CIBERCRIME

CYBERCRIME

Herivelton Rezende de FIGUEIREDO[1]

Resumo: O presente trabalho analisa o cibercrime sob a perspectiva da sociologia sistêmica caracterizando seus atores sociais, a fragilidade do ciberespaço que se serve do anonimato para cometer crimes que lesam diversos bens jurídicos, quebrando a confiança no uso da informática como meio seguro de troca de dados de forma a demandar políticas que visam gerenciar esses riscos a níveis aceitáveis e no caso de falha da segurança, então aplica-se o Direito Penal.

Palavras-chaves: Criminologia; Direito Penal; Cibercrime.

Abstract: *This paper analyzes cybercrime from the perspective of systemic sociology characterizing their social actors, the fragility of cyberspace that serves anonymity to commit crimes that harm many rules, shattering confidence in the use of computers as a means of secure data exchanges to demand policies to manage these risks for acceptable levels and when failure of security, then applies the Criminal Law.*

Keywords: *Criminology; Criminal Law; Cybercrime.*

1. INTRODUÇÃO

Inicialmente partimos para o estudo dos papéis sociais que formam a cultura do ciberespaço, sendo elas: os hackers, usuários da rede informática e empreendedores. A manutenção desta nova realidade depende da confiança na segurança da instituição, por isso os riscos devem ser tutelados pelo Estado.

[1] *Bacharel em Direito pela UCDB. Mestrando em Ciências Jurídico-criminais pela Universidade de Lisboa. Escrevente Técnico do TJ/SP; dreptu@ig.com.br.*

Logo, o Direito Penal desempenha um importante papel não somente de repressão, mas também de prevenção geral negativa ao criminalizar determinadas condutas que ameacem ou quebrem os princípios básicos do ciberespaço que são a confidencialidade, integridade e disponibilidade. Neste aspecto, a Convenção do Cibercrime possibilitou uma repressão e prevenção uniforme aos perigos causados pelo uso indevido do sistema de informática entre os Estados europeus e também serve de inspiração aos demais países para legislarem acerca do tema, contribuindo desta forma para delimitar os parâmetros de um conceito operativo de cibercriminalidade de âmbito global.

Por fim procuramos demonstrar como as instituições públicas e privadas previnem os ataques no ciberespaço e caso falhem temos o instituto repressivo do Direito Penal.

Com isso esperamos oferecer uma visão da cibercriminalidade dentro do contexto sociológico, preventivo e repressivo, de tal forma que possibilite uma visão interdisciplinar deste novo fenômeno, suas estratégias de prevenção e a contenção desse problema.

2. A SOCIEDADE NA ERA DA INFORMAÇÃO

Oportuna a observação de Gidens:

> Muitos defendem que, hoje em dia, nos finais do século XX, nos encontramos no início de uma nova era, que as ciências sociais devem questionar a qual nos estará a levar para além da própria modernidade. Tem sugerida uma variedade estonteante de termos para designar esta transição alguns dos quais se referem positivamente à emergência de um novo tipo de sistema social (tais como "sociedade da informação", ou " sociedade de consumo"), mas cuja maioria sugere, antes, que um estado de coisas precedentes se aproxima do fim ("pós-modernidade", "pós-modernismo", "sociedade pós-industrial", "pós-capitalismo", etc.). Alguns dos debates sobre estes temas concentram-se principalmente nas transformações institucionais, em particular aqueles que sugerem que estamos a deslocar-nos de um sistema baseado no fabrico de bens materiais para um mais centrado na informação[2].

A globalização é um processo de conexão entre diferentes contextos sociais ou regiões que se ligam em rede através de toda a superfície da Terra. Neste

[2] *GIDENS, Anthony. As consequências da modernidade. 2005, P. 1.*

contexto, a internet é um dos instrumentos mais poderosos na sociedade dado sua capacidade de distribuir a informação alterando a noção de tempo e espaço. Com ela, temos acessos a diferentes versões do mesmo fato de acontecimentos distantes e uma maior participação política (as redes sociais como facebook pressionam o governo, mostram a tendência de consumo, etc).

Segundo Castells[3], uma maior flexibilidade, eficácia na realização de tarefas e tomadas de decisão coincidiu com as necessidades de uma economia globalizada, valores da liberdade individual e da comunicação aberta.

É neste contexto que se desenvolve a cultura hacker que é o terreno no qual se originam inovações servindo de ponte entre os projetos empresariais e a sociedade; não são em princípio pessoas sem escrúpulos que pretendem criar desordem no meio informático, são responsáveis, por exemplo, no desenvolvimento do software livre. Enquanto a cultura hacker proporcionou os fundamentos tecnológicos da internet, a cultura comunitária (utilizadores da rede informática) configurou seu uso social, de modo a tornar o âmbito da internet tão diverso e contraditório quanto a própria sociedade tornando a comunicação horizontal e livre para qualquer pessoa encontrar seu próprio destino na rede para criar e publicar sua própria informação.

A partir dos anos 90, a internet foi configurada para uso comercial de forma a dar um impulso vertiginoso a sua expansão. Possibilitou vender ideias aos possuidores de capital de risco que transformam-nas em empresas, que depois de criada vendem aos investidores por meio da venda pública de ações em bolsas de valores. Os empreendedores da internet baseiam-se no seu know-how tecnológico para criar produtos e serviços que vão conquistar o mercado. Assim, temos nesta cultura empreendedora uma composição de pessoas organizada em rede sendo investidores, tecnólogos e capitalistas de alto risco. Se os Estados são os atores no âmbito da ordem da política global, as empresas são os agentes dominantes da economia global.

Como se observa neste cenário, a confiança não é investida em indivíduos, mas na capacidade abstrata. É uma forma de fé na segurança de que os resultados prováveis exprimem um algo a mais do que um entendimento cognitivo de forma a garantir uma expectativa. Isso não se trata apenas dos empreendedores da internet, mas de todos esses novos atores sociais. Este novo princípio orientador da modernidade está relacionado com a ausência de tempo e espaço, pois não haveria necessidade de confiar em alguém ou no sistema se fossem continuamente visíveis, conhecidos e entendidos.

O impacto da tecnologia substitui a ideia de sorte para o conceito de risco e perigo dentro de padrões institucionalizantes da estrutura circundantes da confiança

[3] *CASTELLS, Manuel. A galáxia internet: Reflexões sobre internet, negócios e sociedade. 2007, p. 16.*

(transações financeiras, operações com cartões de crédito pela internet, investimento em ações, etc.), ou seja, deve ser conscientemente calculado. A segurança consiste em um equilíbrio entre confiança e o risco aceitável.

As instituições modernas se encontram ligadas a mecanismos de confiança, em especial nos sistemas técnicos, ou seja, sempre que alguém levanta o dinheiro do banco ou acende uma luz reconhece implicitamente amplas áreas de ações e acontecimentos coordenados e seguros que tornam possível a vida social moderna.

Nessa sobreposição de cultural forma-se um novo ambiente social no qual governo e sociedade convergem para criar uma nova doutrina de segurança necessária para controlar hackers hostis que podem efetuar ataques de maneira individual ou em grupos de especialistas capazes de escapar à detecção ou contra-ataque. Temos a *noopolitik* (ambiente global de informação, que inclui o ciberespaço e todos os outros meios de comunicação) em oposição à *realpolitik* que é a tradicional postura do Estado por meio da negociação, uso da força ou potencial uso da força que se configurou para responder aos fluxos de informação de modo a prevenir não tão somente os crimes, mas também os conflitos políticos e sociais criando alianças subjacentes a opinião pública e ao comportamento político coletivo.

3. A CIBERCRIMINALIDADE

A internet não é um campo neutro. Está cheia de vírus, worms, crackers que atravessam firewalls e roubam números de cartões de crédito, ativistas políticos que desativam e alteram os sítios da web e arquivos de computadores com informações confidenciais são posta em circulação na web.

O ataque de qualquer ponto da rede de computadores revelou a impotência das formas tradicionais de controle policial baseado nos poderes do Estado dentro de suas fronteiras nacionais. Isto faz com que a confiança no sistema fique ameaçada levando a cabo um esforço dos governos para atuar no novo espaço global de ação policial. A reunião do G-8 em junho de 2000 foi o início da ação para uma regulamentação e controle policial fazendo eco no Conselho da Europa que formulou uma Convenção contra o cibercrime.

A inovação tecnológica permitiu melhorar a produção de documentos falsos graças ao aprimoramento do software e da impressão, por isso, segundo Helena Carrapiço[4], o conceito de cibercrime refere-se a um conjunto específico de crimes relacionados com a utilização de computadores e de redes informáticas. Portanto, temos um conceito operativo, que não está ligado diretamente a um determinado bem jurídico, o que permite dividir o cibercirme em dois tipos de criminalidade: a informática como alvo da criminalidade, como por exemplo, alteração de dados

[4] *CARRAPIÇO, Helena. O crime organizado e as novas tecnologias: uma faca de dois gumes. Nação e Defesa, 2005, 181.*

no sistema (trata-se da criminalidade informática em sentido próprio); ou ataque a outros bens jurídicos utilizando-se da informática, por exemplo, falsificação de documentos (trata-se da criminalidade informática em sentido impróprio).

Contudo, para Castells[5] o que se verifica com a criação do cibercrimes é uma tentativa de neutralizar o poder de encriptação que está nas mãos ampliando de forma considerável o poder do governo nas escutas telefônicas e de tráfico de dados obrigando os fornecedores de serviços da internet a instalar técnicas de identificação dos utilizadores dentro de um espectro de situações e circunstâncias muito amplo e vagamente definido. Logo, primeira vítima desta regulamentação global é o próprio Estado que reduzirá sua soberania ao partilhar a informação e a segunda vítima é a liberdade (privacidade) em detrimento da segurança.

O nível de repressão pode variar segundo o grau de liberdade de cada país. Por exemplo, o consumo legal de marijuana na Holanda por um cidadão norte-americano pode ser denunciado ou punido (mediante leis) nos Estados Unidos como consequência da vigilância conjunta da distribuição de drogas[6] ou que o fato de ser gay em alguns países constitua um delito punível e a vigilância sobre as salas de chat trará graves consequências para estas pessoas. A grande questão é que a ideia de vigilância permanente pode resultar na dificuldade em prever as consequências dos nossos comportamentos expostos, que dependem dos contextos de interpretação e dos critérios utilizados para julgá-los, podendo tornar um governo mais autoritário e repressivo em nome do princípio da confiança no sistema.

Com a devida *vênia*, pensamos que a existência de um ciberespaço é um fato atrativo para o criminoso pelo pouco risco que acarreta ao praticar uma ação a grande distância e pela comodidade de poder colher grandes frutos em pouco tempo ao abrigo da dificuldade de detecção e investigação deste tipo de crime que, por não ter fronteira, exige uma cooperação internacional. Além disso, lesam não tão somente o Estado, quanto os indivíduos. Assim poderão integrar nesta categoria desde a difamação na blogesfera até o acesso ilegítimo.

Segundo Helena Carrapiço[7] podem ser identificados três tipos principais de cibercrime: atividades contra indivíduos, contra a propriedade e contra o Estado.

O primeiro gênero diz respeito principalmente à pornografia infantil com a proliferação de sites da internet contendo imagens e vídeos de crianças, especialmente com a evolução dos sistemas de pagamento eletrônicos que permitem cada vez mais manter o anonimato do comprador e fornecedor, além disso, possibilita o aliciamento de menores através das salas de conversação de virtuais; o tráfico de mulheres para a prostituição forçada ou até mesmo a escravatura. Os crimes contra indivíduos podem incluir ainda extorsão, roubo de dados, fraude e o assédio, podendo ser realizadas facilmente pela internet ou correio eletrônico.

[5] *CASTELLS, Manuel. Op. Cit., p. 212.*
[6] *CASTELLS, Manuel. Op. Cit., p. 214.*
[7] *CARRAPIÇO, Helena. Op. Cit., p.182.*

O roubo de dados dos cartões de crédito consiste em uma tentativa de se fazer passar por uma entidade bancária, pedindo à vítima determinadas informações para reestruturar o sistema informático. Trata-se da prática do *phishing*, o meio pelo qual ocorre o roubo de identidade digital[8] como ato preparatório para crimes mais graves. Consiste em uma reprodução de uma página da *web* que pode ser de uma entidade governamental ou de um banco, de forma que peça à vítima que se identifique, introduzindo seus códigos confidenciais. Pode ser usado também o *pharming*[9] que utiliza métodos da difusão de um vírus (*worms*) via *spam* nos correios eletrônicos em ficheiros ocultos que se instalam nos computadores das vítimas para alterar os ficheiros de "favoritos" e registro de cookies para que, quando a vítima ao aceder o seu habitual site bancário, o sistema desloca-o para outro site idêntico ao original e dessa forma obtém os dados.

O segundo tipo trata-se do vandalismo informático, que consiste na propagação de vírus susceptível de danificar os computadores e os sites da internet visados, além de constituir uma ameaça à economia global, minando a confiança pública no comércio eletrônico e nas novas tecnologias em geral. A interceptação de dados relaciona-se com os desvios de informações comerciais e crimes financeiros em geral praticados contra empresas.

Os Estados também podem ser vítimas de vandalismo, fraude ou interceptação de dados. Podemos citar o caso brasileiro alvo de ataque dos hackers no site governamental brasileiro com o fim de praticar vandalismo realizado no dia 22/06/2011:

> O ataque hacker às páginas da Presidência da República, Portal Brasil e da Receita na madrugada desta quarta-feira (22) foi o maior já sofrido pela rede de computadores do governo brasileiro. De acordo com o Serviço Federal de Processamento de Dados (Serpro), o ataque - que não causou danos às informações disponíveis nas páginas - partiu de servidores localizados na Itália. Para derrubar os sites, os hackers utilizaram sistemas que faziam múltiplas tentativas de acesso ao mesmo tempo, técnica batizada de "negação de serviço" e conhecida pelas iniciais em inglês DDoS (DistributedDenialof Service). O objetivo dessa ação é tornar o serviço indisponível. A ação foi reivindicada pelo grupo LulzSecBrazil, que teria ligações com o LulzSec, responsável por ataques recentes a empresas de videogame como Sony e Nintendo, às redes de televisão americanas

[8] Em um mundo digital temos pessoas digitais, isto é, uma compilação de dados para identificar os indivíduos visando com que as empresas conheçam seus clientes e facilitar o e-commerce, contudo uma quebra de dados pode fornecer informações pessoais e financeiras para contribuir com a prática de fraudes (VIANO, C. Emilio. 2007/2008, p. 37.)

[9] VERDELHO, Pedro. Phishing e outras formas de defraudação nas redes de comunicação, 2009, p. 415.

> Fox e PBS e a órgãos governamentais americanos como a CIA (agência de inteligência americana) e o FBI (polícia federal), além do serviço público de saúde britânico, o NHS. Nos ataques a sites do governo brasileiro, foram mais de 2 bilhões de tentativas de acesso em um curto período de tempo. Entre as 0h30 e 3h as páginas ficaram fora do ar por causa do ataque, mas entre a 0h40 e 1h40 foi o período de maior concentração dos ataques e o sistema ficou congestionado[10].

Conforme notícia da Europol:

> O valor da economia cibercriminosos como um todo ainda não é conhecida, uma estimativa recente de perdas globais das empresas é de cerca 750 mil milhões de euros por ano. Este negócio é apoiado por uma infra-estrutura de códigos maliciosos e hackers, web especializadas e redes alugadas de milhares de computadores comprometidos que realizam ataques automatizados online, para acesso e roubar dados pessoais. Grupos cibercriminosos muitas vezes não têm liderança óbvia, mas divide o trabalho de acordo com habilidades técnicas, com a maioria dos membros apenas sabendo-se mutuamente online. Portanto, fóruns online são ferramentas essenciais para a economia digital subterrânea para recrutar e fazer as apresentações, permitindo que os criminosos trabalhem juntos em projetos específicos. Nestes fóruns também ensinam o seu ofício através de tutoriais. As habilidades de alta tecnologia necessária significa que os envolvidos em crimes cibernéticos raramente se encaixam no perfil tradicional dos grupos de crime organizado transnacional[11].

Desde 1990 às Nações Unidas estão estudando o fenômeno do crime informático que é cometido por um vasto leque de pessoas: estudantes, amadores, terroristas e membros de grupos do crime organizado. O que os distingue é a natureza do crime cometido e o nível de habilidade para cometê-los. Qualquer pessoa de idade variada, com um mínimo de habilidade, motivado pelo desafio técnico, potencial ganho de notoriedade, ou vingança, ou promoção de crenças ideológicas, é um potencialcriminoso em computador. Uma série de estudos concluiu que os funcionários representam a maior ameaça. Um estudo estimou que 90 por cento dos crimes informáticos econômicos foram cometidos por funcionários das empresas

[10] Informação disponível em: <http://g1.globo.com/tecnologia/noticia/2011/06/ataque-hacker-foi-o-maior-ja-sofrido-por-sites-do-governo-na-internet.html>. Acessado em 09/01/2012.

[11] Informação disponível em: <https://www.europol.europa.eu/content/press/cybercrime-business-digital-underground-economy-517> Acessado em 09/01/2012.

vítimas. Uma recente pesquisa na América do Norte e na Europa indica que 73 por cento do risco para a segurança do computador foi atribuída a fontes internas e apenas 23 por cento para a atividade criminosa externo[12]. Mas, com os avanços continuam a ser feitos em processamento de dados remoto. A ameaça de fontes externas irá provavelmente aumentar, logo o perfil do criminoso marcha para a mudança.

Somente em 2005, a partir do XI Congresso das Nações Unidas sobre Prevenção ao Crime e Justiça Criminal[13] o cibercrime tornou-se um dos enfoques de destaque da ONU que reconheceu a importância crítica de responder eficazmente ao desafio de criminalidade informática, observando em especial a sua diversidade de infrações abrangidas por ele. Observaram que o crescimento do comércio eletrónico (e-commerce) aumentou drasticamente as possibilidades de exploração criminosa. Considerou também o impacto da criminalidade informática em vítimas individuais, em especial o impacto da fraude e da exploração sexual.

Já no XII Congresso das Nações Unidas sobre Prevenção ao Crime e Justiça Criminal[14] reconheceu-se que no atual período de globalização, a tecnologia da informação e do rápido desenvolvimento das telecomunicações e novos sistemas de rede de computadores têm sido utilizados para fins criminosos. Assim, saudamos esforços para melhorare complementar a cooperação existente para prevenir, investigar e reprimir o crime de alta tecnologia e de informática, incluindo o desenvolvimento de parcerias com o setor privado. Destacaram a importância das Nações Unidas nos fóruns regionais e internacionais de luta contra a cibercriminalidade de modo que convidam a Comissão de Prevenção ao Crime e Justiça Criminal, para analisar a viabilidade da prestação de assistência adicional na área, sob a égide das Nações Unidas, em parceria com outras organizações igualmente concentrada.

Para resolver os problemas e desafios em torno de cibersegurança e cibercriminalidade, a Organização das Nações Unidas Conselho Econômico e Social (ECOSOC) realizou um evento especial sobre "Segurança Cibernética e Desenvolvimento[15]", organizado conjuntamente pelo Departamento de Assuntos Econômicos e Sociais (DESA) e da União Internacional de Telecomunicações (ITU) em 9 de Dezembro, em Nova York. De acordo com um dos documentos produzidos no evento[16] a preocupação não é apenas com a divulgação falsa ou enganosa de informação, mas acima de tudo com conteúdo malicioso, roubo, fraude e falsificação. Se os usuários estão a beneficiar de todas as vantagens da Internet, então a confiança no sistema é fundamental e de extrema importância.Contudo, a infra-estrutura complicada da Internet torna mais difícil rastrear os criminosos,

[12] Disponível em: <http://www.ictparliament.org/node/2128>. Acessado em 29/05/2012.

[13] Disponível em:<http://www.un.org/events/11thcongress/declaration.htm>. Acessado em 29/05/2012.

[14] Disponível em: <http://www.un.org/News/Press/docs/2010/soccp349.doc.htm>. Acessado em 28/05/2012.

[15] Disponível em: <https://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html>. Acessado em: 28/05/2012.

[16] Disponível em: <http://www.un.org/en/ecosoc/cybersecurity/itu_cybersecurity_overview.pdf>. Acessado em: 04/04/2013

considerando, ainda, que eles não são as únicas ameaças à Internet, sendo um chamariz para terrorismo e espionagem. Ciber-guerra e espionagem podem representar sérias ameaças à infraestrutura de informação crítica.

Brechas em marcos legais estão sendo exploradas por criminosos, e a harmonização entre as leis existentes está longe de ser satisfatória. Juntamente com a falta de organização adequada.Mesmo considerando queas medidas nacionais estão sendo tomadas, as ameaças cibernéticas permanecem um problema internacional, por isso merecem uma solução global.

4. PREVENÇÃO NO CIBERESPAÇO: CIBERSEGURANÇA

Para minimizar os riscos que a internet apresenta surgiu uma variedade de tecnologias de controle: identificação, vigilância e investigação[17]. Por seu turno, isso funciona orientados por três princípios básicos: a confidencialidade, integridade (autenticidade) e disponibilidade.

A primeira garante que somente as pessoas autorizadas tenham acesso a informação, o segundo princípio integridade refere-se a proteção do sistema contra alterações de quem não está autorizado a fazê-lo e a terceira garante que os programas e dados estão acessíveis a quem legitimamente queira usá-los.

As tecnologias de identificação incluem o uso de passwords e cookies que são marcadores digitais da *web* gravando os movimentos on-line realizados no computador, sendo a autenticação a garantia de identificação certa do usuário que em geral funcionam por níveis. Por exemplo, um dos primeiros protocolos de segurança na internet foi o SSL, introduzido pela Netscape e usado por consórcios de empresas emissoras de cartões de crédito e comércio eletrônico.

As tecnologias de vigilância também se baseiam nas tecnologias de identificação para poder localizar o utilizador individual, mas interceptam mensagens e colocam marcadores que permitem seguir os fluxos de comunicação a partir de um determinado computador e controlar a atividade da máquina dia e noite. Isso permite que os governos possam obter dos servidores da internet a identidade de um potencial suspeito de crime. Temos como exemplo: ECHELON[18] utilizado para a espionagem realizada via satélite sobre sistemas de comunicação feita por telefone, fax, internet ou e-mail criado por meio da cooperação entre Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia, o que representa uma possível ameaça à privacidade e às empresas, não somente porque é um sistema de monitoramento poderoso, mas também pelo fato de operar à margem da lei, não sendo destinados aos residentes do país.

[17] *CASTELLS, Manuel. Op. Cit., p. 204.*

[18] *Disponível em <http://www.fas.org/irp/program/process/rapport_echelon_en.pdf>. Acessado em 10/01/2012.*

As tecnologias de investigação referem-se à elaboração de base de dados através dos resultados de vigilância e acumulação de informação obtida assiduamente. Às vezes trata-se tão somente de elaborar um perfil, como nos estudos de mercado, mas ocasionalmente pode ser determinada pessoa por um conjunto de informações da sua *pessoa digital*, obtidas por meio de pagamentos com cartão de crédito, visitas a sítios da web, correio eletrônico.

A encriptação é a tecnologia que permite a privacidade da mensagem, que em geral ocorre no caso da encriptação da chave pública no qual temos duas chaves:a chave pública que é de livre acesso e a chaveprivada que somente o dono da mensagem conhece. Ambas as chaves podem cifrar ou decifrar dependem da garantia que se procura se é autenticidade ou confidencialidade, assim se a chave pública cifra, logo a privada decifra e o que se pretende garantir é a confidencialidade o contrário (chave privada cifra e a pública decifra) por seu turno visa garantir a autenticidade da informação.

No setor privado a cultura da segurança é imperiosa no sentido de atuar preventivamente, tendo em vista o contexto atual marcado pela desregulamentação e privatização do setor de telecomunicações. Dessa forma há necessidade de uma orientação dos poderes públicos e a participação do setor privado. Por exemplo, os fabricantes de software deverão atualizar frequentemente seus produtos por uma questão de segurança e também a rápida troca de informações entre o setor público e privado para uma ágil detecção de ataques às redes. Outro exemplo importante foi a criação do GBDe (Global Business Dialogue on Eletronic Commerce[19]). Trata-se de um agrupamento privado de gigantes que tem desenvolvido por conta própria modelos de segurança e certificação digital dirigidos ao fomento da autenticação eletrônica e da assinatura digital.

Contudo, por uma segurança no ciberespaço temos uma guerra de código contra código. O controle em detrimento da liberdade produzindo um nicho comercial. Cite-se, a título de exemplo, algumas empresas, como a ZipLip, criaram um tipo de correio eletrônico autodestrutível que utiliza tecnologia de encriptação; outras empresas, como a Freedom, dificulta a perseguição encriptando o correio eletrônico e os requerimentos de navegação pela web.Temos aqui um rápido desenvolvimento da tecnologia de proteção da privacidade que preocupa os governos e tenta proibir o uso privado dessas tecnologias[20].

A cooperação entre entidades públicas e privadas é necessária, porque a primeira aplica a lei e a segunda tem capacidade de mobilizar os meios tecnológicos para o exercício da função pública no combate a criminalidade. O professor Pedro Verdelho[21] cita como exemplo o anúncio no final de 2003 de um programa de

[19] *VERDELHO, Pedro. Cibercrime e segurança informática, 2005, p. 166.*
[20] *CASTELLS, Manuel. Op. Cit., p. 217-218.*
[21] *Op. cit.*

cooperação entre a Microsoft e a Interpol tendo em vista a formação de policiais para a investigação na internet dos crimes de pedofilia e pornografia infantil.

No setor público diversos países têm optado por criar unidades nacionais especializadas no combate ao crime informático. Nos Estados Unidos, por exemplo, existe uma força de vigilância permanente nas páginas da web e também de chat rooms.

A Europol[22] fez algumas recomendações para os países membros da União Europeia: parceria com o setor privado, desenvolvimento de uma coordenação centralizada de inteligência para a análise de modo a estabelecer um centro europeu de cibercrime para analisar os dados, sensibilizar os usuários individuais e empresas para uma série de questões incluindo o download ilegal, engenharia social, segurança na utilização dos cartões de pagamento, segurança das conexões da internet sem fio e os riscos que a internet representa para as crianças.

Ela também desempenha um papel na força europeia de combate ao cibercrime formando um grupo de peritos junto com os representantes da Eurojust e da Comissão Europeia de forma a trabalhar em conjunto com os chefes dos departamentos de cibercrimes para facilitar a luta contra cibercriminalidade transfronteiriça e intercâmbio de informações, realiza uma analise estratégica das tendências do cibercrime bem como a relação do crime organizado com a internet, está em fase de desenvolvimento à coordenação centralizada de relatórios de cibercrime para reportar as autoridades dos países membros da União Europeia e também dar suporte técnico e treinamento para a aplicação da lei.

Há em Portugal uma proposta de estratégia nacional de cibersegurança de responsabilidade do Gabinete Nacional de Segurança, regulamentado pelo Decreto-Lei no 3/2012, que visa garantir a segurança da informação no âmbito nacional e internacional do qual Portugal é parte, bem como a fiscalização das entidades que atuam no sistema de certificação eletrônica do Estado e a infra-estrutura de chaves públicas que exige necessariamente uma abordagem integrada e otimizada das redes de comunicação eletrônicas.

No Brasil, também em estágio embrionário, a cibersegurança encontra regulamentação no Decreto 6073/2008 como uma estratégia de Defesa Nacional com planos de metas a serem alcançados dentre os quais temos: capacitação tecnológica para que não dependa de tecnologia estrangeira; desenvolvimento dos setores industriais, educacionais e militares voltados à área cibernética e aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, que permitam seu pronto restabelecimento, a cargo da Casa Civil da Presidência da República, dos Ministérios da Defesa, das Comunicações e da Ciência e Tecnologia,

[22] Disponível em Informação disponível em:<http://g1.globo.com/tecnologia/noticia/2011/06/ataque-hacker-foi-o-maior-ja-sofrido-por-sites-do-governo-na-internet.html>. Acessado em 09/01/2012 >.Acessado em 09/01/2012.

e do Gabinete de Segurança Institucional da Presidência da República.E, por fim, o Ministério da Defesa e as Forças Armadas intensificarão as parcerias estratégicas e o intercâmbio militar com as Forças Armadas das nações amigas, neste caso particularmente com as do entorno estratégico brasileiro e as da Comunidade de Países de Língua Portuguesa.

5. A REPRESSÃO NO ORDENAMENTO JURÍDICO BRASILEIRO

No Brasil não temos um estatuto próprio que cuida deste assunto, mas se compararmos com a Convenção do Cibercrime,vamos encontrar tanto no Código penal como em legislações esparsas, instrumentos repressivos semelhantes começando pela Lei 12737/2012 que altera o Código Penal e cria o Art. 155-A, criada a *toque de caixa* como uma reação ao fato que chocou o país no qual a atriz brasileira Carolina Dickman que foi alvo de ataque hacker e suas fotos nus que estavam na caixa de e-mail foram divulgadas na internet, este artigo exige que a violação recaia sobre um mecanismo de segurança de forma que não será tipíca a conduta se ficar provado, por exemplo, que no computador não havia sequer um anti-vírus gratuito ou que o acesso de alguma forma estava livre como uma rede wi-fi sem segurança, ademais a invasão por si só não é crime exigindo o dolo específico de invadir com o fim de obter dado sem autorização expressa ou tácita do titular do dispositivo, exatamente como a Convenção do Cibercrime também o define.

A interceptação ilegítima de dados informáticos está tutelada na Lei 4117/62, pois define os serviços de telecomunicação (Art. 4o) como a transmissão, emissão ou recepção de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza, por fio, rádio, eletricidade, meios óticos ou qualquer outro processo eletromagnético, indo ao encontro do disposto na Convenção do Cibercrime, e o Art. 55 prevê como crime a interceptação, entretanto o dispositivo não possui o preceito secundário de forma que a conduta torna-se atípica (nullun crimen sine poena), não cabe o Art. 151 do CP, porque este não tipifica a interceptação de emissão eletromagnética, elétrica e óptica, contudo se interceptarem um computador que emita dados via rádioelétrico neste caso será tipificado pelo artigo supracitado. A interferência de dados encontra-se protegido pelo Art 155-A do CP quando descreve as condutas de adulterar ou destruir dados como uma finalidade especial do tipo, também temos o Art. 313-A do CP, mas com um diferencial em relação à Convenção que é o fato de ser crime prórpio (somente o funcionário público pode cometer), o sujeito passivo é a Administraçào Pública e possui uma finalidade especial que além do dano é obter vantagem indevida para si ou para outrem.

A interferência em sistemas seria uma agravante da interferência de dados de tal modo que o sistema informático mediante a introduçào, transmissão,

destruição, eliminação, deterioraçào, supressão ou modificação de um dado, trata-se de conduta atípica no ordenamento brasileiro quando praticado por particular e/ou o sistema não for da Administração pública, caso contrário estará tipificado no Art. 313-B do Código Penal.

O uso abusivo de dispositivo, por exemplo, ter um programa trojan ou vírus para atacar outro computador não encontra tipificação.

A falsidade informática pode ser tutelada no Art. 298 do CP, visto que o conceito de documento particular admite interpretação extensiva podendo ser não somente um contrato em papel, mas também um contrato virtual.

A burla informática é o estelionato previsto no Art. 171 do CP, assim, por exemplo, caso alguém crie uma página falsa na web com o fim de induzir em erro outrem, as pessoasacreditam que trata-se de uma paágina idônea, e com isso ao realizarem negócios terão prejuízos, neste caso o infrator responderá no termos deste artigo.

As Infrações relacionadas com pornografia infantil encontra-se amparo no Art. 241-A e 241-B da Lei 8069/90 (Estatuto da Criança e do Adolescente).

Por fim, as infrações relacionadas com violação do direito do autor e dos direitos conexos tem resguardo no Art. 184 do Código Penal.

6. CONCLUSÃO

A tecnologia da rede de informática contribuiu para o processo de globalização ao ampliar o acesso a informação e poder de comunicação entre as pessoas, por outro lado este novo ambiente social gera um risco para o próprio sistema capitalista, por exemplo, a eficiência das transações financeiras que utilizam a internet como meio de execução, gera em contrapartida um campo fértil para as fraudes envolvendo cartões de créditos.

Portanto, o setor privado atua inovando as tecnologias de identificação do usuário e encriptação de dados com o objetivo de minimizar os riscos que o sistema apresenta. E também o Estado que responde por meio de parcerias com o setor privado, sistemas de vigilância, intercâmbio de informações com outros Estados e a criminalização de condutas, sendo que muitas delas são de perigo abstrato.

Assim, a criminalização de determinadas condutas surge diante da insegurança que o sistema causa à medida que sua importância aumenta para a infra-estrutura dos Estados e empresas, logo o tema tem sido alvo de debates internacionais em especial do Conselho da Europa culminando na Convenção do Cibercrime de vocação universal, propondo a criminalização do acesso ilegítimo, interceptação ilegítima, interferência de dados e sistemas, uso abusivo de programas ou dados informáticos, falsidade informática, burla informática, pornografia infantil e violação do direito do autor e dos direitos conexos.

7. REFERÊNCIAS

CARRAPIÇO, Helena. *O crime organizado e as novas tecnologias*: uma faca de dois gumes. Nação e Defesa, Lisboa, n. 111, série 3, p. 175-192, 2005

GIDDENS, Anthony. *As consequências da modernidade*. Trad. Fernando Luís machado e Maria Manuela Rocha. 4. ed. Oeiras: Celta, 2005.

CASTELLS, Manuel. *A galáxia internet*: Reflexões sobre internet, negócios e sociedade. 2. ed. Trad. Rita Espanha. Lisboa: FundaçãoCalousteGulbenkian, 2007.

EUROPOL.*Cybercrime as a business*: Thedigital underground economy. Disponível em: <https://www.europol.europa.eu/content/press/cybercrime-business-digital-underground-economy-517>. Acessado em: 09/01/2012.

G1. *Ataque hacker foi o maior já sofrido por sites do governo na internet*. Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/06/ataque-hacker-foi-o-maior-ja-sofrido-por-sites-do-governo-na-internet.html>. Acessadoem: 09/01/2012.

NAÇÕES UNIDAS. *Cybersecurity*: A global issue demanding a global approach. New York: Department of economic and social affairs, 2011. Disponível em: <https://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html>. Acessadoem: 28/05/2012.

NAÇÕES UNIDAS..*Bangkok Declaration - Synergies and Responses*: Strategic Alliances in Crime Prevention and Criminal Justice New York: Department of public information, 2005. Disponível em: <https://www.un.org/events/11thcongress/declaration.htm>. Acessado em 29/05/2012.

NAÇÕES UNIDAS. *Cybersecurityand ITU*. Disponível em: <http://www.un.org/en/ecosoc/cybersecurity/itu_cybersecurity_overview.pdf>. Acessadoem 04/04/2013.

NAÇÕES UNIDAS. *International review of criminal policy* - United Nations Manual on the prevention and control of computer-related crime.Disponível em:<http://www.ictparliament.org/node/2128>. Acessado em 11/06/2012.

NAÇÕES UNIDAS. *12th UN Congress on Crime Prevention and Criminal Justice Committee II2nd& 3rd Meetings (AM & PM)*: Delegates Consider Best Response to Cybercrime as Congress Committee Takes Up Dark Side of Advances in Information Technology. New York: Department of public information, 2010. Disponível em: <http://www.un.org/News/Press/docs/2010/soccp349.doc.htm>. Acessado em: 28/05/2012.

RODRIGUES, Anabela Miranda. *Política criminal*: Novos desafios, velhos rumos. In: CORREIA, Eduardo, et. al. (Org.).Direito penal económico e europeu: Textos Doutrinários. Coimbra: Coimbra Editora, Vol. 3. p. 159-182, 2009.

SCHMID, Gerhard. *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)*.Bruxelas/ Estrasburgo: Parlamento Europeu, 2001. Disponível em:.<http://www.fas.org/irp/program/process/rapport_echelon_en.pdf>. Acessado em: 10/01/2012.

VERDELHO, Pedro. *Cibercrime e segurança informática*. Polícia e Justiça, série 3, n. 6, p. 159-175, jul/dez. 2005.

_____. *Phishing e outras formas de defraudação nas redes de comunicação*. In: Faculdade de Direito da Universidade de Lisboa, et. al. (Org.). Direito da Sociedade da Informação, Coimbra, vol. 8, p. 407-420, 2009.

VENÂNCIO, Pedro Dias. *Lei do cibercrime*: Anotada e comentada. Coimbra: Coimbra Editora, 2011.

VIANO, Emilio. C. *The online world and cybercrime*: a nenw reality for criminal law and criminology. Direito e Cidadania, Praia, ano 9, n. 27, p. 29-41, 2007/2008.

Recebido em: 20/10/2014
Aceito: 13/02/2015