ESCOLA DA MAGISTRATURA DO ESTADO DO PARANÁ
XXXIV CURSO DE PREPARAÇÃO À MAGISTRATURA
NÚCLEO CURITIBA

KAREN DE SOUSA OLIVEIRA

CYBERCRIME E *CYBERWAR* EM GRANDES EVENTOS: COPA DO MUNDO 2014 E OLIMPIADAS 2016

CURITIBA
2016

KAREN DE SOUSA OLIVEIRA

CYBERCRIME E *CYBERWAR* EM GRANDES EVENTOS: COPA DO MUNDO 2014 E OLIMPIADAS 2016

Monografia apresentada como requisito parcial para conclusão do Curso de Preparação à Magistratura em nível de Especialização. Escola da Magistratura do Paraná.

Orientador: Prof. Daniel Tempski Ferreira da Costa

CURITIBA
2016

TERMO DE APROVAÇÃO

KAREN DE SOUSA OLIVEIRA

***CYBERCRIME* E *CYBERWAR* EM GRANDES EVENTOS: COPA DO MUNDO 2014 E OLIMPIADAS 2016**

Monografia aprovada como requisito parcial para conclusão do Curso de Preparação à Magistratura em nível de Especialização, Escola da Magistratura do Paraná, Núcleo de Curitiba, pela seguinte banca examinadora.

Orientador: _____

Avaliador: _____

Avaliador: _____

Curitiba, de de 2016.

AGRADECIMENTOS

Nesta fase final do curso de pós-graduação, agradeço a Deus, pois seu cuidado me sustentou e me manteve disposta a vencer os desafios, de modo que a sua palavra me trouxe esperança e força para o deslinde dessa trajetória.

Aos meus pais, José Ibernon e Maria Helena e a minha irmã, Karla, os quais me incentivam todos os dias e me ensinam que, independente das circunstâncias, somos mais do que vencedores.

Aos Excelentíssimos Professores da Escola da Magistratura do Paraná por tanto brilhantismo em seus ensinamentos. Com grande honra, pude vivenciar dias de um sonho a ser realizado, qual seja, o de me tornar uma Magistrada que busque cumprir o poder-dever de fazer a justiça e o bem.

SUMÁRIO

RESUMO

O presente trabalho monográfico tem a intenção de analisar os conceitos de *cybercrime e* cyberwar, considerando, para tanto, os grandes eventos realizados no Brasil, quais sejam a Copa do Mundo em 2014 e os Jogos Olímpicos em 2016. Pretende, ainda, analisar as Leis vigentes relacionadas ao *cybercrime*, pontuando os riscos decorrentes da utilização das novas tecnologias para o cometimento de delitos informáticos. Analisa-se, ainda, a infra-estrutura dos grandes eventos e a vulnerabilidade da segurança cibernética.

Palavras-chave**:** Grandes Eventos. Crimes cibernéticos. Segurança Cibernética.

01 – INTRODUÇÃO

O presente trabalho de conclusão de curso de pós-graduação, como ponto de partida, analisa os conceitos tradicionais, bem como conceitos peculiares, quais sejam, *cybercrime e cyberwar,* considerando, principalmente, que o Brasil foi sede de grandes eventos como a Copa do Mundo 2014 e Olimpíadas 2016.

Tais eventos se mostram uma oportunidade para o cometimento de delitos favorecidos a partir da tecnologia. O Conselho do Desenvolvimento Econômico e Social (CDES)[1] afirma que:

> É uma oportunidade excepcional e, como toda oportunidade, carrega riscos. Por isso, é preciso desenvolver políticas atentas a necessidades reais e não pelo apelo das mídias. A discussão de um modelo sustentável tem que atender a um conjunto de questões, não só a logística de transporte, de construção de arenas, é preciso ter uma preocupação ambiental e social na organização dos eventos, considerar a demanda energética e de telecomunicações e sua necessidade de ampliação, para atender ao público visitante. A segurança pública também é uma questão vital e o Brasil deve ter, como exemplo, iniciativas e problemas que ocorrem em outros países e incorporar as boas práticas internacionais.

Importante destacar que o Brasil ocupava o quarto lugar em 2011, referente a uma lista a qual continha 24 países, com maior quantidade de crimes cibernéticos aplicados. De acordo com a Polícia Federal, as redes do Governo Federal recebem mais de 2 mil ataques por hora[2]. Além disso, mais de 80% dos usuários da internet foram vítimas de delitos cibernéticos. E, ainda, de acordo com a Secretaria para Grandes Eventos, anualmente, o prejuízo chega a R$ 15 bilhões[3].

Dessa forma, faz-se necessário a análise das Leis vigentes relacionadas ao *cybercrime*, o qual se refere aos crimes praticados contra ou por meio de computadores. Trata-se de uma série de atividades criminosas, incluindo os crimes contra dados armazenados em meios eletrônicos e sistemas, crimes relacionados aos computadores, ofensas de conteúdo e ofensas de direitos autorais (Kaminski, 2011, p. 43).

---

[1]MOTA, Humberto. **Grandes eventos esportivos:** oportunidade excepcional para o Brasil. Dez. 2010 Disponível em:<http://www.cdes.gov.br/noticia/18355/grandes-eventos-esportivos-oportunidade-excepcional-para-o-brasil.html> Acesso em: 17 jul. 2016.

[2]Divisão de Comunicação Social da Polícia Federal. Disponível em: <http://www.dpf.gov.br/agencia/noticias/2012/junho/pf-inaugura-centro-contra-ataques-ciberneticos>. Acesso em: 17 jul. 2016.

[3]WAMBURG, Jorge. **Segurança na Internet**. Marc. 2014. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2014-03/curso-prepara-policiais-para-enfrentar-crimes-ciberneticos-na-copa>. Acesso em: 17 jul. 2016.

Em uma amplitude maior, tem-se o conceito de *cyberwar*. John Arquilla e David Ronfeldt, em Ciberwar is Coming (1997, p. 31), conceituam c*yberwar* como a destruição de sistemas de informação e de comunicação. Aduzem que a "ciberguerra" pode ter amplas implicações para a organização militar, bem como para a doutrina com a ampliação de estratégia, sendo esta aplicável tanto em conflitos de baixa intensidade quanto alta intensidade.

Outro conceito é o de Parks e Duggan (2001, p. 122):

> Guerra Cibernética é o sub-conjunto da guerra da informação que envolve ações realizadas no mundo cibernético. O mundo cibernético é qualquer realidade virtual compreendida numa coleção de computadores e redes. Existem diversos mundos cibernéticos, mas o mais relevante para a Guerra cibernética é a internet e as redes a ela relacionadas, as quais compartilham mídia com a Internet. A definição militar mais próxima para o nosso termo, guerra cibernética, é uma combinação de ataque a redes de computadores e defesa de redes de computadores, e possivelmente, operações especiais de informação. Nós definimos guerra cinética como sendo a guerra praticada no "mundo real". Todos os tanques e navios e aviões e soldados tradicionais são os protagonistas da guerra cinética.

Dessa forma, o campo de conflito não mais se restringe a um campo físico, como em guerras históricas, e sim em um campo definido como ciberespaço ou espaço cibernético. Sendo assim, o Ciberespaço pode ser definido como qualquer espaço através do qual se tem acesso à informação, ampliando a noção de território (Fiorillo, 2013, p. 15).

Com isso, milhares de pessoas estão interligadas e conectadas digitalmente devido ao avanço das telecomunicações, possibilitando o tráfego intenso de informações, inexistindo limitação de fronteiras (Fiorillo, 2013, p. 160).

Assim, visível a ausência de um comando central com o qual pode ter origem em diversos pontos na rede mundial de computadores (Fiorillo, 2013, p. 160).

A partir da conceituação, mostra-se que o mundo real e o mundo digital estão interligados de modo que as ações praticadas no mundo cibernético produzem efeitos no mundo real. Como exemplo, tem-se a indisponibilidade de serviços essenciais como a segurança pública e a telefonia quando estes são atacados ciberneticamente.

O trabalho pontualiza os problemas decorrentes da interferência do modo de utilizar as novas tecnologias de informação e comunicação (TICs) nas relações

sociais. Tal interferência necessita de tutela jurisdicional para as relações realizadas no meio ambiente digital.

E, com o avanço das TICs, bem como os ataques realizados a partir da rede mundial de computadores, há que se analisar a perspectiva das condutas delitivas de caráter tecnológico.

Sendo assim, faz-se necessário o estudo a partir de consultas ao ordenamento jurídico brasileiro e internacional, tendo em vista os países que foram sede, como exemplo, o Brasil, e que ainda receberão a Copa do Mundo ou os Jogos Olímpicos.

Levando em consideração os conceitos e o contexto ao qual são aplicados, tem-se o presente trabalho estruturado da seguinte forma: o segundo capítulo versa sobre o histórico da Internet e o Ciberespaço, bem como conceitua os termos *cybercrime* e *cyberwar* e suas características principais; o terceiro trata dos grandes eventos como a Copa do Mundo já realizada e as Olimpíadas realizadas em 2016, analisando a estrutura dos eventos, os preparativos e a vulnerabilidade da segurança cibernética.

Por fim, o quarto capítulo apresenta as atuais legislações, as Leis Nº 12.737/2012 (BRASIL, 2012), alterações relativas ao Decreto-Lei Nº 2.848/1940 (BRASIL, 1940) e Lei Geral da Copa - Lei Nº 12.663/2012 (BRASIL, 2012), avaliando a potencialidade frente aos delitos informáticos, considerando o cenário de realização de grandes eventos para entender como tratam dos delitos informáticos, as exigências de proteção e segurança da sociedade brasileira, bem como um estudo comparado de modo a analisar as técnicas de segurança tomadas por países como a África do Sul, que sediou a Copa do Mundo, o Canadá, que sediou os Jogos de Inverno e o Brasil, sede da Copa do Mundo de 2015 e Jogos Olímpicos, como exemplo.

2. *CYBERCRIME E CYBERWAR*

Com o avanço da era digital, o desenvolvimento tecnológico envolveu a sociedade de modo que as atividades da coletividade passaram a ser praticadas por meio da Internet.

O advento da Internet fez com que a comunicação e outras atividades como compras, transações bancárias e serviços governamentais passassem a ser cada vez mais dependentes da rede de computadores.

Entretanto, além dos benefícios da Internet, destaca-se a possibilidade de condutas ilícitas, reprováveis pela sociedade, as quais podem ser desde o envio de *spams* a invasão de sistemas, entre outros.

Observa-se o aumento dos delitos cometidos por meio da Internet no Brasil. Os motivos são diversos, porém, o principal incentivo do sujeito ativo do delito passou a ser o lucro. Com a utilização econômica da rede informática, a informação ficou cada vez mais acessível à medida que milhares de usuários utilizam a Internet para transações, negócios e trabalho. Destaca-se ainda, a ausência de fronteira já que o agente não precisa se deslocar para a prática do ilícito, bem como a sensação de anonimato que a rede confere a ele.

Logo, em detrimento da evolução das tecnologias surge a necessidade de uma regulamentação capaz de acompanhar tal crescimento. Como afirma Sydow (2013, p. 53), a Internet gera insegurança devido à modificação constante, ocasionando ciclos de revolução de conceitos. Dessa forma, visualiza-se a Internet como meio para a prática de condutas violadoras de bens jurídicos tutelados.

Inicialmente, faz-se necessário delimitar o conceito dos delitos e suas características principais. Em que pese não tenha uma uniformidade sobre a denominação, tendo em vista que ora a doutrina utiliza o termo crimes informático, ora crimes eletrônicos, crimes digitais ou *cybercrimes*, todos utilizam as novas tecnologias de informação e comunicação (TIC) como instrumento facilitador para o cometimento. Para isso, é preciso apresentar o contexto referente à Internet e o ambiente criado no mundo digital para a prática dos delitos informáticos, qual seja, o ciberespaço.

2.1 A Internet e o Ciberespaço

No período da Guerra Fria, em meados da década de 60, o Departamento de Defesa dos Estados Unidos financiou experimento que resultou na principal forma de comunicação entre computadores, ou seja, a denominada "*Advanced Research Projects Agency*" ou, simplesmente, ARPA. Inicialmente, tal inovação ficou restrita

aos centros tecnológicos americanos devido à pretensão de imunidade contra-ataques soviéticos.

Durante os anos 70, criou-se o projeto da ARPANET visando à criação de uma rede de comunicação capaz de armazenar os dados sigilosos em casos de ataques nucleares de forma integral (Castells, 2003, p. 70). Com isso, o projeto foi aperfeiçoado e permitiu que fosse disponibilizado para as universidades, passando a ser denominado ARPA-INTERNET.

Seguindo as fases de evolução, com a criação do protocolo de controle de transmissão TCP/IP (*Transmission Control Protocol/ Internet Protocol*), a rede foi liberada para domínio público e no início dos anos 90, foi desenvolvido o sistema chamado de Hipertexto World Wide Web (WWW) (Fiorillo, 2013, p. 14).

E, com a criação do protocolo de transmissão TCP/IP, foi possível o crescimento da rede interligando diversos países até o estabelecimento deste protocolo como padrão (Fiorillo, 2013, p. 14).

Com o passar do tempo, foram estabelecidos provedores independentes, privatizando a Internet de modo a originar serviços digitais/virtuais diversos expandindo a Internet além do almejado no período militar.

Para o acesso, foram elaborados navegadores como o Internet Explorer, proveniente da *Microsoft*, o que facilitou e possibilitou a busca de dados e informações de modo *online*. Destaca-se a utilidade em forma de entretenimento já que a Internet passou a integrar a vida em sociedade.

No Brasil, por meio do Laboratório Nacional de Computação Científica (LNCC), localizado em Petrópolis, Rio de Janeiro, foi possível a primeira conexão[4]. Como havia, nesse período, restrição ao acesso de tecnologia estrangeira, devido às medidas protecionistas, o uso do computador ficava restrito aos centros de pesquisas nas Universidades.

Contudo, o Ministério de Comunicações e de Ciência e Tecnologia visualizaram o *status* comercial da Internet, abrindo o setor que antes era privado da Internet para exploração comercial.

Em uma breve definição, considera-se a Internet como uma rede internacional composta de 150.000² redes de computadores e milhões de usuários, estando unida por meio de um protocolo ou uma linguagem em comum (Kaminski, 2011, p. 37).

---

[4]SIMON, Imre. **Histórias das Redes no Brasil.** Disponível em: <https://www.ime.usp.br/~is/abc/abc/node25.html> Acesso em: 17 jul. 2016.

Kaminski (2011, p. 39) entende que a Internet não possui limite territorial tradicional conferindo o caráter de liberdade, caso se entenda por existir uma natureza.

A partir do advento da Internet, surgiu o ciberespaço. Este foi definido por Gibson em 1984 na obra de ficção científica *Neuromancer*. Nesta obra, o autor utiliza termos que se difundiram anos mais tarde como vírus e ações de *hacker* (Kaminski, 2011, p. 40) Conforme aduzem diversos autores, o ciberespaço seria equiparado ao termo “mundo virtual”, sendo um meio que liga dispositivos diversos, permitindo o surgimento de relações no ciberespaço.

O autor cita, ainda, o conceito da UNESCO (2011, p. 40):

> O ciberespaço é um novo ambiente humano e tecnológico de expressão, informação e transações econômicas. Consiste em pessoas de todos os países, de todas as culturas e linguagens, de todas as idades e profissões fornecendo e requisitando informações; uma rede mundial de computadores interconectada pela infraestrutura de telecomunicações que permite à informação em trânsito ser processada e transmitida digitalmente.

Fiorillo (2013, p. 15) expõe o conceito de forma clara ao analisar que por meio do advento da Internet e do ciberespaço, a noção de território está ligada a uma idéia nova, qual seja, a rede. Logo, o ciberespaço transcende à vida real.

Faz-se uma conexão entre o advento da Internet e o ciberespaço com a modificação da concepção do território que passou a ser qualquer ponto através do qual se tem acesso à informação. Assim, a informação é o principal elemento que identifica o território no espaço, surgindo a necessidade de estabelecer um centro de comando.

Com isso, conceitos como Internet e espaço digital se desenvolveram e consolidaram relações digitais, uma sociedade de informação marcada pela evolução tecnológica que transformou e intensificou as relações sociais, originando a Revolução Tecnológica ou Revolução Digital. A partir dessa consideração, Fiorillo (2013, p. 16) entende necessário o estudo da “Sociedade da Informação”.

Importante salientar que o início da “Sociedade da Informação” não se originou no Brasil, e sim em 1993, no Conselho Europeu de Copenhague ao estruturar a ideia de infraestrutura da informação (Fiorillo, 2013, p. 17). Insere-se no contexto da evolução tecnológica a qual reformulou o conceito de vida e organização em sociedade.

Paesani (2007, p. 62) define a Sociedade da Informação como “um novo ciclo histórico cuja marca é o surgimento de complexas redes profissionais e tecnológicas voltadas à produção e ao uso da informação, que alcança ainda sua distribuição através do mercado, bem como as formas de utilização desse bem para gerar conhecimento e riqueza”.

Com isso, sobrevieram os reflexos das TICs trazidas pela sociedade da informação como o interesse de milhões de usuários em busca de entretenimento e lazer através de comunidades virtuais as quais apresentam consequências jurídicas em diversos ramos do direito, em especial, ao direito criminal (Fiorillo, 2013, p. 65).

Desse modo, houve uma alteração das relações jurídicas com o advento da concepção reformulada de tempo e espaço (Fiorillo, 2013, p. 134), necessitando de tutela específica, como exemplo, a integridade das informações devido às atividades que se realizam na rede mundial de computadores.

Nesse contexto, a Internet se mostra como uma importante ferramenta no que diz respeito às novas tecnologias de informação e comunicação, integrando a sociedade da informação, o que pode ser visível pelo crescente acesso de usuários que, muitas vezes a utilizam como meio de entretenimento e lazer.

Surge então a imprescindibilidade de segurança tecnológica diante as relações entre a sociedade e a tecnologia, adequando os institutos jurídicos, políticos, econômicos e sociais já que em uma sociedade em que não há mais distância ou delimitação de espaço ou tempo é preciso um amparo e fortalecimento de institutos que tutelem os bens produzidos.

Dessa forma, surge a necessidade de integrar as novas tecnologias ao direito de acesso seguro das informações, de modo que direitos como propriedade e privacidade sejam assegurados.

Como tratado por Fiorillo (2013, p. 15), o Direito deve se adequar à nova realidade, existindo de fato o binômio Direito e Internet, o qual trata de uma realidade que deve ser explorada de modo aprofundado a fim de garantir os direitos fundamentais em todos os campos das ciências jurídicas.

Entretanto, as novas tecnologias vêm sendo utilizadas de modo diverso para cometimento de crimes, seja através do uso do computador, seja contra o computador ou contra a informação, criando uma série de mecanismos que possuem caráter preventivo para evitar danos irreversíveis aquele usuário que utiliza

a rede mundial e, em contrapartida, gera um benefício ilícito ao agente que se apropria das suas informações, por exemplo, com ânimo de lucro.

Sydow (2013, p. 52) coloca que a informática se tornou um nicho de exploração contínua do cidadão e este passou a ser vigiado e monitorado de forma que o usuário da rede deve ter cuidado ao visitar *sites* desconhecidos, comparando a fase da infância onde se aprende que não se deve conversar com estranhos.

Em detrimento do vultuoso desenvolvimento tecnológico e os recursos informáticos, condutas reprováveis e violadoras de bens jurídicos diversos passaram a ter resultado concreto, de modo que a análise dessas condutas faz-se imprescindível.

2.2 *Cybercrime*: definições no ordenamento jurídico e classificação

Há inúmeras definições em países como Canadá, Estados Unidos, Austrália e outros, considerando o tema no âmbito internacional.

Sendo assim, diversos doutrinadores citam a Conferência do Conselho da Europa sobre aspectos criminológicos em Estrasburgo como a primeira iniciativa internacional sobre crimes informáticos, no ano de 1983. Em meados de 1983, a Organização para a Cooperação Econômica e Desenvolvimento (*Organization for Economic Cooperation and Development*) trouxe a seguinte definição[5]:

> Qualquer comportamento ilegal, imoral ou não autorizado que envolva a transmissão ou processamento automático de dados.

Em 2001, foi estabelecida a Convenção sobre o *Cybercrime,* qual seja a Convenção de Budapeste, atuando como instrumento jurídico trazendo a tipificação como infração aos sistemas e dados informáticos, infrações relacionadas com computadores, infrações relacionadas com o conteúdo, infrações relacionadas com a violação de direitos autorais.

Entende-se por *cybercrime*, de acordo com o *United Nations Office onDrugsand Crime* (UNODC, 2013, p.19):

---

[5] COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática.** Disponível em: <http://jus.com.br/artigos/1826/crimes-de-informatica/2>. Acesso em: 17 jul. 2016.

> atos relacionados com o computador para o ganho ou prejuízo pessoal ou financeiro de outro, incluindo as formas de crimes relacionados à identidade e aos atos relacionados ao conteúdo de computadores (software, dados e informações)" – tradução livre.

Por outro lado, a definição pode ser mais ampla, incluindo atividades como: acesso não autorizado e pornografia infantil. Nogueira (2009, p.63) explica que existem algumas tipologias de crimes cometidos contra o computador, a saber: crime contra o *hardware*, crime contra o *software*, espionagem industrial e invasão de site do Poder Público e do Setor Privado. O autor ainda destaca o "crime de informática puro", o qual constitui "toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas".

Ferreira (2000, p.208) define sucinta e amplamente que "Crime Informático é toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão".

Nesta mesma linha, Fiorillo (2013, p. 143) cita a definição de Cláudio Líbano Manzur, secretário executivo da Associação de Direito e Informática do Chile:

> Todas aquelas ações ou omissões típicas, antijurídicas e dolosas.Trata-se de fatos isolados ou em série, cometidos contra pessoas físicas ou jurídicas, realizadas com o uso de um sistema de tratamento da informação e destinadas a produzir prejuízos para a vítima, através de atentados à saúde técnica informática, a qual, geralmente, produzirá de maneira colateral lesões a diversos valores jurídicos, ocasionando, muitas vezes, um benefício ilícito ao agente, seja patrimonial, ou não, atue ele com ou sem ânimo de lucro.

Ferreira (2011, p. 8) anota e justifica a conceituação dos "crimes informáticos" diante a ferramenta utilizada, qual seja, o computador. Aduz que, do mesmo modo, considera-se aquele crime cometido com o auxílio de um computador, sendo que este é utilizado como instrumento facilitador para a consumação delitiva.

Afirma, ainda, levando em consideração a estrutura essencial de um delito, que (Ferreira, 2011, p. 8):

> Crimes de computador são qualquer conduta humana (omissiva ou comissiva) típica, antijurídica e culpável, em que a máquina computadorizada tenha sido utilizada e, de alguma forma, facilitado de sobremodo a execução ou a consumação da figura delituosa, ainda que cause prejuízo a pessoas sem que necessariamente se beneficie o autor ou

> que, pelo contrário, produza um benefício ilícito a seu autor, embora não prejudique a vítima de forma direta ou indireta.

Diante disso, há denominações diversas relacionadas às novas tecnologias de modo que alguns doutrinadores se referem à criminalidade mediante computadores, criminalidade do computador, delitos cibernéticos, *cybercrimes, entre* outros.

Considerando a classificação propriamente dita, Vianna traz a denominação de crimes informáticos os quais podem ser subdivididos em crimes informáticos próprios ou puros, crimes informáticos impróprios ou mistos e crimes informáticos mediatos ou indiretos.

Crime virtual puro seria aquele que tem como objetivo a inviolabilidade das informações automatizadas, ou seja, dados. Em se tratando dos crimes mistos, consideram-se como aqueles complexos em que, além da proteção da inviolabilidade de dados, a norma visa a tutelar bem jurídico de natureza diversa. Já os crimes mediatos ou indiretos possuem finalidade não informática, ou seja, utilizam o computador como meio para possibilitar a consumação.

Já a definição de Fiorillo (2013, p. 144) faz alusão aos crimes subdivididos em puros, mistos e comuns. Os crimes virtuais puros atacam o sistema informático *software* (programa informático), *hardware* (parte física do computador), dados, sistemas e meios de armazenamento. Os crimes mistos têm o computador como condição da prática do crime, como exemplo, a transferência ilícita de quantias em milhares de contas. Por fim, os crimes comuns os quais se encontram tipificados na legislação penal brasileira e utilizam o computador como meio de execução dos delitos, tais como estelionato, descrito no artigo 171, do Código Penal (Brasil, 1940) e crimes contra a honra, expostos nos arts. 138 a 140, do referido Código.

O grande desafio citado pelo supramencionado autor é em relação aos crimes informáticos puros, devido à dificuldade de correspondência típica na legislação, considerando que o princípio da legalidade é tido como norteador do Direito Penal.

Seguindo esta linha, Nogueira (2012, p. 18) utiliza o termo “crimes cibernéticos” para definir delitos praticados contra ou por intermédio de computadores. Subdivide-os em crimes cibernéticos abertos e crimes exclusivamente cibernéticos. O primeiro é definido como aquele que utiliza o computador como meio para a prática de crime, o qual poderia ser cometido com ou

sem o uso do computador. O segundo seriam aqueles que somente poderiam ser praticados através da utilização de computadores ou de outro recurso tecnológico com acesso à internet, como exemplo, utiliza o crime de aliciamento de crianças praticado por intermédio de salas de bate papo na internet (SANTIN, 2012, p.288-301), tipificado no artigo 241-D do Estatuto da Criança e Adolescente, Lei Nº 8.069/90 (BRASIL, 1990).

Kaminski (2011, p. 29) entende que tais crimes também podem ser chamados de crimes digitais ou transnacionais, os quais afetam diversos países e possuem uma característica peculiar, qual seja, o sujeito age em seu próprio domicílio. Tal fato chama atenção da polícia em se tratando da materialidade e evidências. Por isso, surgiu a necessidade do FBI e outros como a Real Polícia Montada do Canadá de formar policiais chamados de *Cybercops*, alertando a coletividade sobre o potencial das ameaças virtuais.

O que mais contribui para o aumento dos delitos informáticos é o crescimento geográfico do uso da Internet e sua absoluta dispersão e falta de controle, o que possibilita a atividade dos criminosos através das revolucionárias vantagens do espaço cibernético, bem como suas habilidades técnicas.

Como exemplo de crimes com uso de alta tecnologia, cita-se o estelionato caracterizado pelo agente que faz transferências eletrônicas de contas bancárias para seu próprio benefício, furtos de dados, apologia ao racismo, crimes contra a honra, terrorismo, clonagem de cartões, crimes contra a propriedade intelectual como falsificação e pirataria de informação, inserção de dados falsos em sistemas de informações, fraudes como vendas e investimentos fraudulentos.

2.3 *Cybercrime*: características

Considerando os sujeitos dos crimes informáticos, têm-se o sujeito ativo e passivo. O ativo é aquele que pratica a conduta descrita na lei, ou seja, o fato típico, podendo haver ou não a associação para ser considerado sujeito ativo. Em se tratando da capacidade, o supracitado autor defende que toda pessoa natural a possui, independente da idade ou do estado psíquico.

Já o sujeito passivo é o titular do bem o qual fora lesado pela conduta criminosa, podendo existir mais de um sujeito passivo. Assim, todos aqueles que são lesados ou os seus bens jurídicos sofrem ameaças, são vítimas de crimes informáticos. Lima acertadamente expõe (2011, p. 36):

> O sujeito passivo ou a vítima dos crimes de computador é o ente sobre o qual recai a conduta omissiva ou comissiva realizada pelo sujeito ativo e, no caso dos “delitos informáticos”, podem as vítimas ser indivíduos, instituições creditícias, governos e outras tantas que utilizem sistemas automatizados de informação, conectados ou não à Internet.

A vítima, muitas vezes, não detém de conhecimento informático suficiente para discernir ou perceber a ação do sujeito ativo. Ocorre que tal fato é comum em ações como as de fraude. Com isso, o mencionado autor cita que a vítima inicialmente procura erros de programação ou falhas técnicas e, somente depois, chegam à conclusão de que a causa poderia ser uma ação delitiva.

Kaminski (2011, p. 31) revela que a conduta do sujeito passa por três estágios como o desafio, o dinheiro extra e os altos gastos e o comércio ilegal. E, quanto ao perfil do sujeito ativo afirma:

> O perfil do criminoso, baseado em pesquisa empírica, indica jovens, inteligentes, educados, com idade entre 16 e 32 anos, do sexo masculino, magros, caucasianos, audaciosos e aventureiros, com inteligência bem acima da média e movida pelo desafio da superação do conhecimento, além do sentimento do anonimato, que bloqueia seus parâmetros de entendimento para avaliar sua conduta como ilegal, sempre alegando ignorância do crime e, simplesmente, “uma brincadeira.

Analisando o perfil, nota-se que o sujeito ativo possui características como a habilidade sobre sistemas informáticos e possuem acesso à informação, de modo a perceber a oportunidade para a prática delitiva, bem como seu anonimato.

A partir disso, o doutrinador entende que os crimes variam desde crimes leves, como exemplo, aqueles que ofendem a honra, até vultuosos desvios financeiros que acabam por trazer instabilidade para a sociedade e desafios para a investigação, constituindo um problema global que envolve soberanias, culturas e sistemas jurídicos diferentes, possibilitando a dificuldade de coibir as condutas delitivas.

Também é o posicionamento de Ferreira (2011, p. 07) ao expor que, como os agentes não podem ser vistos ou ouvidos, estando ocultos em um terreno virtual e minimamente explorado, os delitos afetam diversos países e pessoas com diversas nacionalidades e distintas legislações, apesar de inexistir o deslocamento em território físico do sujeito ativo.

A partir do exposto, faz-se necessário mencionar as denominações dos agentes de crimes informáticos como: *hackers, crackers, phekers, cardes* e *cyberterrorists.*

Os *hackers* têm como objetivo tornar vulneráveis os programas informáticos. Em contrapartida, os *crackers* adulteram os programas, além de invadi-los.

Consoante expõe Firorillo (2013, p. 150), os computadores alheios denominados de “máquinas zumbis” ou “*botnets*” sãos aliados na aplicação de golpes virtuais. As chamadas “*botnets”* são computadores caseiros controlados de modo virtual por um invasor que pretende cometer crimes sem o consentimento do proprietário, de modo que tem acesso aos dados pessoais daquele como senhas de banco ou número de cartões de crédito as quais são digitadas na máquina. Dessa forma, invasores recrutam máquinas de outros países para atacar instituições financeiras em seu país originário.

Já os chamados *phekers*, são especializados em telefonia e atacam os sistemas de telecomunicação. Os *cardes* são aqueles que se apropriam do número de cartão telefônico através da invasão de listas eletrônicas a partir da instalação de programas que permitem acesso a qualquer informação inserida no computador invadido

Por fim, os *cyberterrorists,* segundo Fiorillo (2013, 153), são aqueles que desenvolvem vírus ou “bombas lógicas” objetivando provocar a queda do sistema de provedores, impedindo o acesso dos usuários e causando prejuízo econômico.

Outrossim, o sujeito ativo está longe de ser caracterizado como estudantes de classe média que acreditam ser especialistas no ramo da informática. Os agentes são aqueles que trabalham, normalmente, com a informática, bem como possuem um perfil de insensibilidade, mínima temibilidade em relação à norma, sendo motivados pelo lucro, vingança ou simplesmente para chamar a atenção.

Em contrapartida, nota-se o entendimento de Valdez (1996, p. 103) ao comentar que uma parcela de indivíduos poderiam seu sujeitos de tais delitos posto que seriam detentores de conhecimento técnico.

É preciso habilidade para o cometimento dos delitos informáticos em face dos novos programas de computadores. Entretanto, não se faz necessário um conhecimento aprofundado no ramo da informática já que muitas condutas

praticadas por computador são ações ocupacionais, ou seja, são realizadas quando o sujeito ativo se encontra em suas atividades de rotina.

As ações ocupacionais se caracterizam pelo fato de o agente se aproveitar de uma situação no mundo do sistema tecnológico e econômico das instituições financeiras para as práticas dos delitos.

Além da denominação dos agentes, é preciso classificar os programas utilizados. Fiorrillo (2013, p. 154) aduz que os *softwares* que se destacam são: *spammers, hoaxes, cookies, spywares* e vírus em geral.

O primeiro dele, *spammers,* trata de mensagens enviadas ao usuário de forma massificada e não autorizada por seu destinatário. São utilizadas para a invasão da privacidade dos usuários e como instrumento de espionagem de dados do usuário da Internet. Para isso, são utilizadas técnicas que chamam atenção do usuário com a intenção de enganá-lo como propagandas enganosas e brincadeiras que induzem o usuário a abrir como aqueles que possuem com assunto “fotos importantes”, “fotos da nossa viagem”.

Os *hoaxes* consistem em envio de email cujo conteúdo é falso em nome de empresas importantes e, geralmente, acompanhado de vírus. O terceiro, os *cookies*, são *softwares* que captam informações digitadas pelo sujeito passivo, objetivando, muitas vezes, o furto de informações do sistema. Os *spawares* consistem em programas que monitoram as atividades do internauta com a finalidade de vender as informações ou furtar dados e senhas. Consiste no monitoramento das atividades realizadas virtualmente com o intuito de verificar qual *spam* poderia ser enviado e aceito pelo próprio usuário.

Os vírus em geral são programas que copiam informações, podendo destruir arquivos e inutilizar a máquina. Podem ser instalados através de programas, *pen drives*, abertura de arquivos e outros.

Com isso, traçamos as características do Cybercrime. Ressalta-se a consideração de Fiorillo (2013, p. 141) de que a criminalidade informática possui características parecidas com as da informatização global e, dentre elas, a mais relevante é a transnacionalidade, posto que todos os países têm acesso ou fazem uso da informática de modo que se pratica o ilícito penal a partir de qualquer lugar da sociedade global.

2.4 *Cyberwar*: definições e características

Como exposto nos tópicos anteriores, as tecnologias da informação e comunicação se desenvolveram na sociedade de modo que o comércio eletrônico, o desenvolvimento tecnológico e econômico, entre outros, ganhou maior proporção, integrando a vida em sociedade. Em que pese o desenvolvimento das tecnologias da informação e comunicação (TIC) tenha possibilitado a troca mais célere das informações, um cenário propício a ataques cibernéticos foi criado.

Assim, sistemas de defesa, transporte, energia, telecomunicações e outros segmentos passaram a ser avaliados e reestruturados em se tratando da segurança de seus sistemas e redes de informação.

O *Department of Homelnd Security* (DHS), diante a necessidade de prevenção ao mau uso das tecnologias da informação, assegurou que deve ocorrer a prevenção aos danos devido a não autorização da informação e de sistemas de comunicação, devendo ser reestruturados os sistemas de comunicação, no caso de ataque ou desastre natural, observando a confidencialidade, integridade e disponibilidade[6].

Para entender as conseqüências e métodos de prevenção aos ataques cibernéticos no cenário atual, certamente é necessário frisar o conceito base de *Cyberwar.*

Cyberwar é uma "modalidade de guerra onde a conflitualidade não ocorre com armas físicas, mas através da confrontação com meios eletrônicos e informáticos no chamado ciberespaço". Nogueira (2012, p. 05) lembra que a guerra cibernética é mais ampla que "terra, mar, ar e espaço cideral", pois atinge o "5º domínio da guerra – o espaço cibernético". Além disto, esta modalidade de guerra permite que os "conflitos sejam assimétricos", fato que pode potencializar os ataques e enfraquecer os atacados.

Consoante Parks e Duggan (2001, p. 122):

> Guerra Cibernética é o sub-conjunto da guerra da informação que envolve ações realizadas no mundo cibernético. O mundo cibernético é qualquer realidade virtual compreendida numa coleção de computadores e redes. Existem diversos mundos cibernéticos, mas o mais relevante para a Guerra cibernética é a internet e as redes a ela relacionadas, as quais

[6]Acordo entre os Estados Unidos da América e a República Portuguesa para reforçar a cooperação do domínio da prevenção e do combate ao crime. Disponível em: <https://www.dhs.gov/xlibrary/assets/dhs_portugal_crimeagreement_port.pdf> Acesso em: 20 jul. 2016.

> compartilham mídia com a Internet. A definição militar mais próxima para o nosso termo, guerra cibernética, é uma combinação de ataque a redes de computadores e defesa de redes de computadores, e possivelmente, operações especiais de informação. Nós definimos guerra cinética como sendo a guerra praticada no "mundo real". Todos os tanques e navios e aviões e soldados tradicionais são os protagonistas da guerra cinética.

Considerando tais definições, visualiza-se a separação entre o mundo virtual ou cibernético e o mundo real ou cinético. Entretanto, aqueles se encontram inter-relacionados já que as ações praticadas no mundo cibernético geram conseqüência no mundo cinético, conforme expõe Carvalhais (2011, p.02).

John Arquilla e David Ronfeldt, em *Ciberwar is Coming* (1997, p.30) conceituam *Cyberwar* como a destruição de sistemas de informação e de comunicação. Aduzem que a "ciberguerra" pode ter amplas implicações para a organização militar, bem como para a doutrina com a ampliação da estratégia, sendo esta aplicável tanto em conflitos de baixa intensidade quanto alta intensidade.

Os supramencionados autores comparam a guerra cibernética a um campo de batalha. Chegam à conclusão de que há uma visão diferenciada posto que a *Cyberwar* depende menos do terreno geográfico do que a natureza eletrônica do *ciberespaço,* o qual deve ser aberto através de aplicativos de tecnologia avançada. Logo, a forma de posicionar os bancos de dados, sensores relacionados a estes, redes de comunicação podem ser tão importantes quanto tanques ou frotas de bombardeio utilizados na Segunda Guerra Mundial.

Nesta linha, corrobora a definição de Portela (2010, p. 485) a qual aduz que "a guerra é, fundamentalmente o conflito armado que envolve Estados soberanos e cujo objetivo principal é solucionar uma controvérsia pela imposição da vontade de uma das partes na disputa".

Annunciação (2003, p.9) afirma que o Departamento de Defesa dos Estados Unidos, em 1997, tentou desvendar as dimensões de suas vulnerabilidades diante ameaças cibernéticas. Consistia em invadir a rede dos EUA utilizando *softwares* disponíveis na Internet. Com isso verificaram a vulnerabilidade dos sistemas de energia e comunicação, por exemplo.

Seguindo o entendimento de Annuciação (2003, p. 6), este cita que a guerra cibernética poderia ser usada dentro do conceito de guerra irrestrita, onde seriam atacados não só alvos estratégico-militares, mas também alvos civis de um país, com a finalidade de causar uma desordem generalizada, difundindo medo. Logo

após o ataque, técnicas como ações terroristas, seriam utilizadas objetivando resistência. Com isso, elenca alvos dos ataques cibernéticos, a saber, comando das redes de distribuição elétrica, comandos das redes de comunicação em geral, os quais são denominados como infra-estrutura crítica.

Dessa forma, através de um programa ilícito, como os vírus e sistemas operacionais, é possível o ataque, transferindo informações a terceiros ou desabilitando os sistemas operacionais. Os ataques objetivam a destruição das conexões, dos equipamentos. Neste caso, visam a indisponibilidade, ou seja, fazer com que um certo serviço fique inativo, indisponível para os seus usuários, podendo durar dias. De outro lado, a terceira classe refere-se às pessoas, denominados *insiders.* Nesta classificação, ocorre a disponibilidade de senhas obtidas através de vírus, permitindo o acesso de terceiro não autorizado, bem como instalação de programas que possibilitem os ataques e modificações de hardware.

Percebe-se que, os doutrinadores em sua grande maioria, citam em comum os sistemas passíveis de riscos, ou seja, sistemas que compõem a infra-estrutura o qual possui extrema importância nacional ou até mesmo local, quais sejam: os da rede financeira, rede elétrica, sistema de controle aéreo, distribuição de água, de transportes e sistemas governamentais.

Ressalte-se a inexistência de fronteira para o uso das tecnologias da informação e os conflitos gerados. Os chamados “guerreiros virtuais” podem ser recrutados em diversos países para o ataque aos diversos sistemas citados acima.

De igual importância, faz-se necessário, considerando a exposição lógica até aqui realizada, do que se denomina de terrorismo cibernético e guerra cibernética, já que foram citados os conflitos e ataques. Por sua vez, o terrorismo cibernético se reduz ao uso do ciberespaço para fins terroristas. Em contrapartida, a guerra cibernética envolve uma situação mais ampla entre Nações, tendo como base a campanha militar.

Surgem, portanto, desafios para a prevenção de ameaças as principais infra-estruturas através de políticas de segurança. Dessa forma, fez-se necessário analisar a situação dos Grandes Eventos e a publicação de leis que especifiquem os crimes virtuais posto que grandes eventos gerem conseqüências e reflexos que anseiam por estratégias de defesa de modo preventivo e repressivo.

3. GRANDES EVENTOS: COPA DO MUNDO 2014 E OLIMPÍADAS 2016

O Brasil começou a se estruturar para a realização de grandes eventos, tais como, a Copa do Mundo que ocorreu em 2014 e as Olimpíadas em 2016.

A estrutura significa a preparação de Estados e Municípios em relação às suas infra-estruturas, construção de novos aeroportos, estádios e suas reformas, turismo e transporte público, principalmente nas áreas de acesso aos eventos e segurança pública.

Como conseqüência, a infra-estrutura vai além da construção de estádios e abrange a segurança cibernética. Assim, necessária a criação de mecanismos de defesa na rede com projetos que assegurem a atuação em rede com segurança.

Tal preocupação em planejar e definir ações especificamente de segurança para os eventos tem como base o fato de o Brasil ser um dos países com maior ocorrência de crimes cibernéticos, existindo prejuízo calculado em bilhões de dólares. Além disso, para a prática de ações ilícitas, os agentes buscarão falhas nos sistemas de segurança.

Assim, o Ministério da Defesa aprovou estratégias de defesa cibernéticas por meio da Portaria Nº 3.389, lançada em 2012 e publicada no Diário Oficial da União (BRASIL, 2012). Foi prevista a implantação de uma estrutura composta por civis e militares para desempenharem atividades de defesa a qual é estruturada por militares do Exército, Marinha e Aeronáutica. Anterior a tal Portaria, foi criada pelo Decreto 7538 (BRASIL, 2011), da Secretaria de Segurança para Grandes Eventos. Dessa forma, foi possibilitada a capacitação de policiais, principalmente, para acompanhar os responsáveis pelos ataques cibernéticos, bem como evitar danos aos sistemas tanto do governo como de cidadãos, os quais são vulneráveis de ameaças.

Houve autorização, inclusive, para a atuação das Forças Armadas contra o terrorismo, fiscalização de explosivos, agentes químicos ou nucleares em todas as cidades-sede. E, por meio da criação do Decreto Nº 7.538 (BRASIL, 2011), a Secretaria Extraordinária de Segurança para Grandes Eventos promoveu a integração de órgãos estaduais, federais, municipais e distritais para o planejamento, coordenação, implementação e acompanhamento das ações de segurança.

Ainda no ano de 2012, ocorreu a Conferência Internacional de Perícia em Crimes Cibernéticos, em Brasília, para discutir os desafios de prevenção e

investigação de crimes cibernéticos diante das vulnerabilidades tecnológicas que a Copa do Mundo de 2016 e as Olimpíadas estão sujeitas.

O diretor de inteligência da Secretaria Extraordinário de Segurança para Grandes Eventos (SESGE), Rodrigo Morais, citou que a capacitação na área de segurança pública na análise e produção de conhecimento a partir de dados e informações que circulam no ambiente cibernético, possibilita a mitigação das vulnerabilidades que ameaçam a segurança das instituições de Estado e dos eventos[7].

Ainda, dados da Agência Brasileira de Inteligência (ABIN) repassados aos deputados federais da Comissão Parlamentar de Inquéritos demonstraram que "o que se observou é que, desses dois milhões de ataques, 100 mil foram dirigidos contra governos de 200 países. Dentro dos ataques contra governos, nós temos precisamente 12.405 ataques contra serviços do governo brasileiro. "Isso é uma ameaça presente, cuja ocorrência naqueles momentos de grandes eventos se acentuou, razão pela qual se conclui que tende a ocorrer novamente"[8].

3.1 Os Riscos de Segurança

Por tratar-se de espaço cibernético e não territorial, as ameaças, sejam naturais ou intencionais como crimes, terrorismo e guerra são impulsionadas, ganhando conotação e dimensão superior. Isto porque a inserção no mundo informático principalmente devido à busca pela globalização expôs os cidadãos a uma série de riscos (Lima, 2011, p. 53).

Lima (2011, p. 53) aduz que tais riscos os quais anseiam por proteção aos bens jurídicos violentados são conseqüência da "ânsia tecnoeconômica" das diversas nações.

Com isso, a *International Telecommunication Union*, com sede em Genebra, cujo objetivo é desenvolver as telecomunicações e redes de informação, expôs os principais focos de segurança cibernética a partir da divisão entre áreas de elevada

[7] WAMBURG, Jorge. **Segurança na Internet.** Marc. 2014. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2014-03/curso-prepara-policiais-para-enfrentar-crimes-ciberneticos-na-copa> Acesso em: 21jul. 2016.

[8] Agência expõe ameaças cibernéticas contra os jogos olímpicos em CPI da Câmara. Abr. 2016. Disponível em: <http://www.abin.gov.br/agencia-expoe-ameacas-ciberneticas-contra-os-jogos-olimpicos-em-cpi-da-camara/> Acesso em 22 set. 2016.

atenção, ou seja, áreas prioritárias e áreas que necessitam de maior esforço, consideradas como áreas de extrema relevância (BRASIL, 2010).

As áreas prioritárias correspondem ao combate cibernético em nível nacional com o aumento da cultura de segurança cibernética e promoção da educação. Já as áreas relevantes consistem em desenvolvimento de pesquisas, bem como o procedimento de avaliação dos riscos e seu monitoramento (BRASIL, 2010).

No Brasil, com a vulnerabilidade do sistema de segurança cibernética, empresas, organizações e especialistas uniram-se em um movimento que colheu mais de 120 mil assinaturas. O manifesto foi criado visando à proteção, ao aumento da consciência e compreensão dos líderes, tanto empresários como governamentais para que a segurança cibernética seja visualizada como um princípio fundamental.

Pautado em quatro pontos fundamentais, o manifesto "Segurança Cibernética no Brasil – Um Manifesto por Mudanças" considerou a formação de líderes com experiência em "cibersegurança", aprimoramento da privacidade juntamente com a colaboração do setor público e transformação das pessoas em primeira linha de defesa[9].

Consoante o Manifesto, os ataques invasivos dos criminosos almejando ganho financeiro, espiões de governos e terroristas produzem efeitos devastadores sobre o país[10].

Considerando os eventos no Brasil, ressalta-se a notícia veiculada em diversos setores sobre a invasão a página do Comitê Paulista da Copa do Mundo em maio de 2014. O grupo *Anonymous* consistia uma ameaça à segurança cibernética diante a possibilidade de ataques a sites referentes à Copa do Mundo de 2014.

Quanto às Olimpíadas, a Secretaria Extraordinária de Segurança para Grandes Eventos pontuou os ataques cibernéticos como um dos principais riscos que poderiam impactar a segurança dos jogos, de modo que a repressão aos crimes cibernéticos constituiu um dos pilares de atribuições dos órgãos responsáveis pela segurança pública[11].

---

[9] Segurança Cibernética no Brasil. Um manifesto por mudanças. Disponível em: <http://www.cyber-manifesto.org/> Acesso em: 21 jul. 2016.

[10] Segurança Cibernética no Brasil. Um manifesto por mudanças. Disponível em: <http://www.cyber-manifesto.org/> Acesso em: 21 jul. 2016.

[11] Segurança nos jogos olímpicos. Jul. 2016 Disponível em: <http://www.brasil2016.gov.br/pt-br/presskit/imagens/fact-sheet-seguranca> Acesso em 23 set. 20016.

Visualiza-se que os riscos advêm, principalmente, a partir da velocidade. Esta é uma característica peculiar do delito informático que resulta da conexão mais veloz a cada dia, possibilitando a transferência de dados que passam a ser transferidos em um curto espaço de tempo (Sydow, 2013, p. 109).

Sydow (2013, p. 110) expõe que por terem os arquivos maliciosos tamanho reduzido, ingressam em aparatos alheios em segundos, de maneira imperceptível pelo usuário. Isso dificulta a proteção e o domínio dos acontecimentos.

Conclui também que é peculiaridade da velocidade, a eficiência da navegação de modo que essa se dará pela rede mundial de computadores. Tal fato contribui para o aumento dos ataques como a contaminação por *malwares*, escravização de máquinas, etc., permitindo a criação de *sites* descritos como *sites-armadilha,* os quais contêm *scripts* na página acessada que instalam arquivos no usuário que está acessando, bem como a possibilidade de ataques múltiplos e envio de mensagens comerciais não solicitadas em quantidade considerada elevada (Sydow, 2013, p. 110).

Consequentemente, a segurança cibernética constituiu um dos níveis que compreendia os pilares da segurança no planejamento estratégico de segurança na Copa do Mundo de 2014[12].

Outrossim, conforme tratado no VII Encontro Nacional da Associação Brasileira de Estudos de Defesa[13], a discussão exposta neste presente trabalho é relatada pelo governo estadunidense como um problema nacional, de modo que necessita da intervenção militar, o que remete ao *Cyberwar,* como já reportado.

Tal problemática ensejou o processo de securitização, como bem ressaltado no Encontro Nacional da Associação Brasileira de Estudos de Defesa, uma vez que o governo americano estaria ameaçado por ataques de Hackers que poderiam invadir a infra-estrutura dos transportes, sistema financeiro e as redes de computadores.

[12]Planejamento Estratégico de Segurança para a Copa do Mundo FIFA Brasil 2014. Jan 2012. Disponível em :< http://www.conectas.org/arquivos/editor/files/PlanejamentoEstrategicoSESGE%20%282%29.pdf> Acesso em 22 set. 2016

[13] VII Encontro Nacional da Associação Brasileira de Estudos de Defesa.Agos. 2013. Disponível em: <http://www.abedef.org/download/download?ID_DOWNLOAD=76> Acesso em 22.09.2016

Vê-se, portanto, que o governo americano criou o chamado *Cyberspace Policy Review*[14]*,* o qual consiste em políticas de ciberespaço para a realização de uma revolução da tecnologia da informação.

Ainda assim, as pesquisas demonstram que as ameaças persistiram de tal modo que houve um aumento de 81% nos ataques realizados por hackers em 2011[15]. Já em 2012, durante os jogos olímpicos em Londres, houve o registro de cerca de 165 milhões de incidentes de segurança e, consoante entrevista do Vice-Presidente da IBM Security "há muitos indicadores de que o nível de atividade está crescendo. O crime organizado está reforçando sua capacidade cibernética com muita rapidez"[16].

Para tanto, vê-se que anteriormente à realização dos jogos em Londres, o governo britânico realizou uma simulação para testar a sua capacidade de proteção aos ataques virtuais, de modo que utilizou 87 empresas voluntárias para simular um ataque *online* em face de bancos britânicos para visualizar o grau de dependência das tecnologias de informação e a capacidade de defesa[17].

Quanto aos riscos na África do Sul, sede da Copa do Mundo em 2010, vislumbra-se da análise feita pela SERASA EXPERIAN que operações criminosas foram realizadas para burlar sistemas e praticar fraudes contra empresas, de modo que o valor da perda devido à fraude de cartão de crédito aumentou 53% no período de realização do grande evento esportivo[18].

No Brasil, foi criado pelo Ministério da Justiça juntamente com a Secretaria de Segurança para Grandes Eventos, o planejamento estratégico o qual estabeleceu

---

[14] Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure. Disponível em: <https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf> Acesso em: 22 set. 2016.

[15] Segurança Cibernética. Proteção contra ataques. Disponível em:<http://www.trendmicro.com.br/br/tecnologia-inovacao/seguranca-cibernetica/> Acesso em: 22 set. 2016.

[16] Turistas se tornam alvos de criminosos cibernéticos em jogos olímpicos. Folha de S. Paulo. Agos. 2016.Disponível em:<http://www1.folha.uol.com.br/esporte/olimpiada-no-rio/2016/08/1799281-turistas-viram-alvos-de-criminosos-ciberneticos-nos-jogos-olimpicos.shtml> Acesso em: 22 set. 2016.

[17] Bancos fazem testes para se protegerem de ataques virtuais durante a olimpíada de Londres. Nov. 2011.Disponível em:< http://www.omelhordelondres.com/tag/hacker/> Acesso em: 22 set. 2016.

[18] Aumento no número de fraudes durante grandes eventos esportivos. Jun. 2014. Disponível em:< http://noticias.serasaexperian.com.br/copa-do-mundo-levantamento-aponta-aumento-no-numero-de-fraudes-durante-grandes-eventos-esportivos/> Acesso em: 22 set. 2016.

que a segurança do espaço compreenderia quatro níveis, a saber: aéreo, terrestre, marítimo e cibernético[19].

Quanto aos delitos cibernéticos, esses restaram previstos no planejamento, bem como o uso não autorizado dos sistemas de Tecnologia da Informação, Marketing de emboscada além de trotes e ameaças as quais poderiam ocasionar constrangimentos e até a suspensão do evento[20].

Com isso, o diretor da ABIN, Carlos Silva, em sua participação na audiência pública na Câmara dos Deputados sobre a segurança cibernética de Estado na Comissão Parlamentar de Inquérito dos Crimes Cibernéticos, afirmou que nos períodos dos jogos olímpicos, haveria a possibilidade de inúmeros ataques de roubo de senha, tentativa de *phishing* e uso de cartões de créditos de outros países, o que ocasionaria a necessidade da segurança de todos os usuários dos jogos[21].

Assim, percebe-se que além da segurança aeroportuária, controle migratório, segurança de infra-estrutura, local do evento, adequação dos sistemas de compra de ingresso, a segurança cibernética constituía uma das metas para a organização desse grande vento, considerando os riscos de segurança.

3.2 Os Delitos Informáticos nos Grandes Eventos

Considerando o grande número de usuários da rede mundial de computadores, é crescente a preocupação especialmente em relação às transferências e veiculação de informações e dados que circulam na rede (Lima, 2011, p. 73).

Lima (2011, p. 85) afirma que o principal local de acesso são as *lanhouses*, totalizando quase 31%, seguindo das próprias casas dos usurários. Sendo que a previsão para 2014 era de que o número de usuários deveria dobrar, devido à acessibilidade das tecnologias. Assim, a projeção seria de dois computadores para três pessoas. Em contrapartida à disponibilidade de acesso à rede, suscita que deve

---

[19]Planejamento Estratégico de Segurança para a Copa do Mundo FIFA Brasil 2014. Disponível em: <http://www.conectas.org/arquivos/editor/files/PlanejamentoEstrategicoSESGE%20%282%29.pdf> Acesso em: 22 set. 2016.

20Planejamento Estratégico de Segurança para a Copa do Mundo FIFA Brasil 2014. Disponível em: <http://www.conectas.org/arquivos/editor/files/PlanejamentoEstrategicoSESGE%20%282%29.pdf> Acesso em: 22 set. 2016.

[21] Segurança cibernética durante a olimpíada preocupa autoridades. Disponível em:<http://www.laadsecurity.com.br/2016/seguranca-cibernetica-durante-a-olimpiada-preocupa-autoridades/> Acesso em 12 out. 2016.

haver a segurança da informação tecnológica através de pesquisas que auxiliem na prevenção, principalmente de fraudes em documentos, assinatura eletrônica e autenticação virtual.

Verifica-se que, com a expansão do uso da Internet, a atividade comercial intensificou na rede mundial de computadores. Assim, a atividade de compra e venda passou a ser chamada de comércio eletrônico, a qual pode ser conceituada como “transações de compra e venda de mercadoria e serviços realizadas por intermédio de computadores e a Internet” (Lima, 2011, p. 87).

Desta feita, as relações comerciais foram facilitadas com o uso da Internet, já que o usuário não precisa se deslocar do seu lar, podendo efetivar um negócio em qualquer horário, com o surgimento de lojas virtuais e um sistema *on-line* crescente. Assim, o comércio eletrônico passou a ser um ramo visado pela criminalidade informática. Importante ressaltar que, quase a totalidade das transações eletrônicas comerciais pressupõem a utilização de cartão de crédito como meio de pagamento (Lima, 2011, p. 90).

Tendo em vista o comércio eletrônico gerado na Copa do Mundo de 2014 com a compra e venda de ingressos, foi criado o Projeto de Lei do Senado Nº 728 (BRASIL, 2011) o qual define os novos crimes da Copa como falsificação, revenda ilegal de ingressos e venda fraudulenta de serviço turístico[22]. Os tipos penais objetivavam a garantia dos direitos dos participantes e espectadores dos jogos.

Neste sentido, vê-se a atuação do comitê nos jogos olímpicos em face da venda ilegal de ingressos e o combate às vendas tanto no Brasil quanto no exterior, consoante se extrai de *sites,* através dos quais o próprio Comitê disponibilizou informações sobre a venda de ingressos[23], bem como há de ressaltar que, durante a realização dos jogos olímpicos, foi preso um membro do comitê por suspeita de facilitar a venda ilegal de ingressos, marketing de emboscada e formação de quadrilha[24]

---

[22]Segurança para a Copa. Disponível em: <http://www.copa2014.rs.gov.br/conteudo/2316/seguranca-para-a-copa> Acesso em: 21 jul. 2016.

[23] Rio-2016 alerta que ingressos revendidos podem ser cancelados. Folha de S. Paulo. Mai. 2016. Disponível em:<http://www1.folha.uol.com.br/esporte/olimpiada-no-rio/2016/05/1776760-grupo-da-policia-tem-sucesso-no-combate-a-venda-de-ingressos-ilegais-diz-rio-2016.shtml> Acesso em: 22.09.2016

[24] Membro do COI é preso por suspeita de venda ilegal de ingressos no Rio. Agos. 2016. Disponível em: <http://g1.globo.com/rio-de-janeiro/olimpiadas/rio2016/noticia/2016/08/membro-do-coi-e-preso-por-venda-ilegal-de-ingressos-no-rio.html> Acesso em 22.09.2016.

A compra e venda de ingressos teve grande destaque devido aos milhões de espectadores em todo o mundo objetivando assistir aos jogos no Brasil. Dessa forma, milhares de ingressos circularam na Internet durante a Copa do Mundo[25] e os Jogos Olímpicos. Entretanto, a FIFA e a COI em entrevistas e publicações, afirmaram que a única fonte oficial de ingressos para os jogos seria o *site* oficial. De imediato, declarou que o espectador que se deparasse com qualquer página da Internet comercializando ou divulgando ingressos, deveria entrar em contato com os responsáveis pela comercialização dos ingressos oficiais antes de efetuar qualquer transação não autorizada.

As tentativas não se consumaram apenas com a criação de páginas na Internet como também por meio de SMS e e-mail. Dessa forma, milhares de e-mails falsos foram enviados reiteradamente oferecendo ingressos para a Copa do Mundo, em forma de promoção.

Ao efetuar a compra online a partir do e-mail recebido, é emitido um boleto bancário para realizar o pagamento do ingresso "sorteado". Entretanto, os ingressos não chegam à residência do consumidor, gerando apenas uma expectativa[26].

Outro caso ocorrido na Copa do Mundo trata-se da simulação de sorteio, através de *sites*, o qual se passava por grande empresa de pagamentos eletrônicos. Em troca, a empresa pagaria como prêmio, valores em dinheiro ou a possibilidade de assistir aos jogos na Copa do Mundo 2014. O procedimento utilizado consistia na validação do CPF pelo usuário, bem como o fornecimento dos dados bancários[27].

Tal conduta é definida por Wendt (2012, p. 39) como *phishing.* O termo deriva da palavra inglesa *fishing,* a qual significa pescar. Logo, é a conduta daquele que pesca a informação sobre o usuário de um computador. Também se refere ao encaminhamento de mensagens cuja finalidade é induzir a vítima a preencher um formulário com dados pessoais ou a instalar códigos que transmitem ao "criminoso cibernético" as informações pessoais.

---

[25]Saiba identificar se um ingresso da Copa do Mundo é falso ou verdadeiro. Portal do Consumidor. Jun. 2014. Disponível em: <http://www.portaldoconsumidor.gov.br/noticia.asp?id=26658> Acesso em: 21 jul. 2016.

[26]Ganhe um par de ingressos para a Copa do Mundo FIFA 2014. Jun. 2014. Disponível em: <http://www.profissionaisti.com.br/2014/06/ganhe-um-par-de-ingressos-para-a-copa-do-mundo-fifa-2014/> Acesso em: 29 jul. 2016.

[27]Golpe online usa informações da Copa do Mundo para roubar dados de brasileiros. Marc. 2014. Disponível em: <http://blogs.eset.com.br/laboratorio/2014/03/14/golpe-online-usa-informacoes-copa-mundo-para-roubar-dados-brasileiros/> Acesso em 29 jul. 2016.

Wendt (2012, p. 39) afirma que, nesses casos, o agente cria uma falsa história para atrair o usuário da rede, visando ao acesso de informações para obtenção de lucro ou até mesmo causar prejuízo para as vítimas.

Em notícias veiculadas sobre a segurança dos Jogos Olímpicos, foram registradas diversas tentativas de golpe *phishing* com e-mails falsos com a intenção de furtar dados do comitê olímpico[28]

Normalmente, a vítima recebe um e-mail, clica em um *link* e é direcionado a um *site* semelhante ao que desejava acessar. Com isso, a vítima preenche formulários nos *sites* que simulavam o sorteio de ingressos, sendo os dados transmitidos diretamente para o computador do *cibercriminoso* como CPF, RG, telefone, dados bancários. Wendt ressalta que o programa pode até ter a funcionalidade de gravar todos os dados digitados, incluindo número da conta bancária, cartão de crédito e senha.

E isso foi o que ocorreu nos casos de simulação. Buscando a aquisição de ingressos, as vítimas preencheram campos, incluindo o CPF. A partir disso, o *phishing* confere a validade do documento e o próximo passo consiste em fornecer dados como código de segurança do cartão de crédito e o limite disponível. O próximo passo, depois de disponibilizados todos os dados bancários, é a simulação para mostrar que pessoas já ganharam prêmios do suposto sorteio[29].Confira-se os passos nas Figuras 1 a 3:

[28] MANNARA, Barbara. **Hackers usam sites de ingressos falsos em ataques com foco na Rio 2016**. Jun. 2016. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2016/06/hackers-usam-sites-de-ingressos-falsos-em-ataques-com-foco-na-rio-2016.html> Acesso em 22 set. 2016.

[29] Está chegando a Copa do Mundo: e as fraudes também. Abr. 2014. Disponível em: <http://blogs.eset.com.br/laboratorio/2014/04/14/esta-chegando-a-copa-do-mundo-e-as-fraudes-tambem/> Acesso em: 29 jul. 2016.

Figura 1: Primeiro Passo: Dados Pessoais

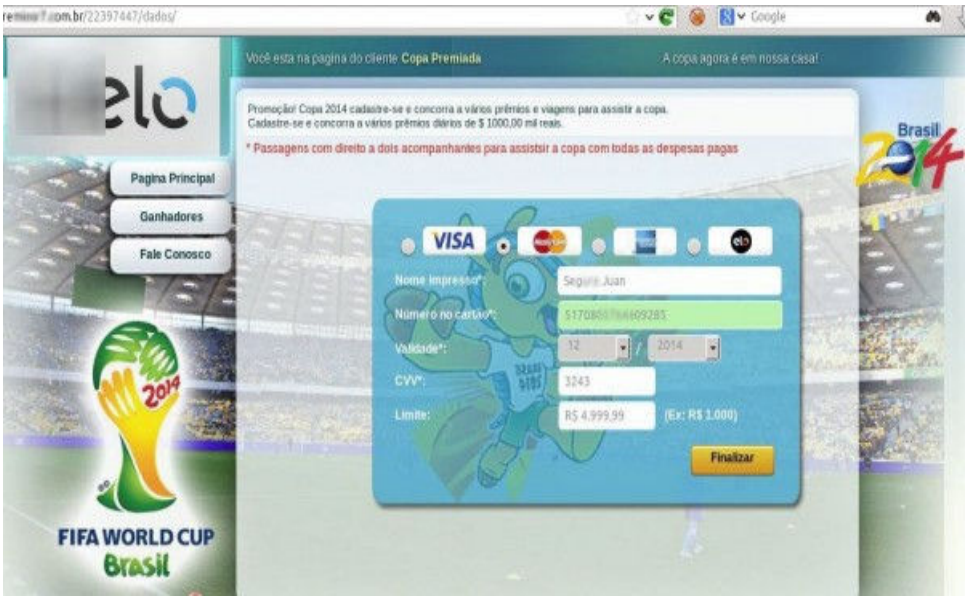


Figura 2: Segundo Passo: Dados bancários

Figura 3: Terceiro Passo: Simulação de sorteio

Fonte http://blogs.eset.com.br/laboratorio/2014/04/14/esta-chegando-a-copa-do-mundo-e-as-fraudes-tambem/

Outro exemplo de *phishing* durante a Copa do Mundo de 2014, além da simulação e venda de ingressos, consistia em um simples cadastro para participar de uma promoção, oferecendo a possibilidade de assistir “o jogo da sua vida”. A conduta é parecida com aquela exposta anteriormente. Entretanto, o que diferencia é a proposta feita a vítima. Embora pareça legítimo o e-mail recebido, ao clicar no *link,* a vítima é direcionada para outra página para que forneça os seus dados bancários[30], como mostrado nas Figuras 4 e 5:

Figura 4: E-mail promovendo a promoção

[30] Está chegando a Copa do Mundo: e as fraudes também. Abr. 2014. Disponível em: <http://blogs.eset.com.br/laboratorio/2014/03/14/golpe-online-usa-informacoes-copa-mundo-para-roubar-dados-brasileiros/> Acesso em: 29 jul. 2016.

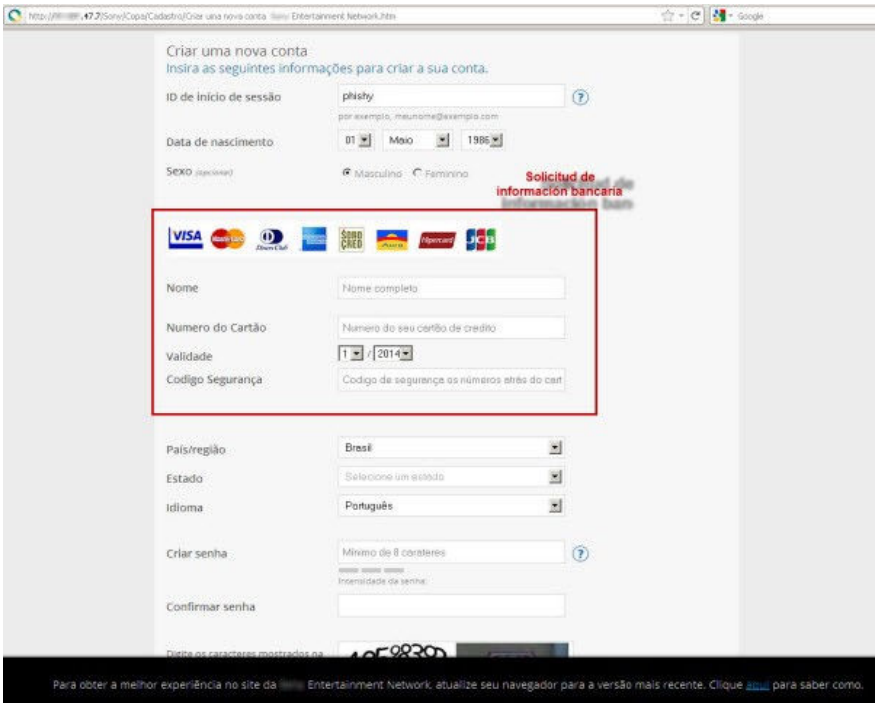
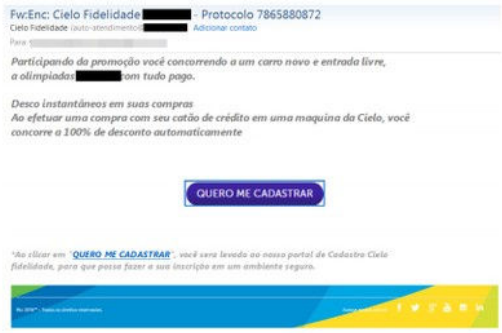


Figura 5: Cadastro através do fornecimento de dados bancários

Fonte - http://blogs.eset.com.br/laboratorio/2014/03/14/golpe-online-usa-informacoes-copa-mundo-para-roubar-dados-brasileiros/

Veja-se o que também ocorreu durante os Jogos Olímpicos:



A título de exemplificação, o Egrégio Tribunal de Justiça do Estado do Paraná julgou caso similar, tendo em vista o artifício utilizado pelo agente, qual seja, a obtenção de vantagem através de e-mail enviado pelo *site*

> *APELAÇÃO CRIMINAL - ESTELIONATO - ALEGAÇÃO - FALTA DE PROVAS DA AUTORIA - RÉU AFIRMA TER ADQUIRIDO O BEM DE TERCEIRO - DESCABIMENTO - DECLARAÇÃO DA VÍTIMA QUE ENVIOU O PRODUTO E DO ENTREGADOR MAIS APREENSÃO DO*

> *COMPUTADOR NA POSSE DO RÉU CONFIRMAM A AQUISIÇÃO DO PRODUTO JUNTO A VÍTIMA - OBTENÇÃO DA VANTAGEM ILÍCITA MEDIANTE ARTIFÍCIO ATRAVÉS DE E-MAIL SUPOSTAMENTE ENVIADO PELO `SITE' `MERCADO PAGO' CONFIRMANDO O PAGAMENTO DA MERCADORIA - FRAUDE COMPROVADA PELO E-MAIL ENVIADO PELO `SITE' `MERCADO LIVRE' AFIRMANDO A INEXISTÊNCIA DO REFERIDO PAGAMENTO - PRETENSA DESCLASSIFICAÇÃO PARA RECEPTAÇÃO CULPOSA - INVIABILIDADE - COMPROVADA ORIGEM DO BEM PELA PRÁTICA DO ESTELIONATO - RECURSO IMPROVIDO. 1. A Declaração da vítima e do entregador mais apreensão do computador na posse do réu confirmam a aquisição do produto junto a vítima e não de terceiro localizado em um Shopping da cidade. 2. O artifício usado pelo réu para obtenção da vantagem ilícita restou comprovado pelo e-mail supostamente enviado pelo site Mercado Pago' confirmando o pagamento do produto e conseqüente liberação para entrega, o qual revelou-se falso pelo recebimento de e-mail enviado pelo site `Mercado Livre' confirmando e inexistência de qualquer pagamento e aviso para não entregar a mercadoria.*(TJ-PR - ACR: 6673096 PR 0667309-6, Relator: Marques Cury, Data de Julgamento: 23/09/2010, 3ª Câmara Criminal, Data de Publicação: DJ: 487)

Wendt explica (2012, p. 74) a previsão de tais condutas, as quais são definidas como fraudes no direito penal brasileiro. Sendo umas delas, o estelionato previsto no artigo 171 do Código Penal (BRASIL, 1940). Assim, as fraudes eletrônicas configuram meio para a realização de um delito.

Imprescindível ressaltar a diferença dos casos tipificados como estelionato daqueles tipificados como furto mediante fraude, pois a diferença encontra-se na participação da vítima na concessão do patrimônio ao sujeito passivo. No furto mediante fraude, a vítima não fornece seus dados pessoais, como ocorre nos casos de cartões de crédito clonados, ocorrendo uma subtração por parte do agente através de uma fraude[31].

Mirabete (2011, p. 198) entende que:

> Distingue-se o furto mediante fraude, em que o engodo possibilita a subtração, do estelionato, em que o agente obtém a posse da coisa que lhe é transferida pela vítima por ter sido induzida a erro. Na jurisprudência, apontam-se as seguintes diferenças: no primeiro há tirada contra a vontade da vítima; no segundo, a entrega é procedida livremente; no primeiro, há discordância da vítima; no segundo, o consentimento; no furto, há amortecimento da vigilância; no estelionato, engodo; naquele, o engano é concomitante com a subtração; neste, é antecedente à entrega; a conduta do furto é de tirar, no estelionato é enganar para que a vítima entregue a coisa.

[31]CABETTE, Eduardo Luiz Santos. Furto mediante fraude e estelionato no uso de cartões de crédito e/ou débito subtraídos ou clonados: tipificação penal, competência e atribuição de polícia judiciária. Disponível em: <http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=12631&revista_caderno=3#_ftn1> Acesso em: 29 jul. 2016.

Outro não é o entendimento jurisprudencial:

> *PENAL E PROCESSUAL - CRIMES DE QUEBRA DE SIGILO BANCÁRIO (ART. 10 DA LC Nº 105/2001), DE FURTO QUALIFICADO MEDIANTE FRAUDE (ART. 155, § 4º, II, DO CÓDIGO PENAL) E DE FORMAÇÃO DE QUADRILHA OU BANDO (ART. 288 DO CÓDIGO PENAL)- CONDUTA CONSISTENTE NO EMPREGO DE FRAUDE CIBERNÉTICA, POR MEIO DA INTERNET, COM A FINALIDADE DE SUBTRAIR VALORES DEPOSITADOS EM INSTITUIÇÕES BANCÁRIAS - ABSORÇÃO, PELO FURTO QUALIFICADO, DA CONDUTA PREVISTA NO ART. 10 DA LEI COMPLEMENTAR 105/2001, DE VEZ QUE ESTA CONSTITUI, APENAS, MEIO PARA A PERPETRAÇÃO DO CRIME PRINCIPAL (PRINCÍPIO DA CONSUNÇÃO) - CRIME CONSUMADO –(...) CONCURSO MATERIAL ENTRE O CRIME DE FURTO QUALIFICADO MEDIANTE FRAUDE, EM CONTINUIDADE DELITIVA, E O DELITO DO ART. 288 DO CP - POSSIBILIDADE* - (TRF-1 - ACR: 20249 GO 2005.35.00.020249-7, Relator: DESEMBARGADORA FEDERAL ASSUSETE MAGALHÃES, Data de Julgamento: 28/07/2009, TERCEIRA TURMA, Data de Publicação: 07/08/2009 e-DJF1 p.09)

Tendo em vista o ambiente virtual, as fraudes são denominadas de fraudes eletrônicas (Wendt, 2012, p. 76). Com isso, a vítima realiza o pagamento do valor e não recebe a mercadoria prometida, no caso, os ingressos para as partidas dos jogos.

Cite-se as características dos "*sites* fraude" (Wendt, 2012, p. 76): criação de domínios e hospedagens no Brasil ou exterior: os domínios são registrados em nome de terceiros, chamados de "laranjas" ou pessoas que tiveram seus documentos subtraídos. Já o pagamento do domínio é realizado através de cartões clonados; suposta confiabilidade e credibilidade: em pesquisa na rede, há mensagens positivas, indicando aos próximos consumidores-vítimas a credibilidade e confiabilidade na compra virtual; pagamento à vista, por boleto ou depósito bancário em contas de pessoas físicas: na maioria das vezes, os dados contidos nos boletos bancários não são iguais aos disponíveis no *site*, sendo em regra, de pessoas físicas.

Considerando o fluxo de turistas que o Brasil recebeu em virtude das Olimpíadas de 2016, verifica-se a ocorrência de falsificação de cartões de crédito e débito, conduta recepcionada pela Lei 12.737 de 2012 (BRASIL, 2012).

A partir de notícias veiculadas na Internet, vê-se a preocupação das empresas e o modo de adaptação para aprimorarem os sistemas de segurança[32], tendo em vista que o Brasil ocupa a 5ª posição quanto às fraudes de cartão de crédito e 7ª posição quanto aos cartões de crédito e débito.

3.3 Prevenção

Wendt (2012, p. 41) aduz que uma das medidas para evitar que uma pessoa seja vítima é ler atentamente a mensagem já que, geralmente, há diversos erros gramaticais no e-mail. Também recomenda mover o cursor do mouse sobre o *link*, visualizando na barra de status do programa de e-mail qual o endereço descrito. Isso porque o *link* lido na mensagem pelo usuário é diferente daquele após o "clique".

Dessa forma, toma-se de empréstimo as maneiras de prevenção[33], a saber: verificação do endereço do *site*, observando se há letras a mais ou a menos, análise dos erros gramaticais nos e-mails ou páginas recebidas, acesso ao *site* Registro.br para buscar a titularidade do domínio, podendo verificar a data de registro, constatação do nome da empresa em s*ites* de busca para confirmar existência e procedência, verificar com cuidado a existência de ofertas na rede.

A Secretaria para Grandes Eventos destacou os principais riscos relativos à Copa do Mundo de 2014, enumerando-os[34]. Isso se deu a partir da experiência dos Oficiais de Inteligência da Agência Brasileira de Inteligência (ABIN) e do Sistema de Análise de Riso com Ênfase na Ameaça (ARENA).

Dessa forma, elencou a criminalidade de massa, fraudes como pirataria, falsificações de ingressos e o uso não autorizado de sistemas de TI, além de trotes e ameaças os quais ocasionam constrangimentos e até a suspensão de eventos. Enumeraram o terrorismo como uma das áreas de riscos, pois a realização de um

---

[32] Penta campeão da Copa, Brasil é o 5ª país no ranking mundial de fraudes de cartão de crédito. Jan. 2014. Disponível em: <http://www.e-konomista.com.br/a/penta-campeao-da-copa-brasil-e-o-5-pais-no-ranking-mundial-de-fraudes-de-cartao-de-credito/> Acesso em: 29 jul. 2016.

[33] Ganhe um par de ingressos para a Copa do Mundo FIFA 2014. Jun. 2014. Disponível em: <http://www.profissionaisti.com.br/2014/06/ganhe-um-par-de-ingressos-para-a-copa-do-mundo-fifa-2014/> Acesso em: 29 jul. 2016.

[34] Planejamento Estratégico de Segurança para a Copa do Mundo FIFA. Disponível em: < Brasil 2014. http://www.conectas.org/arquivos/editor/files/PlanejamentoEstrategicoSESGE%20%282%29.pdf> Acesso em: 29 jul. 2016.

grande evento é um acontecimento que atrai ações de grupos terroristas e os cuidados devem abranger o período do evento quanto a sua preparação para que as ações sejam detectadas e neutralizadas[35].

Em relação aos jogos olímpicos, a Secretaria para Grandes Eventos pontuou que a segurança e defesa cibernética compreende as ações de segurança e defesa que visam a contribuir para a proteção dos ativos de informação, bem como dos sistemas de tecnologia de informação e comunicações (TIC's) que sustentam as estruturas para coordenar as ações de segurança e defesa cibernética[36].

Para tanto, foi estabelecida a composição da atividade inteligência para a segurança dos jogos Rio 2016, como exemplo, a coordenação do Sistema Brasileiro de Inteligência (SISBIN), cooperação internacional, avaliações de riscos, pesquisas para credenciamento visando identificar fatos relevantes que envolvam nomes de pessoas que participaram dos jogos, segurança da tecnologia da informação e das comunicações para promover a segurança dos dados e conhecimento de inteligência entre os centros e seus respectivos usuários, emprego de observadores de inteligência para a coleta de dados e o desenvolvimento de atividades de inteligência relacionadas à prevenção e ameaças terroristas.[37]

Em uma breve consideração, visualiza-se a preocupação das secretarias de segurança quanto aos riscos e prevenção de tais delitos diante a informação de que os números no universo da Segurança da Informação cresceram de modo que os torcedores, os quais estavam no Maracanã na final da Copa do Mundo de 2014 enviaram cerca de 12 TB (Terabytes) de seus smartphones. Em contrapartida, na Copa do Mundo de 1998 realizada na França, os espectadores geraram apenas 2 MB (Megabytes) utilizando mensagens de texto. Já em comparação com a Copa do Mundo de 2006, na Alemanha, o volume de dados gerados totalizou 30 GB (Gigabytes)[38].

---

[35]Planejamento Estratégico de Segurança para a Copa do Mundo FIFA Brasil 2014. Disponível em: <http://www.conectas.org/arquivos/editor/files/PlanejamentoEstrategicoSESGE%20%282%29.pdf> Acesso em: 29 jul. 2016.

[36] Segurança nos jogos olímpicos e Paralímpicos Rio 2016. Jul. 2016. Disponível em: <http://www.brasil2016.gov.br/pt-br/presskit/imagens/fact-sheet-seguranca> Acesso em: 23 set. 2016.

[37] Segurança nos jogos olímpicos e Paralímpicos Rio 2016. Jul. 2016. Disponível em: <http://www.brasil2016.gov.br/pt-br/presskit/imagens/fact-sheet-seguranca> Acesso em: 23 set. 2016.

[38]SOUZA, Denis Augusto Araújo. 2015, O ano do Cibercrime. Disponível em: <http://convergecom.com.br/tiinside/seguranca/artigos-seguranca/06/02/2015/2015-o-ano-cibercrime/#.VUT74iFViko> Acesso em: 29 jul. 2016.

Considerando tamanha troca de informações, além dos riscos já enumerados como a criação de sites falsos para a venda de ingressos, destaca-se o vazamento de informações e as aplicações falsas do evento para *smartphones*.

Como bem ressaltou a Secretaria de Segurança para Grandes Eventos, exposto anteriormente, a segurança deve ser feita de modo preventivo, ou seja, antes da realização do evento e de modo repressivo, durante a realização do evento. Isso porque houve ameaças passíveis de realização durante o evento, seja a Copa do Mundo já realizada em 2014 e as Olimpíadas realizadas em 2016, a saber: ataques de negação de serviço; disseminação de vírus em dispositivos móveis em estádios; ataques ao sistema de energia visando à paralisação do evento ou bloqueio das comunicações; ataques aos sistemas de fornecimento de água, resfriamento, portas automáticas, elevadores, etc.

Considerando os riscos nos grandes eventos, Vianey, Delegado da Polícia Federal, atuante na Repressão a Crimes Cibernéticos, afirmou que “ataques assim tomam proporção ainda maiores já que o país fica em evidência no cenário mundial, representando riscos e oportunidades”, devendo haver um preparo para combater a criminalidade cibernética[39].

Visando à proteção, em 2012, o governo brasileiro destinou aproximadamente 90 milhões de reais ao Centro de Defesa Cibernética do Exército para a segurança das redes. A preocupação era oferecer antecipadamente a segurança a Rio+20, da ONU e após, a preparação da segurança para a Copa do Mundo de 2014 e para as Olimpíadas de 2016[40].

Sendo assim, as Forças Armadas desempenharam atividades de coordenação, gerenciamento e segurança[41]. Para isso, foi criado o Centro de Defesa Cibernética (CDCIBER) em 2013 cujo objetivo principal é coordenar e integrar as

---

[39]COUTINHO, Mateus. PF vê riscos emergentes de ataques de Hackers e fraudes eletrônicas em 2014. Dez. 2013. Disponível em: <http://politica.estadao.com.br/blogs/fausto-macedo/pf-ve-riscos-emergentes-de-ataques-de-hackers-e-fraudes-eletronicas-em-2014/> Acesso em: 02 agos. 2016.

[40]Brasil encara desafios da cibersegurança. Out. 2012. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/8388/brasil-encara-desafios-da-ciberseguranca> Acesso em: 02 agos. 2016.

[41]Forças Armadas Brasileiras terão papel fundamental nos jogos olímpicos Rio 2016. Nov. 2014. Disponível em: <http://dialogo-americas.com/pt/articles/rmisa/features/2014/11/05/feature-09> Acesso em: 02 agos. 2016.

ações de defesa e segurança cibernéticas contra ações cibernéticas hostis, colaborando com as medidas de segurança do Grande Evento[42].

Uma das ações de defesa conta com um simulador de conflitos digitais. Por meio dele, são realizadas operações de guerra, simulação, estratégias de defesa e ataque, por exemplo, o ataque de negação em que há inúmeros acessos instantâneos e o sistema não consegue atender as conexões ou até mesmo quando um *site* ou um aplicativo é recriado para coletar dados de quem acessa[43].

O simulador de guerra cibernética, denominado de SIMOC, é uma tecnologia brasileira fornecida por uma das empresas estratégicas para a Defesa Nacional e permite, inclusive, a simulação de cenários como a rede interna de uso pessoal ou de uma empresa de energia elétrica[44].

Ressalte-se que tal colaboração se deu devido à aprovação do Decreto Nº 6.703 (BRASIL, 2008) o qual considera a existência de três setores estratégicos de defesa, quais sejam: nuclear, cibernético e espacial. Assim, o Decreto estabelece que ao lado da destinação constitucional, os três setores citados são decisivos para a defesa nacional, devendo as forças armadas operar em rede, entre si e em ligação com o monitoramento do território.

Já Muioio (2006, p. 183) coloca algumas dicas para o usuário da rede como o monitoramento das movimentações financeiras, devendo o usuário ficar atento aos débitos e transações; não publicar informações pessoais como telefone, dados da rotina na rede; alterar a configuração do navegador para restringir a execução de JavaScript, de softs Java e Activex ou automáticos e de pop-ups. Não execute programas desconhecidos obtidos por *download* ou por e-mail e outras.

Em relação aos *sites* fraudulentos cujo objetivo é enganar os usuários, como nos casos das compras de ingressos para os grandes eventos, o CERT.BR também elencou modos de prevenção[45]: realizar uma pesquisa de mercado para comparar o preço do produto exposto no *site,* desconfiando caso o valor seja abaixo do

---

[42] 3º Fórum Brasileiro de CSIRTS. Centro de Defesa Cibernética. Disponível em: <http://www.cert.br/forum2014/slides/ForumCSIRTs2014-CDCiber.pdf> Acesso em: 02 agos. 2016.

[43] Exército brasileiro incluirá Argentina em treinamento de guerra cibernética. Mai. 2014. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/15424/Exercito-brasileiro-incluira-Argentina-em-treinamento-de-guerra-cibernetica/> Acesso em 02 agos. 2016.

[44] Exército brasileiro incluirá Argentina em treinamento de guerra cibernética. Mai. 2014. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/15424/Exercito-brasileiro-incluira-Argentina-em-treinamento-de-guerra-cibernetica/> Acesso em 02 agos. 2016.

[45] Cartilha de Segurança para Internet. Disponível em: <http://cartilha.cert.br/golpes/> Acesso em 02 agos. 2016.

oferecido no mercado; pesquisar sobre a procedência do *site* antes de efetuar a compra, verificando a opinião de clientes anteriores; acessar *sites* especializados em reclamação de consumidores para verificar se existem reclamações da empresa contratante; máxima atenção com as propagandas recebidas por meio de *spam*.

Por fim, faz-se necessário manter-se informado sobre as novas formas de golpes através de consultas como, por exemplo, nos *sites* das empresas mencionadas nas mensagens, bem como *sites* especializados como o Monitor de Fraudes[46].

4. ANÁLISE DO ORDENAMENTO JURÍDICO

Diante o exposto até aqui, os delitos informáticos demandam a evolução da legislação. Com isso, o Direito deu os seus primeiros passos, nas palavras de Fiorillo (2013, p. 94), rumo à informatização. Sendo assim, a Justiça acelerou os procedimentos judiciais à medida que tentou se adaptar às inovações tecnológicas.

Em que pese algumas condutas já estarem previstas na legislação brasileira, nota-se que há práticas delitivas que necessitam de previsão legal para que adquiram tipicidade (Firorillo, 2013, p. 172), ou seja, para que a conduta seja punível, consoante o princípio da Legalidade exposta no artigo 5º, inciso XXXIX da Constituição Federal (BRASIL, 1988) e artigo 1º do Código Penal (BRASIL, 1940).

Tendo em vista as condutas praticadas através dos computadores, o bem jurídico deve ser protegido pela norma penal, podendo ser o patrimônio ou a honra, por exemplo.

Sendo assim, surgiram iniciativas por parte do Poder Legislativo com o objetivo de tipificar as condutas praticadas através dos computadores. Foi criado o Projeto de Lei Nº 84/99 o qual continha como ideia inicial, a busca por definições e criminalização de condutas de dano informático, obtenção indevida de dados, etc (Sydow, 2013, p. 273).

Cite-se também o Projeto de Lei Nº 2.126/2011, conhecido como Marco Civil da Internet, cujo objetivo era apresentar definições e expressões usadas no direito de informática, regrar as circunstâncias de atuação dos usuários e provedores (Sydow, 2013, p. 271).

[46] Monitor das Fraudes. Disponível em: <http://www.fraudes.org/> Acesso em: 02 agos. 2016.

Em contrapartida, Kaminski (2011, p. 97) aduz que a função do operador do direito deve ser encontrar soluções dentro do ordenamento, e não esperar soluções do Poder Legislativo. Logo, o jurista deve se orientar através de instrumentos da hermenêutica, com a finalidade de atualizar a norma e trazer à realidade jurídica do novo presente século.

Contudo, cria-se a necessidade de analisar as Leis vigentes no ordenamento jurídico brasileiro, bem como um estudo comparado de modo a verificar as técnicas de segurança tomadas por países como a África do Sul, que sediou a Copa do Mundo, o Canadá, que sediou os Jogos de Inverno e o Brasil, sede da Copa do Mundo de 2015 e Jogos Olímpicos, como exemplo.

4.1 O ordenamento jurídico brasileiro

Inicialmente, cumpre ressaltar que a Lei nº 12.663 de 5 de junho de 2012 dispõe sobre as medidas referentes à Copa das Confederações em 2013, Copa do Mundo de 2014 e à Jornada Mundial da Juventude realizada em 2013[47].

A criação das normas deu-se pela imprescindibilidade para a efetivação das propostas desenvolvidas e assumidas pelo Governo Federal perante a FIFA[48], devido à escolha do Brasil como sede dos grandes eventos.

Consoante o exposto na apresentação da referida Lei (BRASIL, 2012), apesar de o campeonato ter sido criado por uma instituição privada, os esforços demandam iniciativas governamentais para garantir medidas administrativas, legais e financeiras, indo além da garantia de serviços de infraestrutura urbana.

Inicialmente, deve ser observado que a Lei Geral da Copa estabelece prazo determinado para vigência das normas penais no artigo 36. Sendo assim, caracteriza-se por ser uma norma penal temporária com data certa para entrar em vigor e data final no ordenamento jurídico. Assim dispõe o artigo 36 da Lei 12.633 (BRASIL, 2012):

---

[47] DUARTE, Pedro. Lei Geral da Copa: disposições penais temporárias. Out. 2012. Disponível em:<http://www.egov.ufsc.br/portal/conteudo/lei-geral-da-copa-disposi%C3%A7%C3%B5es-penais-tempor%C3%A1rias-0> Acesso em: 22 set. 2016.

[48] D'URSO, Adriana Filizzola. Parecer Lei Geral da Copa (Lei nº 12.663/2012 e PL 728/2011).Análise da Parte Criminal. Disponível em:<http://www.grupas.com.br/parecer-penal.pdf> Acesso em: 22 set. 2016.

> Art. 36. Os tipos penais previstos neste capítulo terão vigência até o dia 31 de dezembro de 2014.

Sobre a Lei temporária, o Código Penal (BRASIL, 1940) dispõe:

> Art. 3º - A lei excepcional ou temporária, embora decorrido o período de sua duração ou cessadas as circunstâncias que a determinaram, aplica-se ao fato praticado durante sua vigência.

Considerando o texto de Lei, foi criado o Projeto de Lei do Senado (PLS 728/2011) criando tipos penais os quais não constam no Código Penal Brasileiro como a violação de sistema informático e a revenda ilegal de ingressos com a finalidade de complementar a Lei Geral da Copa.

Encontra-se também a previsão, em projeto de Lei, dos crimes praticados através da Internet como violar, bloquear ou dificultar o acesso à página da Internet, sistema de informática ou banco de dados utilizado pela organização dos eventos, com pena fixada de um a quatro anos de prisão, além de multa.

Apesar dos benefícios trazidos com a entrada em vigência da Lei Geral da Copa, há questionamentos e críticas quanto ao alcance da norma. D'Urso anota[49], em seu parecer, que os dispositivos visam à proteção dos interesses dos organizadores, patrocinadores e participantes dos eventos em detrimento dos interesses coletivos, ou seja, da população brasileira.

Deve ser observado que os grandes eventos demandam uma adaptação da legislação já que a Internet passou a ser um meio de viabilizar o consumo em massa a nível global, como ressalta Kaminski (2011, p. 187).

Sakamoto afirma[50] que as primeiras leis surgiram nos Estados Unidos, bem como adaptações e ajustes originados da demanda de uma "cultura baseada em pessoas ligadas à informática", criando uma expectativa de criação de normas em outras partes do mundo.

Importante fazer uma ponte entre a anotação de Sakamoto e a Lei Nº 12.633 quanto o autor conclui que a rede mundial de computadores origina uma demanda a

---

[49] D'URSO, Adriana Filizzola. Parecer Lei Geral da Copa (Lei nº 12.663/2012 e PL 728/2011). Análise da Parte Criminal. Disponível em: <http://www.grupas.com.br/parecer-penal.pdf> Acesso em: 22 set. 2016.

[50] SAKAMOTO, Marcos. O Direito das Gentes e a Informática. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/29184-29202-1-PB.html> Acesso em: 22 set. 2016.

qual tem identidade própria e está ligada a uma cultura uniforme baseada na informática e não em uma demanda apenas regional. Isso porque há um fenômeno global e inexistem fronteiras políticas e físicas. Dessa forma, ensina que as jurisdições devem se organizar e uniformizar uma norma que atenda efetivamente, e de forma comum, os usuários da rede mundial de computadores[51].

A crítica quanto à Lei Geral da Copa feita por diversos autores, dá-se no sentido de que os direitos individuais devem ser respeitados preservando os valores socioculturais.

Nesse sentido, Kaminski anota (2011, p. 187):

> "Visão global, regulamentação dinâmica e célere, respeito aos direitos individuais com a preservação dos valores socioculturais, cooperação em nível de política criminal e de polícia, são alguma das metas que precisam ser perseguidas a fim de que consiga dar regulação às relações na Internet".

Em contrapartida, há quem sustente como afirma Sakamoto, a existência de uma lei específica para tratar do assunto dos chamados crimes informáticos, tipificando os delitos cometidos por meio do computador e há quem sustente que a previsão no Código Penal dos tipos penais como o estelionato, são suficientes. Ainda que, exista Lei definindo determinadas condutas realizadas por meio de computadores, como será explanado a seguir, a indagação sobre a ausência de previsão específica na Lei Geral da Copa encontra resposta na afirmação de Sakamoto quando afirma que realmente a legislação vigente está capacitada para solucionar determinados problemas, porém, existem tipos penais que necessitam de definição e tipificação em lei, uma vez que alguns atos através dos computadores poderiam ser caracterizados como crime.

4.2 Lei nº 12.737 de 2012

A Lei Nº 12. 737 de 30 de novembro de 2012, publicada no Dário Oficial da União em 03 de dezembro de 2012, chamada de Lei Carolina Dieckmann, dispõe sobre a tipificação dos delitos informáticos.

---

[51] SAKAMOTO, Marcos. O Direito das Gentes e a Informática. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/29184-29202-1-PB.html> Acesso em: 22 set. 2016.

No artigo 2º, visualiza-se que o legislador criou uma norma penal que passou a integrar o Código Penal Brasileiro, qual seja, a invasão de dispositivo informático com a seguinte redação (BRASIL, 2012):

> 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.

Sydow enumera as características para a configuração do delito em análise (2013, p. 291): a existência de uma invasão ou uma tentativa de invasão de um dispositivo informático; o dispositivo informático não pode ser de titularidade do agente invasor, ou seja, deve ser de outrem; o dispositivo pode estar conectado à rede de computadores ou não.

Ensina, ainda, que em que pese o elemento do tipo seja a existência de um dispositivo informático, não há menção à definição do que seria o dispositivo, bem como suas delimitações. A partir dessa consideração, conceitua dispositivo informático como qualquer *hardware* que trabalhe com o trato automático de informações e tenha capacidade de armazenamento de dados (Sydow, 2013, p. 291).

Sobre esse tema, vislumbra-se a primeira crítica do autor, qual seja, a exclusão de serviços exclusivamente on-line por ausência de suporte ou dispositivo, bens imateriais os quais são chamados de *softwares* e aparelhos eletrônicos que não possuem a finalidade de armazenar dados resguardados de sigilo como relógios digitais (Sydow, 2013, p. 291).

Expõe a segunda crítica a qual incide sobre o núcleo do tipo, o verbo “invadir”. Sydow explica que o dispositivo informático é o alvo do agente que ingressa sem o consentimento do titular. Dessa forma, o significado do verbo vai além do mero ingresso com o objetivo de superar as barreiras de sigilo, objetivando dados específicos.

Posto isso, explica o autor (Sydow, 2013, p. 292):

> “Acreditamos ser imprescindível que o dolo seja o de afetar dados ou informações específicas, bem como que as mudanças em arquivos ocorridas com a mera finalidade de ingresso no sistema (por exemplo leitura dos arquivos de *log* para descobrimento da senha de acesso a uma

> determinada pasta), por si sós, não bastam para a caracterização do delito por serem meramente meio e não finalidade do agente. Isso porque não restou como conduta tipificada o mero ingresso desautorizado sem finalidade específica. Vinculou o legislador a conduta de ingresso forçado à finalidade do agente acerca de dados ou acerca de vantagem.”.

Destarte, se o dispositivo tiver desprotegido totalmente, não haverá a possibilidade de consumação da invasão, pois deve haver, necessariamente, a violação de segurança. Com isso, faz-se um paralelo entre o delito tipificado com o advento da Lei 12.737/2012 e os casos ocorridos durante a Copa do Mundo e aqueles os quais poderão ocorrer durante as Olimpíadas de 2016.

Como explanado anteriormente, através do *phishing*, o agente invasor adquire as informações necessárias ou faz com que a própria vítima desabilite a segurança para possibilitar o livre acesso do agente. O delito somente será configurado se houver a violação indevida da segurança do computador diante a existência do verbo núcleo do tipo penal. Assim, resta definido que a conduta será punível se houver, além da violação indevida, “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”[52].

Já o §1º refere-se a quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput do artigo 154-A da Lei Nº 12.737 (BRASIL, 2012).

A partir da análise do parágrafo citado, visualiza-se as condutas definidas como ataques DDoS, conhecidos como ataques de negação de serviços distribuídos, como explica Kaminski (2011, p. 165).

Inúmeras notícias publicadas nos meios de comunicação relatam os ataques aos *sites* governamentais, aos patrocinadores e companhias parceiras da organização da Copa do Mundo[53]. E tais ataques são definidos como DDoS.

Como explica Kaminski (2011, p. 165), os ataques de negação de serviço consistem em impedir o normal funcionamento de determinados serviços na Internet e ocorre com a invasão de computadores que se encontram desprotegidos. Com o

---

[52] Análise da Lei 12.737/12 “Lei Carolina Dieckamnn”. Abr. 2013. Disponível em: <http://politicacidadaniaedignidade.blogspot.com.br/2013/04/analise-da-lei-1273712-lei-carolina.html> Acesso em: 22 set. 2016.

[53] Hackers atacam sites voltados à Copa no Brasil. Portal G1. Jun. 2014. Disponível em: < http://g1.globo.com/tecnologia/noticia/2014/06/hackers-atacam-sites-voltados-a-copa-no-brasil-20140611153504964214.html> Acesso em 22 set. 2016.

auxílio de vírus, instala no equipamento invadido um programa zumbi. Dessa forma, as máquinas atacadas passam a obedecer ao comando central e solicitam intensa quantidade de informações aos servidores e, com a sobrecarga, o servidor resta paralisado.

Dessa forma, o controle remoto configura o crime tipificado no artigo 154-A da Lei Nº 12.737/2012 e o ataque propriamente dito configura o artigo 266 do Código penal o qual foi alterado pelo artigo 3º da referida Lei, a saber:

> Art. 266 § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

Como exemplo, podem ser citados os ataques de negação de serviço contra os grandes eventos ou alvos específicos, em campanhas de hacktivismo e ataques para a execução de inúmeros acessos aos *sites* oficiais para impedir o acesso ou bloqueio de contas dos usuários.

Além disso, o artigo 3º da Lei Nº 12.737/2012 alterou o artigo 298 do Código Penal, passando a ter a seguinte redação (BRASIL, 2012):

> Art. 298. Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.” (NR)

Inicialmente, o artigo 298 continha apenas o caput definindo a falsificação de documento particular, a saber:

> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
> Pena - reclusão, de um a cinco anos, e multa.

Percebe-se, então, a tipificação de condutas praticadas durante os grandes eventos, principalmente aquelas que já ocorreram durante a Copa do Mundo de 2014. A partir da intensificação da movimentação financeira devido ao fluxo de turistas que o Brasil recepcionou, a utilização de cartões de crédito e débito também se intensificaram.

Entre as fraudes, destacam-se a clonagem de cartões de crédito e o aumento de compras com tais cartões clonados. Para tanto, pesquisas retratam que o Brasil é o 5º país em um ranking de fraudes envolvendo cartões de crédito e o 7º país em

fraudes as quais incluem cartões de débito e crédito[54]. Importante anotar, também, que as pesquisas relatam que a cada segundo, há uma tentativa de fraude de cartão de crédito.

Não obstante a tipificação de tais condutas a partir da referida Lei, Kaminski (2011, p. 167) conclui que mais importante do que um remédio jurídico que viabilize e minimize os prejuízos causados, é imprescindível a prevenção de tais condutas, ataques por meio de mecanismos de segurança, objetivando a manutenção dos dados e informações disponíveis, garantindo o funcionamento normal dos serviços.

Aduz, ainda, que as empresas e organismos devem fazer o uso de recursos tangíveis, quais sejam, infra-estrutura, *software*, *hardware*, e os intangíveis como elementos éticos e legais de segurança para viabilizar o fluxo de dados e informações no sistema mundial (Kamisnki, 2011, p. 168).

Por fim, importante frisar o que ensina Kaminski (2011, p. 168):

> "No ambiente virtual, os atos ilícitos são produzidos com a mesma facilidade que no ambiente real. Ao pretender tutelar o bem jurídico do cidadão, o Direito deve necessariamente acompanhar toda essa evolução, a fim de possibilitar tal garantia. Somente assim, poderá se falar na utilização (com responsabilidade), dos recursos que a Internet em sua totalidade oferece.".

5. CONCLUSÃO

Consoante o exposto no presente trabalho, resta visível a transformação do conceito de território, tendo em vista que este não mais se restringe às barreiras terrestres, sendo uma característica da conexão cada vez mais célere que interliga indivíduos por meio de tecnologias da informação, como o computador, criando o chamado ciberespaço.

Ocorre que, por tratar-se de espaço cibernético e não territorial, as ameaças, sejam naturais ou intencionais como crimes, terrorismo e guerra ganham proporção ainda maior, tornando o usuário das tecnologias cada vez mais vulnerável.

---

[54] Penta Campeão da Copa, Brasil é o 5ª país no ranking mundial de fraudes de cartão de crédito. Disponível em: < http://www.e-konomista.com.br/a/penta-campeao-da-copa-brasil-e-o-5-pais-no-ranking-mundial-de-fraudes-de-cartao-de-credito/> Acesso em 22 set. 2016.

Surgem, portanto, desafios para a prevenção de ameaças às principais infra-estruturas através de políticas de segurança, bem como a necessidade de adaptação e evolução do Direito de acordo com as relações advindas do uso das tecnologias.

De tal modo, a partir dos grandes eventos ocorridos, principalmente no Brasil, cresceu a movimentação de informações veiculadas por meio dos computadores, o que gerou a imprescindibilidade da publicação de leis que especifiquem os crimes virtuais posto que grandes eventos ensejam conseqüências e reflexos que anseiam por estratégias de defesa de modo preventivo e repressivo.

Vê-se, portanto, que os grandes eventos se revelaram como um meio de cometimento de delitos informáticos, originando a importância de haver uma política nacional de segurança cibernética, já que nem todas as condutas estão tipificadas no ordenamento jurídico.

Tais delitos, os crimes cibernéticos ou informáticos, são conceituados como qualquer conduta em que se utiliza como ferramenta o computador de alguma forma, seja como facilitador da execução ou da consumação, tendo uma característica peculiar, qual seja, o fato de o delito poder ser praticado no próprio domicílio do sujeito, uma vez que independe da localização geográfica, já que basta a utilização do computador ou da Internet.

Com isso, faz-se necessária a regulamentação e tipificação das condutas como restou demonstrado com a análise da Lei Nº Lei Nº 12.663/2012. Em que pese a Lei Geral da Copa não ter se aprofundado e especificado os delitos informáticos, existiu uma preocupação, ainda que superficial, de tutelar os bens jurídicos, ao tipificar como crime a reprodução ou falsificação de símbolos oficiais e a venda de ingressos não autorizados.

A crítica feita pelos doutrinadores quanto a Lei Geral da Copa se deu no sentido de que há a necessidade de lei específica para tratar dos crimes informáticos, uma vez que a legislação vigente é deficiente para solucionar os problemas decorrentes da utilização das tecnologias da informação.

Já a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, trata dos delitos informáticos, criando uma norma penal, qual seja, a invasão de dispositivo informático que passou a integrar o Código Penal.

Quanto a esta Lei, levantou-se um questionamento em se tratando da consumação da invasão, tendo em vista que o delito resta configurado quando

houver a violação indevida da segurança do computador, ou seja, deve haver a finalidade de obter, adulterar, destruir dados, informações ou instalar vulnerabilidade para obter uma vantagem ilícita.

Também restou tipificado na referida Lei o ataque de negação de serviço, uma vez que o art. 266, §1º dispõe que incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

Os doutrinadores explicam que os ataques de negação de serviço constituem na invasão de computadores, principalmente os governamentais, para impedir o funcionamento da rede, de modo que passam a sobrecarregar o servidor para que este seja paralisado, exatamente como ocorreu com os *sites* oficiais.

No que tange ao comércio eletrônico, houve uma intensa preocupação dos comitês olímpicos quanto à venda dos ingressos dos jogos devido à falsificação e venda ilegal.

Isso porque muitos usuários receberam e-mails com informações atrativas para a compra de supostos ingressos e sorteios online, conduta conhecida como *phishing*, a qual se refere à obtenção de informações através do encaminhamento de mensagens na rede mundial de computadores com o objetivo de capturar informações pessoais para serem utilizados por terceiros como número de cartões, documentos pessoais, dados bancários, etc.

Vislumbra-se que tais informações são repassadas pelo usuário, uma vez que estes acreditam que os *sites* acessados ou e-mails recebidos possuem credibilidade. Para tanto, tais domínios passam uma suposta credibilidade para a vítima através de ilustrações que necessitam de uma análise pormenorizada.

Para essa análise e prevenção, os doutrinadores citam a verificação do endereço do site atentamente, observando se há letras a mais ou a menos, verificação de erros gramaticais, titularidade do domínio, verificação do nome da empresa em *sites* de busca para confirmar a procedência e existência, bem como a não publicação de informações pessoais na rede e atenção às movimentações financeiras.

De outro lado, vislumbra-se que deve haver a promoção da educação, a qual seria uma linha de frente ao combate aos crimes informáticos, consistindo em uma das áreas que merecem prioridade.

Isso porque, com a difusão de informações sobre a utilização dos meios tecnológicos e conhecendo os riscos que podem ser ocasionados, avaliando-os e monitorando-os, seria possível criar um mecanismo de proteção e redução de tais delitos com o auxílio conjunto do ordenamento jurídico, através da tipificação de condutas que lesione bens jurídicos.

Dessa forma, visualiza-se que a principal medida de proteção contra os crimes cibernéticos depende dos usuários e de políticas de segurança à medida que aquele que utiliza as tecnologias precisa conhecer os riscos e perigos escondidos na rede mundial de computadores.

Por fim, cumpre ressaltar que a evolução da velocidade e das informações, devem ser acompanhadas pela evolução do ordenamento jurídico e de mecanismos próprios de defesa, prevenção e repressão de condutas que não ocorrem necessariamente dentro de campos de futebol ou ginásios olímpicos, e sim por meio de tecnologias da informação como os computadores, os quais milhões de pessoas figuram como expectadores pela rede mundial de computadores.

REFERÊNCIAS

AGUIAR, Arlete Figueiredo. Muioio, Malu. **Crimes na Rede.** São Paulo: Companhia Limitada, 2006.

ANNUNCIAÇÃO, João Wander Nascimento de. **Ciberwar*:*** uma proposta genérica de ações defensivas para a Marinha do Brasil. 2003, Escola Naval de Guerra.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal:** Parte Geral 1. 15ª Ed. São Paulo: Saraiva, 2010.

BLOG DO LABORATÓRIO. **Está chegando a Copa do Mundo: e as fraudes também.** Disponível em: <http://blogs.eset.com.br/laboratorio/2014/04/14/esta-chegando-a-copa-do-mundo-e-as-fraudes-tambem/>. Acesso em: 29 jul. 2016.

BRASIL, Decreto- Lei nº2.848, 7 de dezembro de 1940. **Diário Oficial**, Brasília, 1940. Disponível em: Acesso em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm> Acesso em: 02. out. 2016. BRASIL, Decreto nº 6.703 de 18 de dezembro de 2008. Aprova a estratégia Nacional de Defesa e dá outras providências. **Diário Oficial da União**, Brasília, DF, 18 dez. 2008.

BRASIL, Lei nº 12.373 de 30 de novembro de 2012. **Diário Oficial da União**, Brasília, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 02. out. 2016.

BRASIL, Lei nº 12.663 de 5 de junho de 2012. **Diário Oficial da União**, Brasília, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Lei/L12663.htm>. Acesso em: 02. out. 2016.

BRASIL, Lei nº 8.069 de 13 de julho de 1990. **Diário Oficial da União**. Brasília, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/l8069.htm>. Acesso em: 02. out. 2016.

BRASIL, Projeto de Lei nº 728 de 2011. Disponível em:<http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=103652>. Acesso em: 02. out. 2016.

BRASIL, Decreto n.7.538 de 1 de agosto de 2011. Altera o Decreto nº 6.061, de 15 de março de 2007, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções Gratificadas do Ministério da Justiça, remaneja cargos em comissão, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 21 dez. 2012.

CABETTE, Eduardo Luiz Santos. **Furto mediante fraude e estelionato no uso de cartões de crédito e/ou débito subtraídos ou clonados:** tipificação penal, competência e atribuição de polícia judiciária. Disponível em: <http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=12631&revista_caderno=3#_ftn1> Acesso em: 29 jul. 2016.

CAMELO, José Ricado Souza. **Centro de Defesa Cibernética.** Disponível em:<http://www.cert.br/forum2014/slides/ForumCSIRTs2014-CDCiber.pdf>. Acesso em: 22 set. 2016.

CARNEIRO, João Marinonio Enke. A **Guerra Cibernética:** uma proposta de elementos para formulação doutrinária no Exército Brasileiro. 2013. 119 p. Tese Doutorado. Escola de Comando e Estado-Maior do Exército, Escola Marechal Castello Branco, Rio de Janeiro, 2012.

CERT.BR. **Cartilha de Segurança para Internet.** Disponível em:<http://cartilha.cert.br/golpes/>. Acesso em: 22 set. 2016.

CONTE, Celso Antonio Pacheco. FIORILLO, Celso Antonio Pacheco. **Crimes no Meio Ambiente Digital**. São Paulo: Editora Saraiva, 2013.

COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática.** Disponível em: <http://jus.com.br/artigos/1826/crimes-de-informatica/2>. Acesso em: 17 jul. 2016.

COUTINHO, Mateus. **PF vê riscos emergentes de ataques de Hackers e fraudes eletrônicas em 2014.** Dez. 2013. Disponível em: <http://politica.estadao.com.br/blogs/fausto-macedo/pf-ve-riscos-emergentes-de-ataques-de-hackers-e-fraudes-eletronicas-em-2014/> Acesso em: 02 agos. 2016.

DUGGAN, David P. PARKS, Raymon C.; **Principles of Cyber-warfare. Proceedings of the IEEEWorkshop on Information Assurance.** West Point: NY, p 122 – 125, 2001.

DUARTE, Pedro**. Lei Geral da Copa: disposições penais temporárias.** Out. 2012. Disponível em:<http://www.egov.ufsc.br/portal/conteudo/lei-geral-da-copa-disposi%C3%A7%C3%B5es-penais-tempor%C3%A1rias-0> Acesso em: 22 set. 2016.

D'URSO, Adriana Filizzola. **Parecer Lei Geral da Copa e PL 728/2011.** Disponível em: <http://www.grupas.com.br/parecer-penal.pdf>. Acesso em: 22 set. 2016.

EKONOMISTA. **Penta Campeão da Copa, Brasil é o 5ª país no ranking mundial de fraudes de cartão de crédito.** Disponível em: <http://www.e-konomista.com.br/a/penta-campeao-da-copa-brasil-e-o-5-pais-no-ranking-mundial-de-fraudes-de-cartao-de-credito/>. Acesso em: 02 agos. 2016.

FERREIRA, Ivette Senise. **A criminalidade informática.** Direito & Internet: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**, 2ª Ed. São Paulo: Atlas, 2011.

MOTA, Humberto. **Grandes eventos esportivos:** oportunidade excepcional para o Brasil. Dez. 2010 Disponível em:<http://www.cdes.gov.br/noticia/18355/grandes-eventos-esportivos-oportunidade-excepcional-para-o-brasil.html> Acesso em: 17 jul. 2016.

NOGUEIRA JORGE, Higor Vinicius. WENDT, Emerson. **Crimes Cibernéticos. Ameaças e Procedimentos de Investigação.** Rio de Janeiro: Brasport, 2012.

KAMINSKI, Omar. **Internet Legal.** Curitiba: Editora Juruá, 2011.

MANNARA, Barbara. Hackers usam sites de ingressos falsos em ataques com foco na Rio 2016. Jun. 2016. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2016/06/hackers-usam-sites-de-ingressos-falsos-em-ataques-com-foco-na-rio-2016.html> Acesso em 22 set. 2016.

MINISTÉRIO DA JUSTIÇA. **Secretaria Extraordinária de Segurança para Grandes Eventos.** Disponível em: <http://portal.mj.gov.br/data/Pages/MJDE2A290DITEMID21B75E46DE0C43338088663E47803C23PTBRNN.htm>. Acesso em: 22 SET. 2016.

MINISTÉRIO DA JUSTIÇA. **Planejamento Estratégico de Segurança para a Copa do Mundo FIFA Brasil 2014.** Disponível em: <http://www.conectas.org/arquivos/editor/files/PlanejamentoEstrategicoSESGE%20%282%29.pdf>. Acesso em: 22 set. 2016.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. **Manual de Direito Penal**, volume II. 28ª Ed. São Paulo: Atlas, 2011.
MONITOR DAS FRAUDES. Disponível em: <http://www.fraudes.org/>. Acesso em: 22 set. 2016.

SAKAMOTO, Marcos. **O Direito das Gentes e a Informática**. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/29184-29202-1-PB.html>. Acesso em: 22 set. 2016.

SIMON, Imre. **Histórias das Redes no Brasil.** Disponível em: <https://www.ime.usp.br/~is/abc/abc/node25.html>. Acesso em: 17 jul. 2016

SOUZA, Denis Augusto Araújo. 2015, **O ano do Cibercrime.** Disponível em: <http://convergecom.com.br/tiinside/seguranca/artigos-seguranca/06/02/2015/2015-o-ano-cibercrime/#.VUT74iFViko> Acesso em: 29 jul. 2016.

SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. São Paulo: Saraiva, 2013.

ZANIOLO, Pedro Augusto. **Crimes Modernos O Impacto da Tecnologia no Direito.** Curitiba: Editora Juruá, 2007.

WAMBURG, Jorge. **Segurança na Internet**. Marc. 2014. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2014-03/curso-prepara-policiais-para-enfrentar-crimes-ciberneticos-na-copa>. Acesso em: 17 jul. 2016.