qual, como foi acessado.

De tal forma que no momento onde o delito for cometido na rede virtual, os logs apresentam-se na posição de melhor forma para registro do caso. Comparação válida seria a dos logs equivalerem aos dados da companhia telefônica, que armazena os números para os quais o usuário está ligando ou recebe telefonema – por infortúnio do investigador, o registro virtual tem característica muito mais dispersa que a maneira uniforme e organizada dos telefonemas serem registrados.

CAPÍTULO 3 DELITOS INFORMÁTICOS NO BRASIL

O Brasil caminha para a melhor compreensão acerca do mundo virtual e os conflitos nesta localizados. O Direito Digital no país, ainda que atrasado em diversos pontos solidificou seus primeiros avanços em textos processuais e desponta certa relevância jurídica.

Projetos de Lei finalmente foram aprovados, numa amostra do avanço nacional nesse quesito o Projeto de Lei número 2.793-C/2011 foi aprovado na forma da Lei 1.737/2012 e ela trás consigo mudanças na esfera, que a despeito da relevância, demonstram uma ineficácia em certos pontos.

Serão abordados os ritos processuais envolvendo mencionada lei, abrindo espaço para a discussão do novo profissional do Direito e da renovação dos operadores do ramo.

3.1. O DIREITO DIGITAL NO BRASIL

O país sofre de um mal provocado pelo imediatismo. Diversas são as leis cuja redação atende aos pedidos da população, no entanto carecem de maior estudo. Peca pelo simbolismo, baseado na urgência de atender a pressão da mídia, cada vez mais imperdoável e roda propulsora que serve para acelerar a demanda dos pedidos. Dessa maneira, acabam procrastinando as reformas realmente necessárias em nosso direito penal.

Novas leis criadas sem esmero tem sua aplicação de cunho dúbio e coloca em xeque o poder de polícia, igualmente assim o poder judiciário. O Estado fica frágil, uma vez onde não vai conseguir plena eficácia e aplicabilidade dessa mesma lei criada. Partindo para o campo informático, não de hoje existem diversas reinvindicações advindas da polícia civil, federal e militar – eles clamam por equipamento apropriado, moderno, a tecnologia ainda é precária.

A evolução da sociedade e dos seus crimes ocasiona o clamor por novos aparelhos que auxiliem nas investigações. A defasagem nos instrumentos se estende para a falta de pessoal especializado sendo que essa ausência, quando conciliada com a internet de baixa velocidade, faz do processo investigativo um completo transtorno. É uma cadeia interligada, onde é ilógico transformar a legislação quando inexiste suporte técnico, ao passo em que fornecer o suporte tecnológico em território sem o mínimo amparo legislativo tornar-se-ia vão.

A competência para legislar sobre conteúdos do direito penal e consequentemente cibernético, de acordo com a Constituição Federal:

> Art. 22, CF. Compete privativamente à União legislar sobre:
> I – direito civil, comercial, penal, processual, eleitoral, agrário, marítimo, aeronáutico, espacial e do trabalho.

O delito virtual agrega uma série de dificuldades mesmo nos quesitos mais simplórios, à exemplo do espaço e tempo nos quais foram executados suas ações – os empecilhos caminham desde a localização do criminoso, para a extensão do delito. No campo digital brasileiro e os crimes nele contidos, ainda não temos uma definição estruturada sobre as funções desempenhadas na responsabilidade.

> A pura aplicação da teoria casual (teoria sinequa non) colocaria, por si só, todo o provedor na situação de responsável, posto que a garantia das ações do delinquente teria como suporte o acesso concedido pelo servidor. A retirada hipotética do provedor faria com que a conduta lesiva fosse impossível, e assim, colocaria-o como fundamental no cometimento do delito. Idem aos provedores de serviços e produtos exclusivamente virtuais. (SYDOW, 2013, p. 235).

Antes de o legislador traçar as mudanças penais, deveria ele delimitar as funções dos agentes virtuais, defender a garantia dos usuários perante a Constituição Federal e suas leis esparsas, para enfim delimitar onde, como e quando o poder público irá interferir.

O PL n. 2.126/2011, conhecido como Marco Civil da Internet brasileira, trabalhava nessa direção. Atualmente chamado de Lei n° 12.965/2014, sancionada pela presidenta Dilma Rousseff, está exposto em seu primeiro artigo a definição básica do que ela retrata.

> Art 1º - Esta lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

A Lei dispõe em seus capítulos sobre importantes apontamentos feitos ao longo desse estudo havendo nela a preocupação em tratar: os direitos e garantias dos usuários, a provisão de conexão e de aplicações de internet, a neutralidade de rede, a proteção dos registros, dados pessoais e às comunicações privadas, disserta a guarda de registros de conexão – ainda sobre registros, fala dos registros de acesso à aplicação de internet na provisão de conexão e de aplicações.

Em sua seção III, encontra-se a responsabilidade por danos decorrentes de conteúdo gerados por terceiros, ainda se depara com um capítulo falando da polêmica atuação do poder público. Todos os elementos elencados já podem ser acessados no site do Planalto.

Diante do exposto, fica exposta a preocupação do legislador nacional acerca do principio da confidencialidade, integridade e disponibilidade. Sintoma da adoção dessa base é perceber a preferência pela neutralidade da rede e no que concerne à integridade dos dados e estruturas. Mas antes do Marco Civil da Internet adentrar a jurisprudência brasileira no ano de 2014, outros projetos de Lei e alterações legislativas merecem destaque.

3.2. O PL N. 84/99 – LEI N. 12.735/2012

Esse Projeto de Lei teve origem na autoria de Cassio Cunha Lima, quando o mesmo era deputado pela Paraíba e apresentava-nos o PL n. 1.713/96. Ele acabou sendo removido da pauta, retornando para propostas em 1999, agora com o impulso do também deputado Luiz Piauhylino. Permaneceu parado por meia década, retornando em 2008 após revisão.

Apenas no ano de 2010 foi adaptado para se adequar na Convenção de Budapeste, sendo essa uma reunião internacional marcante para delinear as condutas consideradas criminosas nas vias informáticas. Ao final de sua saga, o Projeto foi aprovado remanescendo meros seis artigos, tendo sua aprovação no ano

de 2012. A despeito da perda do seu valor inicial, da ideia propulsora que tentou inovar nos tipos penais, algumas alterações ocorreram. Em baila, seis delas:

> a. Acresceu ao art. 298 do Código Penal um parágrafo único, com o nomen iuris de “falsidade de cartão”, equiparando-se a documento particular o cartão de crédito ou de débito (redundante no que se refere ao PL n. 2.793-C/2011, art. 3° segunda parte).
> b. Dentro do Código Penal Militar, no capitulo da traição, título “do favorecimento ao inimigo” tratando-se dos crimes militares em tempo de guerra, alterou o inciso II do art. 356, acrescendo como favorecimento ao inimigo o prejuízo ou a tentativa de prejuízo, o comprometimento ou a tentativa de comprometimento, a entrega ou a exposição a perigo de dado eletrônico;
> c. Dentro do Código Penal Militar, no capitulo da traição, título “do favorecimento ao inimigo”, tratando-se de crimes militares em tempo de guerra, alterou o inciso III do art. 356, acrescendo como favorecimento ao inimigo o prejuízo ou a tentativa de prejuízo, o comprometimento ou a tentativa de comprometimento, a perda, a destruição, a inutilização, a deterioração ou a exposição a perigo de perda, destruição, inutilização ou deterioração de dado eletrônico;
> d. Alterou o inciso II do parágrafo 3° do art. 20 da Lei 7.716/89, dando ao magistrado instrumento processual cautelar para a cessação de prática, induzimento ou incitação a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, permitindo que este determine a cessação das respectivas transmissões eletrônicas ou da publicação por qualquer meio.
> e. Determinou que os órgãos da polícia judiciaria estruturem setores e equipes especializadas no combate à ação delituosa, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivos de comunicação ou sistema informatizado;
> f. Determinou vacatio legis de 120 dias para a vigência da lei. (SYDOW, 2013, p.236).

O Projeto de Cássio Cunha Lima foi um dos pioneiros nesse certame a título nacional, e a despeito do desvio nas suas intenções, modificou pontos no Código Penal Militar ao mesmo tempo onde pediu por mudanças no até então ambiente onde poucos projetos haviam angariado sucesso.

3.3. PL N. 2.793-C/2011 OU LEI NÚMERO 12.737/2012

A Lei número 12.737 foi mais um dos efeitos que a pressão midiática pode ocasionar no legislativo. Resultado do vazamento de fotos íntimas de uma atriz brasileira, sendo que a obtenção das fotos veio de uma manutenção técnica em seu computador.

Essa lei advém do projeto realizado pelo deputado Paulo Teixeira, partidário do PT de São Paulo. Conhecido como PL n. 2.793-C/2011, sofreu algumas alterações antes de ser aprovado nas duas casas legislativas, seguindo para sanção presidencial em seguida. Apelidada pelo nome *"Carolina Dieckmann",* e assim o foi porque o caso de extorsão sofrido pela atriz brasileira criou apelo midiático suficiente para que o Projeto de Lei andasse mais rápido na Câmara Federal. Mas não retira seu mérito, visto que através dela surgiu o novo tipo delitivo nacional do qual os doutrinadores nacionais há alguns anos faziam apelo, os crimes cibernéticos.

Finalmente foi cominada uma pena aos delitos cometidos na esfera informática, sendo que a derrubada dos provedores pode ser punida com um a três anos, de acordo com o artigo 266. Vários são os pontos importantes para análise, principalmente as lacunas deixadas por ela - aqui o enfoque é analisar a primeira alteração realmente válida no Código Penal brasileiro acerca dos delitos virtuais.

Sobre a lei “Carolina Dieckmann”, ou 12.737/12, temos as principais observações de Spencer Roth Sydow (2013, p. 240):

> Criou o delito de invasão de dispositivo informático simples (art. 154-A, CP), criou uma figura assemelhada à da invasão simples de dispositivo informático, com mesma pena do caput para o partícipe do delito principal (ou praticante do delito de meio), impedindo sua punição em menor grau (art. 154-A, 1° do CP); criou uma causa de aumento específica para o delito de invasão simples em autoria ou participação para o exaurimento com prejuízo econômico (art. 154-A 2° do CP); criou uma modalidade qualificada de invasão de dispositivo informático (art 154-A, 3°, primeira parte, CP) pela obtenção de conteúdo sigiloso dos dados obtidos; criou uma modalidade qualificada de invasão de dispositivo informático (art 154-A, 3°, segunda parte, CP) pela obtenção de controle remoto não autorizado; criou uma causa de aumento específica para a invasão de dispositivo informático qualificada, com a divulgação, comercialização ou transmissão a terceiros dos dados obtidos; criou uma causa de aumento geral para os delitos simples e qualificado pela especial qualidade da vítima imediata do delito (basicamente, altos cargos públicos); determinou ser a ação penal pública condicionada a representação nos delitos com vítima comum e a ação penal pública incondicionada, nos delitos com vítimas especiais, no que se refere aos delitos de invasão de dispositivo informático; alterou o nomen iuris do delito do art.266 do CP para "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilizada pública", aumentando o rol dos crimes contra os serviços públicos; acresceu o delito de interrupção ou perturbação de serviço informático, interrupção ou perturbação de serviço telemático e interrupção ou perturbação de informação de utilizada pública; modificou o parágrafo da figura qualificada nos delitos de "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de utilidade pública", visto que determina que seja dobrada a pena caso a conduta ocorra em circunstância de calamidade pública; acresceu ao art. 298um parágrafo único, com o nomen iruis de

> "falsidade de cartão", equiparando-se a documento particular o cartão de crédito ou de débito.

Foi elaborado um texto dialogando sobre punição para os invasores de sistema, sendo que o delito de invasão do dispositivo informático simples encontra-se agora no artigo 154-A, CP. Dentre as implicações processuais penais, ela determinada espécie de pena cabível. Sua composição é de quatro artigos e teve entrada no ordenamento jurídico no dia 1° de abril, no ano de 2013. Alterou os artigos 298, 266 e 156 do Código Penal e possui diversas lacunas em sua redação.

A primeira delas é que no seu artigo inicial há o enfoque de que delitos informáticos serão dispostos. Contudo, o que se vê em seguida é a criação de apenas um delito, nesse caso a invasão de dispositivo informático.

> Art 156 - Subtrair o condômino, coerdeiro ou sócio para si ou para outrem, a quem legitimamente a detém, a coisa comum:
>
> Pena - detenção de seis meses a dois anos, ou multa.
>
> 1° - Somente se procede mediante representação.
>
> 2° - Não é punível a subtração de coisa comum fungível, cujo valor não excede a quota a que tem direito o agente.
>
> Art. 266. - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento.
>
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
>
> § 2° Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.
>
> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
>
> Pena - reclusão, de um a cinco anos, e multa.
>
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

A mudança no artigo 266 mostra um tipo de misto alternativo, porque independente do núcleo que seja cometido o crime, sendo isolado ou de forma cumulativa, serão indiciados no mesmo tipo penal.

> Apesar de delito dito comum, compreendemos que é necessária especial e elevada competência técnica, em muitos casos, para sua prática, especialmente no que se refere àqueles cometidos virtualmente e em face das comunicações informáticas. Assim, apesar de o agente não ser objetivamente qualificado, subjetivamente o é. (SYDOW, 2013, p. 242).

Nesse artigo a utilização de verbos a exemplo de "interromper, impedir e dificultar" omite a questão envolvendo a perturbação do serviço. Ainda que "perturbar" possa adentrar em "interromper" ou "dificultar". Sydow opina sobre perturbar ser tentativa de interromper. Além do quê, esse delito existe somente em seu modo doloso.

Ou seja, a infecção de vírus por meio involuntário do sistema que gere prejuízos, seria classificado como fato atípico. Máquinas utilizadas para fazer ataques e seus usuários também não serão responsabilizadas caso os ataques sejam feitos de modo involuntário. O bem jurídico aqui protegido pelo artigo 266 reformulado seria o serviço em si.

As brechas não param por aí, sendo que a adoção do termo "telemático" em exclusão do "informático" no inciso primeiro demonstra outro problema em sua redação. Isso porque telemática e informática divergem em seu significado. De acordo com o dicionário Aurélio:

> Telemática
> 1. Ciência que trata da manipulação e utilização da informação através do uso combinado de computador e meios de telecomunicação.
>
> Informática
> 1. Ciência que visa ao tratamento da informação através do uso de equipamentos e procedimentos da área de processamento de dados (q. v.).

Ou seja, telemática trata da gestão da informação e aplicação da mesma. Informática adentra no sentido da telemática, se você considerar que ela trata da comunicação à distância. Contudo, aqueles serviços informáticos que não adentrem na seara da comunicação ou não possuem repercussão a distância ficaram distantes do tipo penal, à exemplo dos softwares e hardwares.

Essa norma precisa de complemento para suprir as suas brechas, isso porque a precisão do conteúdo telemático não se encontra definido - ou seja, ele pode gerar debates e seria preferencial que houvesse pronúncia para impedir essa lacuna em branco deixada pela interpretação múltipla.

Opinião do estudo realizado é a de que a pena "um a três anos" passa por muito branda, visto os efeitos devastadores que uma invasão digital pode ter. Esse prejuízo iria de problemas econômicos para alta repercussão, fora que numa

empreitada de crime virtual muitas podem ser as vítimas indiretas. Um atrapalho telemático pode atrasar diversas contas com vencimento de data, além de outros cenários que podem surgir devido à falha na entrega da informação.

O judiciário ficaria impossibilitado de em casos concretos, aplicar em simultâneo o agravante do artigo 61, j e quarta figura do Código Penal, tal como seu parágrafo único do artigo 266. Adiante, temos a mudança no artigo 298 do Código Penal.

Esse artigo entrega um esclarecimento sobre a conduta de falsificação dos cartões de crédito ou débito ao mesmo tempo em que equipara ambos. O legislador, quando trata da falsificação de documentos, divide ambos entre os de documentos públicos e privados. Em algumas situações esses documentos são equiparados com alguns públicos, isso por conta do impacto de ambos na sociedade.

De tal modo, podem ser considerados de força pública usados no fim penal, a exemplo de livros mercantis e testamento particular, dentre outros. Documento público original, por sua vez, agrupa os documentos emitidos por funcionário público, ainda há a equiparação deles no artigo 297 do Código Penal, sendo que os demais documentos podem ser colocados no rol de particulares.

Portanto, a aplicação dos cartões de crédito e débito no elenco dos documentos privados exclui a dúvida envolvendo a aplicação do código penal nas ocorrências de falsificação, adulteração numérica, validade do cartão, assinaturas divergentes, dentre outras. Enfim, o legislador optou pela alteração da sua tipicidade para satisfazer os particulares que forem lesados pelos crimes nesse sentido.

Antes de aprofundar sobre os artigos 154-A e 154-B do Código Penal, segue redação:

> Invasão de dispositivo informático:
>
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1° Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

> § 2° Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3° Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4° Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
>
> § 5° Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I – Presidente da República, governadores e prefeitos;
>
> II – Presidente do Supremo Tribunal Federal;
>
> III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> IV – dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
>
> Art. 154-B Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

O verbo invadir encontrando na primeira estrofe designa à invasão, o acesso indevido, a entrada sem autorização. *Informatique* é uma palavra francesa, anacrônica entre *information* e *automatique*, sua primeira aparição sendo em 1962 por Philippe Dreyfus - ele aplicou tal nome para *Societé d'Informatique Appliquée,* uma empresa de sua propriedade. Esse termo se espalhou em múltiplos idiomas, quando as pessoas queriam se referir ao processamento da informação, tendo o nome informática depois de ser adotado também pelo castelhano.

De acordo com explicação de Rogério Greco em artigo, três são as tarefas que constituem o sistema informático: entrada, processo e saída. Na entrada é a etapa da aquisição dos dados, enquanto o processamento trata dos dedos, para finalmente na saída acontecer a sua transmissão. Lembrando que pode ser considerado aparelho informático todo aparelho apto a receber, transmitir, processar e modificar dados. *Tablets, smartphones, ipads, iphones,* computadores, etc.

O artigo 154 aponta a exigência de o dispositivo ser alheio, pertencer a outrem. Caso a pessoa consiga acessar as informações colocadas em seu aparato, ocorre a descaracterização do delito. Qualquer aparelho informático que esteja ligado ou não esteja conectado com a internet pode configurar fato típico caso seja

invadido, ainda em casos de computadores autônomos que troquem informaçõe entre si. Nesse sentido, Greco elucida sobre as redes mais famosas de computador:

> 1. LAN (Local Area Network) – redes locais, privadas, onde os computadores ficam localizados dentro de um mesmo espaço, como, por exemplo, uma residência, uma sala comercial, um prédio etc.; 2. MAN (Metropolitan Area Network) – redes metropolitanas, onde os computadores estão ligados remotamente, à distancias pequenas, podendo se localizar na mesma cidade ou entre duas cidades próximas; 3. WAN (Wide Area Network) – são redes extensas, ligados, normalmente, entre diferentes estados, países ou continentes, a exemplo do que ocorre com o sistema bancário internacional; 4. PAN (Personal Area Network) – são redes pessoais, presentes em regiões delimitadas, próximas umas das outras[1].

Conhecendo as principais redes, vale reforçar a independência da conexão online. Ou seja, caso seu computador esteja nas mãos de um estranho ou ainda conhecido, mas que entre no seu sistema de segurança protegido por senha sem que você disso tenha conhecimento, fornecido autorização tácita ou expressa, a pessoa incorre em desrespeito à lei. Lembrando-se da finalidade em destruir informações ou os demais elementos colocados na redação do artigo 154-A do Código Penal.

Esse trecho em peculiar incomoda, pois apenas os dispositivos que estejam protegidos por senha acabam configurando elemento condicionado para proteção. Entrementes, a ausência de senhas de forma alguma serve de escusa para conduta invasiva, sendo que o acesso das informações deve ser feito apenas sob autorização do proprietário.

O legislador foi redundante ao usar de "violação indevida", pois de acordo com a semântica, violação é por si só um ato indevido. Caso permissão houvesse, sua entrada teria autorização, perdendo a força de "violar". Reforça ainda o fato de que a mera conduta de intrusão, de acordo com a Lei 12.737, não forma conduta ilegal - sendo um crime de fim, não de meio. É preciso estar atento ao anseio de prejudicar, danificar ou obter vantagem ilícita. Mecanismos de segurança, quando citados, visam:

> Senhas, tokens, cartões de numeração, criptografia, esteganografia, impressão palmar, leitura de íris, todos são exemplos de métodos de

[1] GRECO, Rogério. *Comentários sobre o crime de invasão de dispositivo informático, art. 154-A do Código Penal.* Disponível em: <http://www.rogeriogreco.com.br/?p=2183> acesso em 18 jan. 2015.

> segurança para, simultaneamente restringir acesso alheio e certificar-se da permissão para uso e alteração, por parte de um usuário. (SYDOW, 2013, p. 250).

Visando o termo invasão e o que o legislador quis dizer com isso, imagina-se a hipótese onde o usuário cede temporariamente seu computador ou dispositivo eletrônico para que ele faça a devida manutenção no mesmo. Ao fazê-lo, é de praxe entregar sua senha para liberar o acesso. Portanto, no momento onde o cliente fornece de livre e espontânea sua identificação virtual, senha ou similar, o termo "invadir" perderá sua validade. Veja a justificativa do PL n. 2.793-C/2011:

> [...] apenas quando a conduta do agente estiver relacionada a determinado resultado danoso ou quando o objetivo do agente for efetivamente censurável e não se confundir com atividades legítimas da Internet, excluindo-se assim, mais uma vez, os casos de mero acesso a informações, ou os casos de obtenção de informações que, por sua natureza, não seriam passíveis de restrição de acesso.

Nesse texto contraditório, percebemos uma falha do legislador ao observar as minúcias digitais. Em primeiro lugar, não há precisamente a forma da autorização expressa ou tácita, muito menos o momento de verificação da mesma. De novo ele demonstra insensibilidade ao esquecer-se das formas compartilhadas de uso eletrônico, pois no Brasil ainda é bastante comum o uso de *lanhouses.*

Dentro de um computador, portanto, informações de várias pessoas estranhas entre si podem coexistir. Lembrando ainda das redes de computadores no ambiente de trabalho, que dividem a mesma rede. Ou seja, para o direito penal em seu caput do artigo 154-A, apenas o proprietário da máquina é titular para ação penal.

Ele assume a figura de vítima, por conta da titularidade - ainda em titular, se configura possuidor e aquele que goza do bem. Infelizmente a normatividade penal excluiu os demais usuários desse computador, limitando a relevância ao proprietário da maquinaria.

Outros levantamentos podem ser apontados, apenas a título de exemplo. Mas, caso um computador pessoal, desktop ou não, possua inúmeras contas diferentes sendo todas elas protegidas por senha? Caso alguém desse núcleo familiar ou habitual usuário do aparelho consiga a senha de suas contrapartes

obtendo assim, acesso ao material para fins de destruição ou algo ilícito, cairia ele em crime? A resposta é negativa, visto que o termo "alheio" é inaplicável, haja em vista a posse que ele compartilha.

De acordo com o artigo 154-A, vale reforço da lei:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Outro erro encontrado na eficácia da Lei 12.737/12 é a de que a obtenção da vantagem ilícita, de acordo com redação acima, ocorrerá em ilícita apenas e tão somente se tiver intuito de obter vantagem ilícita, ou seja, feita mediante "violação indevida de mecanismo e segurança". Ou seja, a informação obtida sem expressa autorização, caso o autor do crime não tenha usado de vulnerabilidade para tanto, acaba em branco penal.

Torna-se irrelevante. Ou seja, caso ele tenha acertado a senha que protege o sistema, continua em atípico penal. As brechas na interpretação literária desse dispositivo continuam. O emprego do plural em "instalar vulnerabilidades" abre espaço para entendimento de que o emprego de somente uma vulnerabilidade (exemplos de *trojan, keylogger, malware*) não configura o crime. O inciso primeiro aduz os seguintes termos, importantes a serem compreendidos para um melhor embasamento:

> Art. 154 – I. Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

Seu intuito foi o de punir aqueles que desenvolvam ou facilitem acesso aos programas cujo objetivo em particular, seja a invasão sistemática de aparato alheio - ou ainda, criar vulnerabilidades nele. Tais programas seriam na linha dos vírus, trojans entre outros. Aquele que auxilia, agora, ocupa o mesmo patamar de autor.

No parágrafo segundo do mesmo artigo, se encontra a causa de aumento da pena para um sexto a um terço caso a invasão resulte em prejuízo econômico. A

letra fria permite entender que se fala sobre pessoas físicas e jurídicas, sem detrimento de alguma em favor da outra. Acaba sendo aliviada a pena quando inexiste o prejuízo financeiro, ignorando a solidez de outros tipos de reveses que o consumidor ou usuário pode sofrer.

Existe ainda a ausência da definição desse "prejuízo econômico", anulando a base que poderia ser feita para cada caso isolado. De acordo com doutrina majoritária, ele permanece na Lei dos Juizados Especiais Criminais, permitindo assim os benefícios processuais e também que haja a substituição da pena por restritivas de direito.

Adiante, em seu § 3° temos:

> Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido.
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

É criada uma figura para qualificar a invasão dos dispositivos informáticos em penas mínimas e máximas acima daquelas do caput. Preza pela confidencialidade, visto que é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, de acordo com o artigo 5°, XII.

Informações sigilosas e comunicação eletrônica privada, no parágrafo supracitado, não se estendem apenas aos e-mails e demais correspondências eletrônicas. O doutrinador Sydow, em sua obra Crimes Informáticos estende ainda o rol para as de telefonia via internet, os arquivos de log para comunicadores instantâneos, registros e arquivos feitos por backup das correspondências sociais - existem diversos gêneros de comunicação virtual que aqui podem ser enquadradas e protegidas pela Constituição Federal.

No entanto, a compreensão de segredos comerciais fica por conta de De Plácido e Silva, na obra Vocabulário Jurídico (1967):

> [...] é a discrição ou a irrevelação de fatos concernentes aos negócios comerciais, conhecidos pela pessoa em razão de sua posição junto ao estabelecimento, em que os mesmos se promoveram, ou se firmaram. O

> segredo de comércio, pois, firma-se no negócio, na operação, na transação, ou em qualquer outro fato ocorrido em um estabelecimento mercantil, que não deve ser propalado, divulgado ou tornado público, desde que seu conhecimento deve ser restrito às pessoas que o sabem em virtude de suas funções, ou de suas funções no estabelecimento.

Enquanto isso, segredo industrial seria a guarda do segredo da criação de algum utensílio, dado, produto, ou diferente aparato produzido por uma indústria. E por informação sigilosa, teríamos a definição da Lei de número 12.527/2011:

> Artigo 4°. III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

Ou seja, quando o público não tiver acesso de uma determinada informação por conta da imprescindível máxima de proteger esta última, por conta da segurança e dos riscos que ela fornece para a própria sociedade ou Estado, teremos aqui a definição do artigo quarto, da lei 12.527/2011.

3.3.1. Ritos processuais envolvendo a Lei 12.737/2012

De acordo com o legislador, nas invasões informáticas atentando a administração pública, ou demais serviços considerados públicos, por associação a ação imposta será a penal pública incondicionada. Nos demais casos, ela estará condicionada à representação ou mesmo para a requisição do Ministro da Justiça. A interpretação jurídica transforma os dados informáticos em bens jurídicos disponíveis. O artigo 38 do Código de Processo Penal disserta sobre o prazo de seis meses.

Nesse artigo, tem-se que exceto disposição em contrário, o ofendido, ou seu representante legal, decairá no direito de queixa ou de representação, se não o exercer dentro do prazo de seis meses, contado do dia em que vier a saber quem é o autor do crime, ou, no caso do art. 29, do dia em que se esgotar o prazo para o oferecimento da denúncia.

De acordo com Spencer Roth em Crimes Informáticos, doutrinador da matéria, o prazo da prescrição de pretensão punitiva encontra-se assim:

> Considerando-se a pena máxima em abstrato do art. 154-A, caput, Cp: a prescrição ocorrerá em 4 anos (art. 109, V, CP); considerando-se a pena máxima em abstrato do delito do art. 154-A, caput, CP, com causa de aumento máxima (1/3): a prescrição também ocorrerá em 4 anos (art. 109, V, CP); considerando-se a pena máxima em abstrato do art. 154-A §3° do CP (figura qualificada: a prescrição também ocorrerá em 4 anos (art. 109, V, CP); considerando-se a pena máxima em abstrato do art. 154-A, §3° CP (figura qualificada), com causa de aumento máxima do §4° (2/3): a prescrição ocorrerá em 8 anos (art. 109, IV, CP); considerando-se a pena máxima em abstrato do art. 154-A §3°, CP (figura qualificada), com causa de aumento máxima do §5° (1/2): a prescrição também ocorrerá em 8 anos (art. 109, IV, CP); considerando-se a pena mínima aplicada em concreto, em qualquer dos delitos e em qualquer das hipóteses, seja com causa de aumento em grau mínimo ou máximo: a prescrição ocorrerá em 3 anos (art. 109, VI, CP).

Caberá o benefício da transação penal e ainda da suspensão condicional do processo, ainda antes de ser considerada a pena privativa de liberdade ou que restrinja o direito. A Lei 12.737/12, apesar de criada no intuito de atender a demanda não apenas da população, mas também da lacuna que ocorria no sistema jurídico brasileiro envolvendo matéria digital, mostra-se pífia no sentido prático. Isso porque o grau de condenação das reparações civis é mínimo, sendo esse dispositivo ainda capaz de desapontar no debate envolvendo qual será a competência habilitada para julgamento do caso.

3.4. O NOVO PROFISSIONAL DO DIREITO

O operador do Direito precisa estar conectado. Interligado, envolvido, disposto a aprender com o mundo que lhe cerca – ele deve ser um negociador nato. Passou do tempo onde o profissional do direito, seja ele qual for, precisava viver apenas no âmbito legalista. Conforme a sociedade se transformar, deve ser atrás dela – melhor ainda, à frente dela – que o Direito deve caminhar. As soluções apresentadas por aqueles detentores do exercício legal devem apresentar soluções que condizem com o paradigma contemporâneo.

E compreender o universo digital alavancado nas últimas décadas não é função das mais fáceis, pois a mesma induz para toda uma linguagem específica e interpretação singular. No mundo cibernético composto por softwares, faz-se mister entender pelo menos a sua linguagem básica no intuito de ser eficiente na resolução dos delitos que ocorrem nessa esfera. Suas transformações, no entanto, não ficam limitadas ao campo do pensar. Nenhuma forma de pensamento não exposta consegue atingir o outro, muito menos causar as transformações devidas.

Portanto, o exercício social tem que passar a trabalhar com a informatização. O Poder Judiciário deve caminhar como um todo para o “futuro”, que sequer pode ser considerado como tal, visto que se desenrola há tantos anos e se faz presente de forma massiva nos dias de hoje. Não se pode fazer vista grossa para a necessidade de mudança, sendo preciso dar valor para a informatização, ou até mesmo que o profissional seja educado em sua base – por que não o estudo virtual ser espalhado nas faculdades do país? Ou que eles ao menos detenham o mínimo de saber envolvendo a era digital.

Os tempos mudam e com eles são deixados para trás alguns problemas, dando abertura para o nascimento de outros. Determinados cenários antes nunca vistos faziam apenas do imaginário fictício e agora constituem a realidade.

Como trabalhar em cooperação internacional em crimes digitais? Qual a definição deles? E a questão territorial? Outrora separados por barreiras físicas, mapas, quilômetros de terra, agora estão ao nosso alcance a cada segundo. Um brasileiro pode causar efeitos drásticos numa companhia japonesa, sendo que ele está dentro do aconchego da sua própria casa, em algum lugar no interior do Nordeste. O direito de propriedade também mudou da informação, as barreiras estão sendo derrubadas.

Porquanto, o analfabetismo digital não pode, em hipótese alguma, ser tolerado por aqueles que supostamente deveriam transpassar segurança para a população. O Direito clama por profissionais capazes de acompanhar a velocidade do Novo Mundo, pede que ele tenha visão, implora para seguir lado a lado com a linguagem mundial. As relações pessoais mudam e muito em breve mesmo os escritórios de advocacia devem, além de terem já se informatizado, passarem da barreira física. Nesse sentido:

> [...] a American Bar Association, órgão equivalente à OAB nos Estados Unidos, que já autorizou a operação do site Lexuniversal (www.lexuniversal.com), que é uma rede que reúne 50.000 profissionais de renomados escritórios localizados em diferentes países. Criado pelo advogado brasileiro Ordélio Azevedo Sette, o site disponibiliza praticamente todos os serviços que podem ser prestados num escritório convencional, como uma consulta com advogados, e ainda desfruta das vantagens operacionais típicas dos negócios na rede, como a redução de custos e a celeridade. (PECK, 2013, p. 567).

Aludido texto demonstra a fluidez no sistema informático e como ele se adequa ao Direito em outros países, sendo que o Brasil deveria acompanhar de modo mais rápido. Mudanças positivas no âmbito do Direito Digital ocorreram nos últimos anos, contudo, se o problema também é estrutural ele deveria invocar mudanças nas Universidades.

A formação de profissionais encontra-se, na maioria dos ambientes acadêmicos, desatualizada. Existe um retrocesso ao ponto do legislador tentar dispor sobre trabalho remoto em sua Consolidação das Leis do Trabalho e acabar amputando o uso dos aparelhos eletrônicos, impedindo que o relacionamento profissional evolua conforme o social livremente faz.

Amplos os temas que ganharam adendos nos últimos anos e ainda se encontram com estudos escassos. O Direito Penal, Civil, Tributário, Trabalhista e tantos outros foram agraciados com novos elementos que precisam de enfoque e de um profissional qualificado. Segue o comentário de Patrícia Peck (2014, p. 568), que faz uma resolução:

> Finalmente, a sociedade digital exige que os profissionais do Direito deixem de lado algumas rivalidades acadêmicas para discutirem conjuntamente paradigmas como ordenamento, legitimidade e segurança no âmbito de uma sociedade globalizada, convergente, digital e em constante mudança. É essa postura que o mercado vai cobrar. É esta a nova postura que os profissionais devam adotar para poder atuar no âmbito de uma sociedade digital.

O trecho reforça o apelo em favor de novos profissionais, novas diretrizes e esquemas acadêmicos que permitam ao operador do Direito evoluir não somente em sua profissão, mas que ele também seja bem sucedido em acompanhar as maravilhas que a Era Digital proporciona, visto que seu clamor já passou de sentimento fugaz. Ele é real e precisa ser colocado em prática.

CONCLUSÃO

A tecnologia é o grande trunfo do novo mundo. Impossível ignorar as transformações nascidas dela, principalmente pelo fato de que a contemporaneidade parece circular ao seu redor – novas invenções nascem a cada dia, colocando-nos como testemunhas da reinvenção da medicina, das pesquisas, dos grupos sociais e midiáticos.

O Direito sempre foi consequência do meio, advém da necessidade pela regulamentação e segurança das pessoas que compõem a sociedade. No universo digital, foi-se criado um novo ambiente social, que merece o mesmo tratamento e sistema protecionista daqueles que circulam fora dele.

Buscou-se provar, que na *world wide web*, as redes se interligam de tal forma que a vida na rede abriu portas para uma *sociedade em rede* massiva, diariamente aprimorada com novos adeptos.

A identidade criada na esfera cibernética passou, em muitos detalhes, a lentamente substituir a atmosfera real; há migração constante dos bancos, das compras, do ciclo de amizades, na propagação de informações, etc. Do físico, o homem abraça os bits, o software, o novo hardware. E tomados pela facilidade desse mecanismo, criam de fato um mundo semelhante àquele outrora composto de organismos vivos.

Estudou-se que a fluidez, agora, é informática. Sob este ângulo, descartável o pensamento da internet ser um evento momentâneo – seu momento dura por décadas o suficiente para ser levado em consideração pelo Direito.

Historicamente, a mesma é um composto elitista e criada em benefício de cientistas cujo objetivo foi transmutando de acordo com a passagem dos anos.

O sistema computacional e de cyber rede, a priori fruto da Guerra Fria, perpassando disso para uma cadeia de comunicação entre usuários, e conforme ganhou aprimoramento gráfico passou a ser idolatrada pela comunidade de estudantes da tecnologia e deles para o mercado financeiro, econômico e de comunicação ao passo em que foi angariando mais adeptos.

Destarte, a informática trás consigo uma singularidade intrínseca. Para compreender melhor esse novo ambiente moderno, como é referido por muitos, primeiro é imprescindível entender da sua linguagem. O conceito e *modu operandi* diverge de tudo que conhecemos até então, sendo necessário ao operador de Direito e para o Estado, entender o que nele ocorre. No presente trabalho, mostrou-se as minúcias do processo de funcionamento da rede virtual.

Analisou-se que a internet permite a criação de uma nova identidade, mais perto do que se quer ser num mundo idealizado, quando protegidos pela esfera computacional os usuários podem projetar suas ânsias e opiniões enquanto envoltos por uma redoma de falsa proteção proporcionada pelo anonimato.

Foi o advento do estar anônimo e a capacidade de esconder seus rostos que impulsionou a migração da criminalidade para esse campo e estimulou os delitos cibernéticos. Quem comete delitos virtuais, em suma, poderá proteger sua identidade através dos mais variados métodos – cabe mais uma vez ao Direito, adaptar-se.

Buscou-se provar que é necessário estar um passo adiante, sendo primordial desmembrar os endereços eletrônicos; eles são o endereço postal online, recurso sabiamente utilizado no procedimento investigativo de crimes digitais. Os aparatos utilizados no processo também devem atender a demanda, sendo vital que as delegacias e demais alicerces de investigação estejam bem equipados e preparados – algo que foge da realidade brasileira, ainda despreparada para lidar com esses crimes em larga escala.

Ao redor do mundo, novos sistemas são desenvolvidos no propósito de facilitar o rastreamento de criminosos, contudo, infelizmente estes últimos possuem em sua grande maioria um vasto conhecimento da área e utilizam o mesmo para encobrir seus rastros e dar continuidade ao ciclo de rastreamento e fuga.

Ademais, uma nova gama de criminosos foi classificada de acordo com o aperfeiçoamento dos delitos virtuais, trazendo à tona um rol baseado na conduta praticada.

Supracitado método classificatório é relevante para o sistema penalista, e ainda mais importante é a compreensão dos novos crimes nascituros da tecnologia virtual. A nomenclatura de tais crimes é vasta, alternando de acordo com a doutrina:

pode ser apresentada por crimes mediante computadores, crimes tecnológicos, *high-tech*, da tecnologia da informação, dentre outros.

Ora, se tamanhas foram as mudanças geradas pela Internet, faz-se mister declarar a classificação dos crimes virtuais e investir no estudo destes, para que a engrenagem propulsora do direito e de proteção perante a criminalidade não seja danificada por conta dos progressos tecnológicos.

Juridicamente, medidas foram tomadas para discernir os espécimes de delitos virtuais, tendo o direito internacional auxiliado na diferenciação deles. Conforme uma nova modalidade surge, a mesma deve ser elencada no intuito de não se postergar as devidas medidas judiciais cabíveis.

O Brasil enquanto nação claramente atrasada na regulamentação do meio digital usou do direito comparado, adotou as classificações criadas mundo afora para esse meio novo no qual se insere – há uma tentativa de correr atrás do atraso, apesar da mesma ser tardia.

Doravante, o país precisa se incluir no acompanhamento de novas definições envolvendo territorialidade, identidade, indivisibilidade, responsabilidade e tempo; essas são apenas alguns dos conceitos usuais que foram afetados pela criminalidade de alta tecnologia.

O conflito envolvendo a informática e o Direito deve ser passado adiante, sendo superado por medidas legislativas e esclarecimentos doutrinários em nosso território. Com efeito, foram esmiuçadas algumas das leis nesse quesito, sendo inquestionável que existe tentativa de sanar o espaço em branco acumulado.

A Lei 12.737/2012 foi apenas o primeiro passo efetivo com repercussão midiática, sendo seguida pelo Marco Civil, e assim é esperado que muitos projetos de lei venham ocupar espaço na legislação nacional.

É preciso transcender positivamente no Direito, migrando para uma completa mudança na forma como encaramos os novos quesitos relacionados ao jurídico digital. Os aparatos tecnológicos advindos do século passado e que se perpetuam nesse, sendo refinados e constantemente evoluídos, trazem consigo a necessidade do profissional de Direito ter uma base sólida da matéria.

O arcabouço jurídico nasce ainda na universidade, retrocedendo um pouco mais, na escola – sendo assim, seria interessante que a educação viesse desses patamares. As universidades de Direito deveriam colocar em sua grade, ou

como objeto de estudo, se não o Direito Digital em si, no mínimo as eventuais consequências dele. Pois ele não é estudo unidimensional, envolvendo toda uma categoria de elementos sociais relevantes.

A Internet, portanto, serve de agente transformador. E como um, deve inspirar segurança, e para tanto é preciso que haja investimento em sua regulamentação, estudo e debate.

REFERÊNCIAS

BARBOSA, David Pimentel**.** *Lei Carolina Dieckmann e a definição de "crimes virtuais".* Disponível em: <http://jus.com.br/artigos/24406/lei-carolina-dieckmann-e-a-definicao-de-crimes-virtuais>, acesso em: 29 de julho de 2014.

BAUMAN, Zygmunt. *Modernidad líquida.* Tercera reimpresión, Argentina, 2004.

BRASIL. Decreto-Lei n° 12.737 de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> acesso em 02 de fevereiro de 2015

BRASIL. Decreto-Lei n° 12.735 de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm> acesso em 19 de jan. 2015

BRASIL. Projeto de lei n° 2.126 de 2011. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255> acesso em 19 de jan. 2015

BRASIL. Decreto-Lei n° 12.965 de 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> acesso em 23 de jan. 2015

BRASIL. Decreto-Lei n° 2.848 de 7 de dezembro de 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm> acesso em 28 de jan. 2015

BRASIL. Decreto-Lei n° 7.209 de 11 de julho de 1984. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/1980-1988/l7209.htm> acesso em 26 de jan. 2014

CASTELLS, Manuel. CARDOSO, Gustavo. *A Sociedade em Rede - Do Conhecimento à Acção Política.* Portugal, 2005.

CORRÊA, Gustavo Testa*. Aspectos jurídicos da internet.* São Paulo: Editora Saraiva, 2008.

Convention on cybercrime. Disponível em: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> acesso em 03 fev. 2014

CRESPO, Marcelo Xavier de Freitas. *Crimes digitais.* 1.ed. São Paulo: Saraiva, 2011.

CRUZ, Danielle da Rocha*. Criminalidade informática* – tipificação penal das condutas ilícitas realizadas com cartões de crédito. Rio de Janeiro: Editora Forense, 2002.

DE PLÁCIDO E SILVA. *Vocabulário jurídico.* São Paulo: Editora Forense. 1967.

FERREIRA, Marcelo Paulo. *Crimes de computador e segurança computacional.* Campinas: Millennium, 2006.

GIL, Antonio Carlos**.** *Como elaborar projetos de pesquisa.* São Paulo: Editora Atlas, 2009.

GOMES, Luiz Flávio. *Lei Carolina Dieckmann e sua (in)eficácia.* Disponível em: <http://jus.com.br/artigos/23897/lei-carolina-dieckmann-e-sua-in-eficacia> acesso em 29 jul. 2014

GRECO, Rogério. *Comentários sobre o crime de Invasão de dispositivo informático., art 154-A do Código Penal.* Disponível em: <http://www.rogeriogreco.com.br/?p=2183> acesso em 18 jan. 2015

JAPÃO. *Código Penal Japonês (Act No.45 of 1907)*. Disponível em: <http://www.cas.go.jp/jp/seisaku/hourei/data/PC.pdf> acesso em 30 de jan. de 2015.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. *Fundamentos de metodologia científica.* São Paulo: Editora Atlas, 2002.

LOJKINE, Jean. *A revolução informacional.* Tradução de José Paulo Netto. 3. ed. São Paulo. 2002

LIMA, Paulo Marco Ferreira*. Crimes de computador e segurança computacional.* 2. ed. São Paulo, 2006.

PECK, Patrícia Pinheiro. *Direito digital.* 5. ed. São Paulo: Saraiva, 2013.

REIS, Wanderlei José dos. *Delitos cibernéticos:* implicações da Lei 12.737/12. Disponível em: <http://jus.com.br/artigos/29647/delitos-ciberneticos-implicacoes-da-lei-12-737-12> acesso em: 29 jul. 2014

ROCHA, Carolina Borges*. A evolução criminológica do Direito Penal:* aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012. Disponível em: <http://jus.com.br/artigos/25120/a-evolucao-criminologica-do-direito-penal-aspectos-gerais-sobre-os-crimes-ciberneticos-e-a-lei-12-737-2012> acesso em 29 jul. 2014.

SPYER, Juliano. *Conectado* – o que a internet fez com você e o que você pode fazer com ela. Rio de Janeiro: Editora Zahar, 2007.

SYDOW, Spencer Toth*. Crimes informáticos e suas vítimas;* coordenadores Alice Bianchini, Ivan Luís Marques e Luiz Flávio Gomes. São Paulo: Saraiva, 2013.

WENDT, Emerson. JORGE, Higor Vinicius Nogueira. *Crimes cibernéticos* - ameaças e procedimentos de investigação. Rio de Janeiro, 2013.