ASSOCIAÇÃO CARUARUENSE DE ENSINO SUPERIOR

CENTRO UNIVERSITÁRIO TABOSA DE ALMEIDA

(ASCES-UNITA)

JORGE EDUARDO GOMES DE ARRUDA

CIBERCRIME NO ÂMBITO DAS RELAÇÕES EMPRESARIAIS:

A VULNERABILIDADE DAS EMPRESAS NO TOCANTE À IMPUNIDADE DO ORDENAMENTO JURÍDICO

CARUARU

2019

JORGE EDUARDO GOMES DE ARRUDA

CIBERCRIME NO ÂMBITO DAS RELAÇÕES EMPRESARIAIS:

A VULNERABILIDADE DAS EMPRESAS NO TOCANTE À IMPUNIDADE DO ORDENAMENTO JURÍDICO

Trabalho de Conclusão de Curso, apresentado ao Centro Universitário Tabosa de Almeida – ASCES-UNITA, como requisito parcial para a obtenção do grau de Bacharel em Direito.

Orientadora: Prof. Msc. Renata Lima Pereira

CARUARU

2019

SUMÁRIO

RESUMO

O presente trabalho visa demonstrar o grave problema que assola o ordenamento jurídico brasileiro, que é o sistema de combate e punição ao *cibercrime* nas relações empresariais. Para se chegar ao objetivo proposto, o trabalho descreve o surgimento da tecnologia propiciada pelo advento da globalização, que trouxe para a sociedade uma nova forma de se relacionar, através dos novos meios de comunicação e pelo advento da *internet*. O mundo dos negócios não ficou de fora, grandes e pequenas empresas passaram a incorporar a tecnologia em suas atividades, sendo hoje imprescindível para manter-se no mercado competitivo. Na medida em que a internet tenha propiciado aos empresários inúmeras vantagens, por outro lado, surge um grande problema, os criminosos que atuam auferindo ilicitamente vantagens através de invasões em sistemas dessas companhias. As leis existentes no Brasil não punem de forma eficaz o agente criminoso, o sistema probatório não dispõe de instrumentos e profissionais capacitados para enfrentar os crimes digitais nessa seara. Para tanto, utilizou-se a metodologia indutiva, a partir de uma análise do sistema jurídico brasileiro, da doutrina e da jurisprudência, bem como, pesquisas bibliográficas, com a finalidade de proporcionar informações precisas sobre o tema. Com o que é explanado no trabalho, fica clara a necessidade urgente de tratar de forma adequada o tema, e combater de forma eficaz os crimes cibernéticos, não levando-os a impunidade.

Palavras-chaves: crimes cibernéticos; internet; impunidade; relações empresariais.

RESUMEN

El presente trabajo pretende demostrar el grave problema que azota el sistema legal brasileño, que es el sistema de combate y castigo por delitos informáticos en las relaciones comerciales. Para alcanzar el objetivo, el trabajo describe la aparición de la tecnología proporcionada por el advenimiento de la globalización, que ha llevado a la sociedade una nueva forma de relacionarse, a través de los nuevos medios de comunicación y por el advenimiento de la internet. El mundo de los negocios no ficó de fuera, grandes y pequeñas empresas comenzaron incorporar la tecnología en sus actividades, siendo esenciales hoy para seguir en el mercado. En la medida en que la *internet* ha proporcionado muchos beneficios a los empresarios, por otro lado hay un gran problema, los delincuentes que actúan ilegalmente y que reciben beneficios a través de incursiones en los sistemas de estas empresas. Las leyes vigentes en Brasil no punen con eficácia el delincuente, el sistema probatorio penal no tiene instrumentos y profesionales capacitados para abordar los delitos digitales en este campo. Por tanto, se utilizó la metodología inductiva, de un análisis sobre el sistema legal brasileño, doctrina y jurisprudencia, así como la investigación bibliográfica con el fin de proporcionar informaciones precisas sobre el tema. Con lo que se explica en el trabajo, es claramente la necesidad urgente de tratar adecuadamente el tema y combatir de manera eficaz los crímines *cibernéticos*, no causando impunidad.

Palabras-claves: crímines cibernéticos; internet; impunidad; relaciones comerciales.

INTRODUÇÃO

O presente trabalho é voltado para o estudo na área das Ciências Humanas, abrangendo, nesse sentido, o enfoque sobre o Direito Empresarial. Serão enfatizadas as transformações tecnológicas ocorridas ao longo das últimas décadas, e que provocaram alterações na vida em sociedade. Essa evolução trouxe consigo o surgimento da internet, proporcionando ainda mais a comunicação entre os povos. Em meio ao crescimento desenfreado da globalização, as empresas precisaram aderir a esse novo instrumento, como forma de manter-se no mercado competitivo.

Diante da eclosão da tecnologia, as empresas passaram cada vez mais a utilizarem essa nova ferramenta, e hoje grande parte dessas companhias dependem da internet para concretizarem suas operações, sendo atualmente quase que obrigatório o uso desse mecanismo, pelo fato de facilitar a comunicação, armazenar informações, e agilizar os processos no ambiente de negócios. A informatização vertiginosa dos meios produtivos tem proporcionado benefícios aos empresários, ao passo que tem atraído olhares de indivíduos detentores de elevado conhecimento tecnológico, que utilizam desse instrumento para obter vantagens ilícitas, através de crimes cibernéticos, virtuais, digitais, informáticos, são inúmeras espécies de nomenclatura que caracterizam esse termo.

Esses criminosos agem utilizando o ambiente virtual para a prática de delitos. Atuam em campos diversificados, e um deles é no âmbito das empresas. Os crimes praticados dentro desse universo econômico, estão ligados, na maioria das vezes, ao roubo de dados de clientes, e também a invasão de dados sigilosos industriais *trade secret*, ou seja, violando o segredo da empresa. Neste último caso, os agentes se beneficiam através do fornecimento de dados para terceiros, que na grande maioria, são empresas concorrentes, que objetivam auferir lucro com as informações prestadas.

A espionagem industrial em casos como este, é vista como prática abusiva sob a ótica do Direito Empresarial, a concorrência desleal fica caracterizada pela quebra do sigilo empresarial, ocasionada pela divulgação de informações de caráter confidencial, inerentes a atividade desenvolvida.

Crimes dessa espécie têm crescido cada vez mais no mundo todo, e o Brasil tem se tornado um alvo fácil para a prática desses delitos. O registro dos *cibercrimes* aos órgãos policiais competentes, tem evoluído ao longo dos anos. E em grande

parte dos casos, a prática desses atos criminosos não são informados pelos empresários, que preferem na maioria das vezes ficarem silentes, para eles, preservar a imagem e reputação da empresa torna-se mais importante que punir esse tipo de conduta.

A impunidade nesse tipo de crime tem tornado o país um atrativo para os *hackers*, a superlotação carcerária brasileira tem favorecido a aplicação de penas alternativas e pouco eficazes pelo Judiciário. Como visto, esses agentes agem em um ambiente fechado, onde não há contato direto com suas vítimas, sem envolver qualquer tipo de violência ou sangue, fatores que fazem com que, esses indivíduos, em um primeiro momento não fiquem presos.

Na primeira seção, será abordada de maneira geral, a globalização e os avanços dos meios de comunicação, que propiciaram o surgimento da internet, como também será enfatizada a criminalidade através dos processos informáticos dentro das empresas, delitos que têm crescido vertiginosamente no mundo todo. Na segunda seção, será apresentada a ineficácia do ordenamento jurídico, no que tange à punição dos crimes informáticos no contexto das empresas, como também a falta de preparo dos agentes responsáveis pela investigação, fatores ligados à impunidade, quando se trata de *cibercrime*. Na terceira seção, serão delineadas algumas medidas de combate aos delitos dessa natureza, no que diz respeito ao aprimoramento da segurança em rede, e ao treinamento dos órgãos incumbidos pela investigação.

Para análise do tema em questão, serão utilizados minuciosamente a seleção de inúmeros artigos científicos, trabalhos acadêmicos, legislação e teorias concernentes à matéria. Os critérios de seleção dos artigos têm como base, a experiência dos estudiosos da área do direito da informática, que corroboram ainda mais com a explanação da problemática. Desse modo, a pesquisa bibliográfica de autores e especialistas, será um dos métodos utilizados para o desenvolvimento da pesquisa.

A partir da pesquisa bibliográfica serão confrontadas as questões trazidas pelos autores, interpretando em algumas situações e tecendo reflexões sobre o tema. As soluções para o grande problema, que tem grande relação com o estudo do direito, serão sem dúvida discutidas ao longo do trabalho, como também apresentação de alguns mecanismos que tornem o sistema jurídico brasileiro eficaz, quando se trata de *cibercrime* no contexto empresarial.

1 GLOBALIZAÇÃO E O AVANÇO DOS MEIOS DE COMUNICAÇÃO

1.1 Surgimento da internet e a criminalidade digital no âmbito das empresas

O fenômeno da globalização trouxe para a vida em sociedade grandes transformações, o desenvolvimento tecnológico foi um exemplo disso. A partir dessas modificações ocorridas ao longo das últimas décadas, surgiu o fenômeno da revolução informática, permitindo, dessa maneira que, informações sejam levadas e acessadas em qualquer extremidade do planeta em questão de segundos. Essa nova fase é denominada “Sociedade da Informação” (CHEVALLIER, 2009, p.35), e tem provocado inúmeras alterações, na perspectiva de Estado, Direito e Política.

> A sociedade da informação é determinada pela integração das tecnologias de informação (particularmente microeletrônica) e de comunicação à vida social, profissional e privada, junto com a percepção da informação como fator estruturante da sociedade e insumo básico de produção (intelectual, cultural e econômica) (LUCENA, 1998, p.87).

Assim, como alude o autor acima, a tecnologia hoje passou a integrar a vida das pessoas, sendo um mecanismo essencial, em todos os anseios da sociedade. Esse processo de informatização propiciado pelo fenômeno da globalização, fez com que surgissem novos meios de comunicação, e um deles foi a internet. Seu processo de evolução teve como marco, o contexto da Guerra Fria, onde a necessidade de trocas de informações, entre as forças armadas dos EUA e a segurança dos dados coletados, eram sem dúvida de extrema importância. (ABREU, 2009, p.2). O avanço da tecnologia, influenciada pela internet, permitiu que o envio de uma mensagem, pudesse ser realizado de forma quase que instantânea, possibilitando, dessa maneira, que indivíduos de qualquer parte do mundo, possam comunicar-se a partir de um equipamento interligado em rede.

Temis Limberger diz em seu artigo:

> Hoje em dia os computadores não estão mais isolados, mas sim interligados em redes, em conexão com outros computadores. Isso faz com que seus efeitos saiam de um âmbito restrito e sejam transmitidos globalmente e com uma velocidade ímpar, combinando os fatores de tempo e espaço. (LIMBERGER, 2006, p.250).

Para William Gibson, “*cyberspace* é um espaço não-físico, e composto por um conjunto de redes de computadores através dos quais circulam as formas mais

variadas de informações". (TANCMÁN, 2002, p.50). O distanciamento dos indivíduos através dessa barreira virtual torna esse meio favorável para usuários delinquirem, agindo em desconformidade com os princípios que norteiam a órbita jurídica.

Nessa linha de pensamento, conclui-se que o ciberespaço é um ambiente fictício, onde só há o acesso através de uma máquina, "[...] mesmo assim precisa estar ligado à realidade, pelo uso que temos feito dela nos dias atuais, transformando-o em um espaço intermediário entre o mundo imaginário e o mundo real", (PINHEIRO, 2009, p.2). Do mesmo modo, entende-se que, o ciberespaço mesmo não sendo uma entidade física concreta, deve ser notado como um ambiente imaginário, pois constitui-se em um espaço intermediário, a punição para aqueles que utilizarem esse meio para o cometimento de crimes, deve merecer o mesmo tratamento, não devendo ser afastado da proteção jurídica.

A globalização, assim como qualquer fenômeno, traz repercussões, tanto positivas, como também negativas. Mesmo com as inúmeras facilidades trazidas pelo incremento da internet, a utilização desse recurso tem atraído olhares dos mais diversos tipos de pessoas, dentre elas aqueles que utilizam a rede de computadores, para obterem benefícios ilícitos, perpetrando crimes das mais variadas espécies no ambiente virtual, entre eles delitos praticados no âmbito das empresas.

Como foi visto anteriormente, a internet, mesmo com suas vantagens, ainda acaba trazendo sérios problemas, principalmente àqueles que a utilizam como meio para adquirir recursos financeiros, em especial os empresários, dessa maneira tem se tornado um desafio para o direito, acompanhar essa evolução tecnológica, no que tange a responsabilização de delitos perpetrados nesse ambiente. A invasão de computadores, em especial às redes que conectam dispositivos em grandes empresas, tem tornado um atrativo, para uma infinidade de criminosos, espalhados pelo mundo todo, inclusive o Brasil, que utilizam dessa modalidade para roubar dados confidenciais nesse ambiente de negócios. Essa conduta criminosa é um dos reflexos negativos dessa inovação tecnológica. Assim como assevera Têmis Limberger em sua obra:

> A telemática, diferentemente da eletricidade, não transmite uma corrente inerte, mas veicula informação, e, quando corretamente utilizada, significa poder. Pode-se dizer que isso apresenta dois lados: primeiramente, uma vantagem propiciada pela informática, no sentido de armazenar o conhecimento e transmiti-lo de uma maneira veloz. Por outro lado, há o risco de que as liberdades sejam violadas,

> e tal possibilidade exige a intervenção do poder público, como forma de proteção dos indivíduos. (LIMBERGER, 2012, p.220).

O aumento de crimes nesse ambiente de negócios tem aumentado de forma exponencial, e o motivo está relacionado, ao crescente número de usuários que utilizam a internet. Para se ter uma ideia, mais da metade da população mundial, já conta com acesso à internet, segundo o site de pesquisas *Hootsuite e We Are Social,* no ano de 2018, o número de usuários atingiu a marca de 4,021 bilhões de pessoas online, o que é equivalente a 53% de todas as pessoas do planeta. (WWW.WEARESOCIAL.COM).

Como dito anteriormente, o desenvolvimento da criminalidade digital, sobretudo os crimes cibernéticos, têm aumentado de forma avassaladora nas últimas décadas, tornando o Brasil um dos países mais vulneráveis no contexto de invasões, dados comprovados pelo instituto de pesquisas em segurança de ameaças em rede, *Security Threat Report* Symantec. O número crescente de *hackers* tem, consequentemente, trazido prejuízos para empresas, e cidadãos numa ótica geral, fatores estes que, devem merecer a atenção do ordenamento jurídico pátrio, independentemente da conduta delituosa ter sido praticada na esfera virtual ou não, assim como assevera Vicente Greco Filho:

> Melhor pensando, porém, também concluí que nada existe de especial na possível proteção aos bancos de dados informatizados. Isso porque ou pertencem eles à esfera da intimidade ou à esfera da prática comercial ou industrial e nesses campos sua proteção, deve ser tratada, independentemente de a violação ocorrer por meio da informática. (GRECO, 2000, p.39).

Segundo o autor, nada impede que determinada conduta delituosa, mereça o tratamento jurídico adequado. Mesmo que a prática criminosa tenha sido realizada no ambiente físico, ou virtual. Percebe-se claramente uma diferenciação, no que tange o contexto fático da realização da conduta criminosa, mas mesmo em um ambiente em que, não há o contato direto com o outro indivíduo, onde essa relação dar-se-á, apenas por meio dos meios telemáticos, não deve ser um critério de diferenciação, para efeitos de punição daquele que pratica o ato.

A violação de dispositivos informáticos, precipuamente no âmbito das empresas, é uma prática que merece proteção do mesmo modo, que outros delitos previstos no ordenamento jurídico brasileiro.

No atual panorama sociológico global, é visto, a grande mudança dos paradigmas sociais, propiciados pela difusão dos novos meios de comunicação, e

que surgiram com o advento da globalização. A partir de então, percebe-se, a necessidade do aprimoramento do direito, no que concerne à proteção, daqueles que utilizam os aparelhos de informática no ambiente empresarial, e que hoje é quase que indispensável na vida em sociedade. Com isso, a finalidade de se evitar à impunidade dos chamados delitos informáticos.

> É de se notar, também, a importância que os sistemas informáticos possuem no atual momento social, ressaltando que a maioria das pessoas, físicas ou jurídicas, dependendo do seu dispositivo informatizado, que variam de um simples pendrive ou celular, até um computador com banco de dados sigilosos de uma empresa (BRITO, 2013, s.p).

É indiscutível, no contexto social atual, o distanciamento do direito, com essa categoria de delitos praticados, sobretudo em um universo não físico. Assim como o autor supracitado afirma, a necessidade dessa tecnologia na vida em sociedade, em especial no âmbito empresarial, merece proteção jurídica, em razão da vertiginosa criminalidade cibernética que assola esse ambiente corporativo.

1.2 Atividade empresarial em risco

Diante do acelerado crescimento da tecnologia, mais precisamente dos meios de comunicação modernos, tornou-se imprescindível a adaptação dos empresários às novas ferramentas. Nos dias atuais, é comum a utilização da informática nas grandes empresas, sendo quase que obrigatório que tais ambientes insiram esses mecanismos em suas instalações, seja para facilitar a comunicação, armazenar informações importantes, que muitas vezes estão relacionadas à própria atividade ali desempenhada, como também, agilizar processos no ambiente de negócios.

A busca pela competitividade é característica marcante no mundo capitalista, manter-se atualizado de novas técnicas, e aprimorar relações negociais, é permanecer vivo nesse mercado que, a cada dia, demanda inovações.

Em meio ao surgimento da globalização, esses ambientes de negócios, precisaram se adequar às novas tecnologias que surgiram. Alvin Tofler entende as dificuldades enfrentadas no tocante a esse contexto de mudanças, em que é preciso a sociedade adequar-se as novas formas de aprimoramento nesse ambiente empresarial, “[...] o mundo se movimenta mais rapidamente. Os executivos lamentam-se, porque não conseguem permanecer atualizados em relação às

novidades e ao desenvolvimento de suas profissões". Há um sentimento de inquietação geral, uma vaga desconfiança de que a mudança escapa ao controle (GEHRINGER 2002, *apud* TOFLER 1982, p.93).

Diante da informatização desse universo corporativo, inúmeros empresários se beneficiaram com as mudanças, mas não apenas eles, os criminosos também. A ideia que a globalização traz em seu bojo aspectos negativos, se confirma com o surgimento de uma criminalidade, que utiliza o espaço virtual para o cometimento de crimes. O rápido avanço dos novos meio tecnológicos é integrado rapidamente em toda a sociedade, inclusive por esses criminosos, que têm utilizado desses novos mecanismos, para a perpetuação de delitos no âmbito das empresas. A finalidade de invadir um computador de uma grande companhia, na maioria das vezes, é a obtenção de informações que estão armazenados em banco de dados, e a partir disso, auferir lucro com a invasão desses documentos, caracterizando dessa maneira a conduta ilícita do *cibercriminoso*.

Desse modo, crimes nessa modalidade são difíceis de punir os agentes causadores, e acabam também, na maioria das vezes, sem a tutela do Direito, ocasionando às empresas, prejuízos financeiros altíssimos. Da mesma maneira entende João Monteiro Neto, "[...] os crimes informáticos são difíceis de captar e contextualizar e podem acarretar danos tanto pessoais como empresariais" (LIBERATI 2009 *apud* MONTEIRO, 2010, p.02).

No tocante a esses crimes, perpetrados no âmbito das relações empresariais, influenciados pelo vertiginoso desenvolvimento tecnológico, permitiram que essas corporações agilizassem cada vez mais os seus processos. E a partir disso, passaram cada vez mais a depender de softwares, banco de dados e serviços online. Consequentemente, diante da utilização maciça da tecnologia nas atividades empresariais, essas relações ficaram expostas aos crimes virtuais, como também a tendência de serem visados.

A prática de delitos dentro desse universo econômico está associado, na maioria das vezes, ao roubo de dados de clientes e pela invasão de dados sigilosos industriais, os chamados *trade secrets*, ou seja, o *cibercriminoso* age violando o segredo da empresa, roubando dados que são de extrema importância para o funcionamento dos negócios que ali são empreendidos.

O cometimento de delitos dessa natureza tem crescido no âmbito das empresas, a prática de espionagem industrial tem sido alvo de *hackers,* que utilizam

da internet para realizar condutas ilícitas. Segundo Barral e Langelaan, a espionagem industrial surgiu pelo fato da real necessidade que é imposta pela feroz concorrência existente no meio industrial ou empresarial, nesse sentido afirmam que:

> Um comerciante ou industrial que nada saiba a respeito do mercado ou mercados que lhe interessem, da clientela que adquire seus produtos, de seus concorrentes – do que fabricam, dos processos que empregam, dos planos que fazem para o futuro, de seus novos produtos – da concorrência estrangeira e dos novos mercados possíveis, está fadada a falência, a curto prazo. Daí, a necessidade da espionagem. (BARRAL E LANGELAAN, 1971, p.17).

A espionagem industrial, na modalidade praticada através de invasão de dispositivo informático é vista sob a ótica do direito empresarial, como prática abusiva, caracterizando a concorrência desleal, quando a invasão tiver como finalidade beneficiar empresas concorrentes. “[...] Com relação ao crime de espionagem industrial, e no caso de espionagem industrial por meio de dispositivos tecnológicos denominada como espionagem eletrônica é, a obtenção de acesso às informações não autorizadas” (PINHEIRO; 2013, s.p.). Como visto anteriormente, o acesso ilegal aos dispositivos de informática dentro de empresas, é compreendido com uma prática ilícita. O acesso criminoso aos bancos de dados, é caracterizado a partir do momento em que, o agente infiltra-se por meio de ataques cibernéticos, como também, através de funcionários da própria empresa, que age presencialmente, através de um simples *pen driver.*

A prática delituosa de invadir computadores de companhias, como versado em momento anterior, recebe o nome de espionagem industrial. Atos como estes prejudicam a atividade empresarial e fazem com que essas empresas sofram prejuízos financeiros vultuosos, prejudicando na maioria das vezes a sua relação com o mercado financeiro. “[...] Neste sentido, o crime de espionagem industrial, o bem jurídico a ser tutelado é também a liberdade individual, porém sob o prisma de inviolabilidade de segredo profissional”. (ISHIDA, 2009, p.284). Em casos onde o *cibercriminoso,* pratica o ato com o intuito de auferir ganhos, favorecendo outras empresas concorrentes, estes recebem o nome de concorrência desleal.

Fábio Ulhoa, entende que:

> Incluem-se os espiões a distância (os chamados *hackers*), que se introduzem, sem autorização, nos bancos de dados informatizados das empresas, em busca de informações que possam ser negociadas com concorrentes desleais” (ULHOA, 2012, p. 295).

A ocorrência dessa prática ilícita no meio empresarial, também se configura a partir dos meios informáticos, não se restringindo apenas à modalidade presencial, afirma Fábio Ulhoa Coelho, “[...]espionagem econômica, mesmo realizada à distância, *hacking* é modalidade de concorrência desleal específica”. (ULHOA, 2012, p. 284). Em suma, a concorrência desleal é o tipo de conduta que tem como objetivo principal, prejudicar a reputação da empresa, ou os negócios alheios.

Outra modalidade de crime digital perpetrado nesse ambiente de negócios, é o denominado furto de tempo. Monteiro Neto diz que:

> O Furto de Tempo é a modalidade ilícita mais comum e mais difundida dos crimes informáticos. Ocorre o furto de tempo quando pessoas sem autorização utilizam-se de sistemas informáticos para fins particulares. Normalmente ocorre em empresas quando o funcionário sem possuir autorização para acessar a rede informática burla os sistemas de segurança e utiliza o computador e seus recursos para fins alheios aos interesses do empregador. O acesso não autorizado pode render ao infrator vantagens ilícitas como dinheiro e informações. (MONTEIRO, 2003, p.47).

Esse tipo de delito ocorre, na maioria das vezes, através de funcionários de grandes empresas, que utilizam do seu cargo para acessar dados sigilosos, com o intuito de auferir ganhos com a venda de informações. Esses dados confidenciais, como versado anteriormente recebem o nome de *trade secrets*, ou segredo do negócio, e estão atrelados à fórmulas, métodos de organização (lista de clientes, fornecedores), e modelo de mercado, que por ser mantido em sigilo tenha valor. Esse valor representa a vantagem que essa companhia tem no mercado, em virtude do seu segredo de negócio. Como visto acima, a violação de dados como estes na maior parte dos casos estão ligados, ao próprio corpo de colaboradores da empresa.

“O segredo é a alma do negócio”, expressão comumente utilizada nessas relações empresariais. O domínio da informação implica uma vantagem de competição nesse mercado capitalista. Práticas que visem à obtenção ilegal de informações devem merecer do Ordenamento Jurídico Brasileiro, proteção jurídica adequada, não levando condutas nefastas como estas, sob o sentido da impunidade.

2 SISTEMA PUNITIVO BRASILEIRO DOS CRIMES VIRTUAIS

2.1 Impunidade do *cibercrime* no cenário empresarial

O crescimento desenfreado de crimes cibernéticos perpetrados diariamente no Brasil, fez com que o direito se amoldasse a essa nova forma ilícita de violar dispositivos pessoais, em especial aqueles de utilização nas empresas. “[...] A globalização e seus avanços, assim como exigem das pessoas e da sociedade a alfabetização tecnológica, também exigem que o pensamento jurídico acompanhe tal evolução de modo que se possa a aplicar as normas de acordo com os contextos impostos” (PINHEIRO, 2013, s.p.). Como foi dito em momento anterior, na medida em que cresce o número de usuários e de conexões entre meios informáticos, cresce também a criminalidade, propiciada pelo anonimato ofertado pela rede, como também pela dificuldade de investigação no ambiente virtual.

> O direito deve se adequar à nova realidade, sob pena de perder seu verdadeiro papel, qual seja disciplinar as relações sociais e impor normas de conduta. Assim o binômio Direito e Internet não constitui fenômeno passageiro. Trata-se de uma realidade ainda pouco explorada, mas que deve ser analisada sob todos os campos das ciências jurídicas, a fim de garantir novos direitos fundamentais, bem como a efetivação dos já existentes. (FIORILLO, 2016, p.16).

No cenário atual, tem se tornado um grande desafio para o ramo do direito, acompanhar o surgimento de uma nova criminalidade. Os delitos virtuais praticados dentro das empresas são marcados pelo anonimato do agente criminoso, que se esconde através de um computador, ou dispositivo semelhante para auferir vantagens e causar grandes prejuízos financeiros a essas companhias, sendo desta maneira um dos fatores que levam à impunidade dessa espécie criminosa.

> O Direito em si não consegue acompanhar o frenético avanço proporcionado pelas novas tecnologias, em especial a Internet, e é justamente neste ambiente livre e totalmente sem fronteiras que se desenvolveu uma nova modalidade de crimes, uma criminalidade virtual, desenvolvida por agentes que se aproveitam da possibilidade de anonimato e da ausência de regras na rede mundial de computadores. (PINHEIRO, 2009 *apud* DULLIUS, 2012, s.p.).

Ao longo das últimas décadas, o legislador pátrio vem, de certa maneira, tentando qualificar esses crimes, mas percebe-se que a legislação vigente ainda se mostra insuficiente, no que tange ao combate de crimes virtuais. Desse modo, cabe aos estudiosos do Direito, e pesquisadores da área da informática, o trabalho para a

evolução da dogmática criminológica, segundo uma nova realidade mundial, para que o mundo virtual não venha a se transformar em um universo paralelo, onde as regras disciplinadas pelo direito não atinjam alcance algum.

O direito brasileiro tem incorporado diversos dispositivos que disciplinam a matéria. O crescimento alarmante de condutas relacionadas a invasões e roubos de dados de sistemas de empresas, fizeram com que surgissem debates acerca da referida problemática, e consequentemente a criação de novos meios legais para coibir tais condutas. Uma delas foi o surgimento da Lei 12.737/2012, mas conhecida como a Lei Carolina Dieckmann, que juntamente com o Código Penal, e o Marco Civil da Internet 12.965/14 regulamentam os crimes cibernéticos praticados no âmbito dessas empresas.

A Lei Carolina Dieckmann 12.737/2012, é confusa e pode gerar dupla interpretação, ou mesmo interpretação subjetiva, o que pode ser utilizado para enquadramento criminal de condutas triviais ou mesmo para a defesa e respaldo de infratores cibernéticos, o que a tornaria injusta e ineficaz. (PEREIRA, 2017, s.p.).

> A Lei não pune a invasão. “O hacker que invadiu o celular da atriz norte-americana, Scarlett Johansson, pode pegar até 10 anos de cadeia, aqui no Brasil, em ação semelhante, o cibercriminoso não vai para a cadeia. No máximo vai pagar “cestas básicas” (CAPANEMA, 2013, s.p.).

No tocante ao dispositivo supramencionado é perceptível o seu caráter pouco inibidor. As condutas relacionadas a invasões de dispositivos informáticos no interior das empresas não tem merecido destaque relevante, quando se fala em punir determinado agente delituoso. A redação do dispositivo além de ter sido elaborado de maneira confusa, as penas previstas para crimes como estes são bastante brandas, fazendo com que na grande maioria dos casos fiquem impunes.

Outro dispositivo que também surgiu mais recentemente, e que versa sobre a matéria discutida, é o Marco Civil da Internet, Lei 12.965/14. Essa nova legislação também tem recebido duras críticas dos estudiosos da área do Direito da Informática. Para que haja o fornecimento pelos provedores de rede, de dados relacionados ao *cibercriminoso,* como por exemplo, o IP *Internet Protocol*, que é o endereço do dispositivo utilizado para praticar o delito, deve haver representação judicial. Diante disso, barreiras são criadas, burocratizando a aplicação de uma possível pena, e prejudicando ainda mais o ofendido.

A impunidade continua sendo um atrativo para os *hackers*. Devido ao grande problema carcerário do Brasil, o poder judiciário tem aplicado penas alternativas aos agentes de delitos como estes, fazendo com que os números de invasões de dados importantes das empresas, cresçam a cada dia mais, elevando o país a um patamar crítico quando se fala em cibercrime no contexto empresarial.

A justiça brasileira vem lentamente oferecendo alternativas para o combate ao *cibercrime*, a criação de novos dispositivos legais não tem surtido efeitos no ordenamento jurídico. “[...] O Direito, sobretudo o Penal, com as ferramentas que dispõe hoje, não está totalmente preparado para fazer frente aos desafios do desenvolvimento cibernético e à criminalidade digital”. (SCHIETTI, 2017, s.p.). Assim como entende Rogério Schietti Cruz, Ministro do Superior Tribunal de Justiça, a ausência de preparação, principalmente no meio jurídico, tem ocasionado a deficiência na aplicação de medidas inibidoras de crimes dessa espécie.

Desse modo, conclui-se que o Brasil não carece de novas leis para que a justiça tenha caráter efetivo, basta que as já existentes sejam cumpridas e aplicadas integralmente. Há um caráter pouco efetivo das penas atinentes ao *cibercrime* no âmbito empresarial. Para os juristas, a condenação daqueles que praticam condutas nesse meio virtual, na maioria das vezes, são enquadradas nos procedimentos dos Juizados Especiais, fator que tem contribuído para a não eficiência no combate ao crime cibernético no Brasil, e revelando a ineficácia do sistema jurídico pátrio ao punir o *cibercriminoso.*

2.2 Despreparo dos órgãos de investigação

A investigação probatória tem início com base nas evidências colhidas, assim como ocorre no meio físico. Nos casos onde há a prática de delitos virtuais, essas provas poderão ser retiradas através de qualquer dispositivo eletrônico, seja ele um aparelho celular ou mesmo um disco rígido de um computador. Quando se fala em investigação de crimes digitais no âmbito das empresas, é visto que há um rigor maior no que diz respeito ao procedimento, pois nesse meio há facilidade em adulteração de dados, devendo, dessa maneira, as provas eletrônicas passarem por perícias técnicas, a fim de garantir a validade e obtenção de dados claros e precisos.

Emeline Piva, diz que:

> A impunidade dos criminosos virtuais é uma conseqüência mais da fragilidade das informações de rastreamento do que da falta de legislação específica. Pela natureza da Internet, com seu ciberespaço, é muito difícil fiscalizá-la. O transito de dados é livre e veloz, é instantâneo, e como todas esses dados são traduzidos em bits, facilmente manipulados pelos experts, a prova da conduta ilícita é frágil. (PIVA, 2006, p.26).

A prática desses delitos se caracteriza pela dificuldade em sua comprovação, o *cibercriminoso* está presente em um espaço não físico, o que dificulta a obtenção de provas, exigindo assim qualificação técnica específica nem sempre disponível, e que demanda do poder judiciário pátrio um arcabouço probatório mais encorpado, a fim de garantir que tais condutas criminosas sejam imputadas de forma célere aos verdadeiros agentes delituosos. Mas a realidade do ordenamento jurídico brasileiro é outra, não há ainda um sistema que atue dessa maneira.

> No tocante a atuação da polícia em crimes de computação, crimes dessa natureza requer investigação especializada e ação efetiva. Infelizmente, não existem no Brasil policiais preparados para combater esse tipo de crime, faltando, pois, visão, planejamento, preparo e treinamento (MIRANDA, 2013, s.p.).

No Brasil, o sistema utilizado para investigação de crimes nessa modalidade ainda é muito precário, a falta de equipamentos, pessoas devidamente capacitadas para tal cargo, e a pouca efetividade da legislação existente, contribuem para que os crimes digitais nessa modalidade se alastrem em ritmo desenfreado. A falta de especialização de profissionais para atuarem em casos envolvendo invasão de dados de empresas, é um problema marcante. “[...] No Brasil, no âmbito da polícia civil, existem poucos Estados que possuem delegacias especializadas na investigação de *cibercrimes*”. (COLLI, 2010, p.170). Atualmente, segundo o Portal do Instituto de Defesa Cibernética (IDCIBER), existem apenas onze delegacias especializadas no combate aos crimes virtuais, são elas Espírito Santo, Goiás, Mato Grosso, Minas Gerais, Pará, Paraná, Rio de Janeiro, Rio Grande do Sul, São Paulo, Sergipe e no Distrito Federal. As delegacias especializadas na área ainda são poucas, comparado a quantidade de delitos que ocorrem diariamente, e as que existem operam com dificuldades, não dispondo de profissionais suficientes,

responsáveis para investigar tais crimes digitais.

A punição do *cibercriminoso* no Brasil tem se mostrado inoperante, o grande problema da investigação, legislação pouco eficaz e o anonimato do agente delituoso, são sem dúvida fatores que contribuem para impunidade e faz com que esses delitos aumentem cada vez mais no país. A ausência de identidade física nesse ambiente favorece o anonimato eletrônico, o que demanda uma modificação de postura pela qual o Direito analisa os fenômenos pessoais dentro dessa seara.

Dessa maneira, o direito brasileiro necessita de uma postura mais atenciosa quando se fala em crimes informáticos.

3 MEDIDAS DE COMBATE AOS CRIMES VIRTUAIS

3.1 *Cibercrime* Empresarial: um desafio para o direito moderno

O avanço desenfreado da tecnologia trouxe para o cenário empresarial um novo meio de intensificar relações negociais. Como já foi abordado em linhas anteriores, esse processo vertiginoso não só abarcou pontos positivos, como também negativos, ao passo que a realidade virtual tem atraído indivíduos motivados a perpetrar delitos em consequência dessa nova realidade.

O direito moderno tem acompanhado lentamente essas modificações sociais, ao passo que a velocidade da tecnologia tem sido cada vez mais superior, não tendo preparado as pessoas nem tampouco os juristas para lidar em suas atividades com esses avanços. “[...] A *Internet* mudou, quer para o bem quer para o mal, a forma como os juristas interagem com a informática e as redes eletrônicas”. (MAGALHÃES, 2001, p.292). Diante da rapidez que essas mudanças acontecem, o legislador e os estudiosos do Direito digital não têm acompanhado as várias ameaças que surgem diariamente no país, fator que tem contribuído paras as lacunas presentes quanto a este tema.

A partir disso, é necessário que o Estado moderno avance nesse sentido, dando tratamento jurídico adequado a essa nova realidade a qual se vivencia, dando respostas céleres com o objetivo primordial de punir de maneira eficaz aqueles que utilizam os novos meios de comunicação para a prática de atos ilícitos, sobretudo no meio empresarial.

“[...] Vários países assumem hoje a *Cibersegurança* como missão prioritária”. Para tal, aprovam documentos estratégicos que não só traçam o quadro de ameaças em curso como definem os meios e os bens/instalações a proteger”. (PEREIRA, 2012, p.43).

O Brasil ainda está engatinhando quando se fala em *cibersegurança* no contexto abordado*,* há uma legislação tímida, tratando de maneira ineficiente, bem como os debates e palestras, ainda há um longo caminho a percorrer. Há uma necessidade de leis mais sintonizadas com a realidade, não basta apenas criá-las, mas deve haver uma rigidez mais significativa nesse cenário.

O que tem contribuído ainda mais para que crimes como este aumentem cada vez mais é o baixo grau de informação, sobretudo dos empresários acerca dos riscos impostos pelos crimes digitais. O Estado não investe em campanhas educativas, assim como a educação sexual, cidadania e direito do consumidor, o direito digital necessita de uma atenção maior, pois vivemos em uma era digital. “[...] A população brasileira não está adaptada e devidamente orientada em relação aos problemas de segurança virtual, necessitando de campanhas oficiais e direcionadas aos problemas existentes e sua prevenção”. (WENDT, 2011, p.24). O Brasil apresenta uma falha muito grande nesse sentido, não oferece a conscientização adequada, fator que contribui para o aumento dos delitos. Reforçar a cooperação ente Estado e entidades, é, sem dúvida, uma medida eficaz no combate ao *cibercrime.*

O *e-commerce,* uma nova modalidade de realizar compras através de um computador tem sido um dos reflexos desse processo de informatização, milhares de empresas passaram a comercializar seus produtos através da internet possibilitando aos consumidores, um novo meio para adquirir produtos, e que estão disponíveis em plataformas online. “[...] O comércio eletrônico é a realização de toda a cadeia de valor dos processos de negócio num ambiente eletrônico, por meio da aplicação intensa das tecnologias de comunicação e de informação”. (ALBERTIN, 2010, p.2). A partir do aprimoramento nesse ambiente de negócios, surgem diversos problemas para as companhias, que disponibilizam seus produtos no comércio digital, e que estão associados na maioria das vezes, ao roubo de dados de clientes, espionagem de senhas de cartões de crédito, entre outras fraudes perpetradas no âmbito dessas empresas.

Segundo a Confederação Nacional da Indústria (CNI), o silêncio das empresas ao terem sofrido algum tipo de invasão, ocorre principalmente em grandes redes de varejo que comercializam seus produtos online, como também em instituições financeiras. Essas corporações na maioria das vezes preferem ficar silentes, com receio de perderem a confiança dos consumidores.

> A maioria das empresas virtuais que sofrem invasões não denuncia a ocorrência, haja vista que os dados furtados são de seus 'clientes' e muitas vezes serão utilizados por terceiros sem que estes percebam, pelo menos até que algo pior ocorra (...). Alguns têm medo de tornar a ocorrência pública por temerem que haja dano à marca, que passaria a imagem de ser insegura perante o universo dos consumidores (PINHEIRO, 2011, p. 187).

O que tem contribuído para que isso ocorra, é a falta de um regulamento mais amplo que obrigue essas empresas a informar sua clientela sobre os riscos causados. O país deve ampliar uma discussão política sobre o tema, não se calar perante esse grande problema, e enfrentar esse desafio.

3.2 Aprimoramento do processo investigatório

Como já foi dito em momento oportuno, a característica marcante de delitos informáticos praticados dentro das empresas, é a dificuldade de buscar provas, necessitando de um esforço maior dos órgãos incumbidos pela investigação probatória.

> Enfim, somente a elaboração de leis, decretos e manuais de conduta não trarão grandes resultados no combate aos crimes de informática. O aperfeiçoamento dos meios de investigação, o progresso técnico dos profissionais ligados à área da persecução, a melhor formação e treinamento dos auxiliares da Justiça e a conscientização constituem elementos essenciais a coibir práticas desonestas no mundo virtual. (MALAQUIAS, 2012, p.65).

O Brasil enfrenta grandes dificuldades quando se fala em preparação de profissionais para lidar com crimes dessa espécie, a escassez de recursos técnicos e de agentes preparados, focados no exame pericial, e investigação, é evidente. "[...] A criação de divisões especializadas em computadores, mídias e meios de comunicação poderia ser um dos caminhos a serem seguidos para a resolução de algumas questões ligadas aos *cibercrimes*". (COLLI, 2010, p.167).

Atuar na prevenção dos crimes digitais, e investir em medidas de segurança é sem dúvida, essencial no combate ao *cibercrime,* assim como afirma Vera Elisa:

> A prevenção do crime informático deve, assim, ser feita tanto pelas empresas através da tomada de consciência do problema e da imprescindibilidade das medidas de segurança, como pela informação às potenciais vítimas das técnicas de manipulação e seu encobrimento. (DIAS, 2010, p.22).

O Brasil não tem acompanhado de forma adequada o processo de informatização, levando em consideração o campo do direito digital, a legislação se mostra insuficiente, como já visto anteriormente, sua tipificação legal acaba deixando aqueles agentes delituosos sem a punição adequada, recebendo penas brandas e pouco inibidoras. A escassez de recursos tecnológicos contribui para a não captação de condutas criminosas, e faz com que haja uma descrença dos empresários ao querer informar as autoridades policiais tornando as denúncias de crimes como estes, cada vez mais distantes da realidade. Diante desse grave problema, os cibercriminosos continuam agindo sem medo algum, motivados pela impunidade marcante que rodeia o ambiente virtual. O país precisa oferecer especialização, bem como treinamento adequado, e criar mais delegacias especializadas responsáveis por investigar tais crimes, sendo que hoje a quantidade desses policiais é bastante reduzida, não sendo suficiente para apurar as condutas ilícitas praticadas diariamente, medidas que poderiam minimizar a impunidade marcante nesse cenário empresarial.

CONSIDERAÇÕES FINAIS

A internet tem desempenhado um papel importante na sociedade moderna, o desenvolvimento dos meios de comunicação, e o acelerado processo de globalização trouxeram para a vida das pessoas, uma mudança cultural, e o mundo dos negócios precisou adaptar-se a essa nova forma de interação. A expansão digital experimentou um amplo crescimento nos últimos anos, e fez com que os crimes cibernéticos surgissem em variadas espécies, uma dessas foi dentro do contexto empresarial, e tem causado a essas companhias, prejuízos financeiros vultosos.

Atualmente, o ordenamento jurídico brasileiro possui uma grande dificuldade quando se fala em *cibercrime*, a legislação pune de forma branda aqueles que praticam condutas ilícitas no âmbito das pequenas e grandes empresas.

O incremento da tecnologia tem um papel primordial no ambiente de negócios, ao passo que tem favorecido a infiltração de agentes delituosos, que atuam nesse campo a fim de tirar algum proveito. Invadindo dispositivos informáticos, a fim de auferir alguma vantagem, com o roubo de dados, que na maioria das vezes pertencem ao sigilo da empresa, os chamados *trade secrets*, informações relacionadas a fornecedores, clientela, processos e padrões industriais, e que são considerados segredos comerciais. Esses agentes comercializam esses dados na maioria das vezes, com empresas concorrentes, que acabam se beneficiando com as técnicas empresariais, antes mantidas sob o segredo. O roubo de dados de clientes em empresas que comercializam seus produtos na *internet* também tem sido o alvo dos *cibercriminosos*, estes atuam em fraudes relacionadas a clonagem de cartões de crédito, como roubos de senhas, e documentos pessoais. Diante disso, essas corporações acabam sendo prejudicadas, pelo fato da impunidade do Estado no combate aos crimes digitais.

A informação acerca dos riscos inerentes à utilização das novas tecnologias é um dos fatores que necessitam ser amplamente discutidos no Brasil, levando em consideração a utilização em massa dos novos meios de comunicação. O Estado deve, através de campanhas, orientar sobre os riscos que assola o ambiente de negócios. A necessidade de aperfeiçoamento no combate ao *cibercrime* no âmbito das relações empresariais é, sem dúvida, de extrema importância. Sobretudo investir em áreas como investigação, bastante precária nesse sentido, e que corroboram ainda mais para o aumento dos crimes digitais, nesse campo tão importante para os negócios.

Como visto antes, as normas existentes no Brasil não são suficientes para punir condutas danosas que ocorrem na internet, precipuamente dentro das empresas, o país necessita de um amadurecimento quando se fala em crimes digitais. Deste modo, para que os crimes cibernéticos não permaneçam em silêncio, e que não favoreça a reiteração desses criminosos no Brasil, devem ser realizados investimentos em tecnologias para captar a ocorrências dos crimes digitais, bem como políticas de incentivo e proteção do Estado, e o treinamento de peritos da área da informática, são medidas que facilitariam o combate ao *cibercrime* no país.

REFERÊNCIAS

BARRAL, Jean: LANGELAAN, Geroge. **Espionagem Industrial**. Rio de Janeiro: Expressão da Cultura,1971.

BRITO, Auriney. **Análise da Lei 12.737/12 — Lei Carolina Dieckmann.** Disponível em:<http://politicacidadaniaedignidade.blogspot.com.br/2013/04/analise-da lei1273712-lei-carolina.html> Acesso em: 09 Ago.2018.

CAMPANEMA, Walter.**Lei Carolina Dieckmann é ineficaz em casos de espionagem.** Disponível em: <http://www.covergenciadigital.com.br/cgi/gilua.exe/sys/star.htm?UserActiveTemplate=site&infoid+35305&sid+18>. Acesso em: 09 Ago.2018.

CHEVALLIER, Jacques. **O Estado pós-moderno.** Tradução de Marçal Justen Filho. Belo Horizonte: Fórum, 2009.

COELHO, Fábio Ulhoa. **Curso de Direito Comercial**. Vol.1. 16 edição. São Paulo: Saraiva, 2012.

COLLI, Maciel. **Cibercrimes.** ***Limites e perspectivas à investigação policial de crimes cibernéticos*****.** Curitiba: Juruá Editora, 2010. Disponível em: <http://www.ub.edu/geocrit/sn/sn-170-36.htm> Acesso em: 08 Ago.2018.

DULLIUS, Aladio Anastácio. **Dos crimes praticados em ambientes virtuais**. 2012. Disponível em: <http://www.conteudojuridico.com.br/artigo,dos-crimes-praticados--em--sourcecrimesemambientes-virtuais,38483.html>. Acesso em: 09 Ago. 2018.

FIORILLO, Celso Antonio Pacheco. **Crimes no meio ambiente digital e a sociedade da informação.** 2 edição. São Paulo: Saraiva, 2016.

GEHRINGER, Max. **Não aborde seu chefe no Banheiro**, Rio de Janeiro: Campus, 2002.

GRECO, Vicente Filho. Algumas observações sobre o Direito Penal e a internet. **Boletim IBCCrim**, São Paulo, n. 95, 2000. Disponível em: <http://editorarevistas.mackenzie.br/index.php/rmd/article/view/4811/3692>. Acesso em: 08 Ago.2018.

ABREU, Karen Cristina Kraemer, **História e usos da Internet**, Disponível em: <http://www.bocc.ubi.pt/_esp/autor.php?codautor=1625>. Acesso em: 09 Ago.2018.

LIBERATI, Maria José Crepaldi Ganancio. **Crimes Informáticos**, Disponível em: <http://intertemas.unitoledo.br/revista/index.php/ETIC/article/viewFile/2148/2333> Acesso em: 08 Ago.2018.

LIMBERGER, Têmis. Transparência Administrativa e Novas Tecnologias: o Dever de Publicidade, o Direito a ser Informado e o Princípio Democrático. **Revista de Direito Administrativo**, Rio de Janeiro, v. 244, jan. 2007. ISSN 2238-5177. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/42471>. Acesso em: 08 Ago.2018.

LIMBERGER, Têmis; SALDANHA, Jânia Lopes. Cibercidadania no mundo globalizado: o desafio das novas tecnologias e a concretização dos direitos humanos nas democracias contemporâneas. **Anuario de Derecho Constitucional Latinoamericano**, Bogotá. 2012. ISSN 1510-4974. Disponível em: <http://www.corteidh.or.cr/tablas/r29676.pdf>. Acesso em: 08 Ago.2018.

LUCENA, Carlos José Pereira; CAMPOS, Ivan Moura; MEIRA, Silvio Lemos. **Ciência e tecnologia para a construção da sociedade da informação no Brasil.** Brasília: CNPq/IBICT, São Paulo: Instituto UNIEMP, 1998.

MAGALHÃES, José, ***Homo S@piens, Cenas da Vida no Ciberespaço***, Quetzal Editores, Lisboa, 2001,

MALAQUIAS, Roberto Antônio Darós. ***Crime Cibernético e Prova – A investigação criminal em busca da verdade***. Curitiba: Juruá Editora, 2012.

MIRANDA, Marcelo Baeta Neves. **Abordagem dinâmica aos crimes via Internet .** Jus Navigandi, Teresina, a.4, n.37, dez.2013. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=1828>. Acesso em: 09 jun. 2018.

MONTEIRO, João Neto. **Aspectos Constitucionais e Legais do Crime Eletrônico**, Disponível em:<http://www.dominiopublico.gov.br/download/teste/arqs/cp055676.pdf

PEREIRA, Júlio, **Cibersegurança, O Papel do Sistema de Informações da República Portuguesa, in *Segurança e Defesa***, Revista Trimestral, n.º21, Maio-Agosto 2012,

PEREIRA, Débora Anne da Silva. **Crimes Digitais**, Minas Gerais, 2017. Disponível em <https://www.adrianoedeboraanne.com.br/crimes-digitais/>. Acesso em: 08 Ago. 2018.

PINHEIRO, Emeline Piva. **Crimes virtuais: uma análise da criminalidade informática e da resposta estatal.** Porto Alegre: PUCRS, 2009. Disponível em: <http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2006_1/emeline.pdf>. Acesso em: 08 Ago. 2018.

TANCMAN, Michele. A (Ciber) Geografia das Cidades Digitais. 2002. Dissertação (Mestrado em Geografia) – **Revista Electrónica de Geografia y Ciencias Sociales Universitat de Barcelona,** Rio de Janeiro, v.8. ago.2004. ISSN: 1138-9788.

WENDT, Emerson. **CIBERGUERRA, INTELIGÊNCIA CIBERNÉTICA E SEGURANÇA VIRTUAL: alguns aspectos.** Disponível em: <http://www.abin.gov.br/conteudo/uploads/2018/05/RBI6-Artigo2-CIBERGUERRA-INTELIG%C3%8ANCIA-CIBERN%C3%89TICA-E-SEGURAN%C3%87A-VIRTUAL-alguns-aspectos.pdf> Acesso em: 22 Set.2018.