Regulação da Guerra Cibernética e o Estado Democrático de Direito no Brasil

Cyber Warfare Regulation and the Rule of Law in Brazil

Submetido(*submitted*): 20 de fevereiro de 2014
Parecer(*revised*): 21 de março de 2014
Aceito(*accepted*): 18 de abril de 2014

Ronaldo Bach da Graça*

RESUMO

Propósito – Este artigo tem por finalidade analisar a relação teórica entre os conceitos de Estado Regulador e Estado Democrático de Direito sob a ótica da regulação da guerra cibernética. Esta atividade, que não enxerga fronteiras e que não respeita sequer a declaração efetiva de guerra, pode assegurar direitos básicos tradicionalmente infensos à exclusiva disciplina normativa.
Metodologia/abordagem/design – O texto segue o método de abordagem descritivo e lógico-intuitivo, abordando como está estruturada a guerra cibernética no Brasil e verificando sua conformação com um modelo juridicamente adequado à proteção de direitos.
Resultados – Foi constatado que o tema da guerra cibernética é pouco abordado pela doutrina e jurisprudência pátrias, apesar de sua recorrência na vida em sociedade hodierna. Sua relação com segurança nacional e direitos fundamentais aumenta a importância da abordagem do assunto. Uma regulação adequada pode potencializar os resultados do instituto na medida em que oferece segurança jurídica aos profissionais da área, ao mesmo tempo em que assegura direitos constitucionais.
Implicações práticas – O artigo contribui ao debate da regulação da guerra cibernética, direcionando para aspectos polêmicos de conformação regulatória no tocante à segurança jurídica da atividade de guerra cibernética e à proteção de direitos fundamentais.
Originalidade/relevância do texto – Espera-se que o texto fomente o debate sócio-jurídico sobre temas relevantes de guerra cibernética, a partir da identificação de

*Ronaldo Bach da Graça é Mestre em Operações Militares, Graduado em Ciências Militares (Comunicações) pela Academia Militar das Agulhas Negras e em Direito pela Universidade do Estado do Rio de Janeiro (UERJ), possui diversas especializações, dentre as quais Direito & Tecnologia e Guerra Eletrônica. Foi professor na Escola de Comunicações (RJ) e no Centro de Instrução de Guerra Eletrônica (DF), onde lecionou também Direito Digital. Contato: ronaldobach@hotmail.com.

DOI: https://doi.org/10.26512/lstr.v6i1.21550

potenciais problemas. Isso pode evitar, na prática, conflitos jurídicos futuros e aumentar a sensação de segurança quando do uso de redes de computadores.

Palavras-chave: guerra cibernética, guerra eletrônica, privacidade, direitos fundamentais, segurança nacional, Internet.

ABSTRACT

Purpose *– This paper aims to analyze the relationship between the concept of Regulatory State and democracy through the lenses of the cyber warfare. This activity, which disregards borders and does not even respect the declaration of war, can often ensure basic rights without which the law could not.*
Methodology/approach/design *– The research was implemented using descriptive and logical-intuitive approach, exploring how the cyber warfare is structured in Brazil and verifying its conformation with a legally proper model.*
Findings *– It has been found that this is a topic scarcely explored by national doctrine and judicial decisions, although cyber war is a recurrent subject in society nowadays. Its connection with national security and fundamental rights increases the importance of approaching the subject. An adequate regulation could increase the results of the cyber warfare once it provides legal certainty for professionals, while ensuring constitutional rights.*
Practical implications *– This paper may help in the discussion of the regulation of cyber warfare, guiding researchers to controversial aspects, the regulation of which offers convenience for society and for professionals working in this field.*
Originality/value *– It is expected that this paper foments socio-legal debate on relevant topics concerning cyber warfare, by identifying potential problems. It might prevent, in practice, future legal conflicts and increase the perception of security when using computer networks.*

Keywords*: cyber warfare, electronic warfare, privacy, fundamental rights, national security, Internet.*

Introdução

A importância deste estudo pode ser ratificada pela incipiente regulação do instituto em pauta no Brasil, o que leva a insegurança jurídica para todos os envolvidos. Com isso corrobora o fato do assunto ser pouco explorado tanto pelo enfoque doutrinário quanto jurisprudencial, a despeito de

acontecimentos envolvendo a temática já serem cotidianos para muitos brasileiros, inclusive com repercussão no ambiente diplomático. A supremacia técnica em guerra cibernética pode sozinha, auxiliar sobremaneira o Estado brasileiro a tutelar bens jurídicos mesmo na ausência de cooperação entre atores internacionais. Esta possibilidade reforça o Estado Democrático de Direito.

Inicialmente são firmados os pressupostos teóricos que fundamentam a análise, concernentes ao Estado Regulador e à atividade de guerra cibernética. Neste ponto abordam-se alguns conceitos de direito digital. Posteriormente, analisa-se a possibilidade de a regulação da guerra cibernética reforçar o Estado Democrático de Direito, equilibrando direitos assegurados pela Carta Magna, como o direito à privacidade, como forma de fortalecer a democracia brasileira.

Após a análise do Estado Regulador, algumas noções de direito eletrônico e das definições necessárias para compreensão do problema da regulação da guerra cibernética no Brasil, concluir-se-á como o Estado Regulador pode auxiliar o Estado Defesa, assegurando direitos fundamentais dos que estão sob jurisdição brasileira.

O Estado Regulador

Entender a regulação se faz necessário para que se possa alcançar o objetivo proposto de analisar a influência da regulação da guerra cibernética. Regular comportamentos é a proposta do Estado Regulador, e a regulação, que normalmente possui um viés jurídico-econômico determinante, vê a atuação do Estado na economia ganhar uma faceta diferente. Isso ocorre porque valores não-econômicos relevantes são também mensurados neste estudo: o direito econômico por si só não parece ser suficiente nesta análise.

Castells (1999) destaca que a ascensão do Estado Regulador, que se deu principalmente a partir dos anos 80 (Rossi 1995, 230-242), contribuiu para o declínio dos meios clássicos de regulação do próprio Estado. Dessarte é notada uma crise do embasamento clássico do Estado Industrial democrático sobre os conceitos de soberania e representatividade democrática, que faz com que o Estado se torne cada vez mais frágil no contexto global e menos representativo internamente. A fragilidade notada

DOI: https://doi.org/10.26512/lstr.v6i1.21550

por Castells é reforçada em Estados não centrais, como é o caso do Brasil, em razão das consistentes demandas sociais combinadas com a limitação dos recursos disponíveis para o Estado Administrador notadamente perdulário: *gasta muito, e ao fazê-lo privilegia uns poucos, em detrimento da maioria, pois não investe nos serviços públicos essenciais dos quais esta [maioria] carece* (Machado 2008, 26).

O Estado Regulador aparece atualmente com uma forma redesenhada de intervencionismo estatal, apresentando um novo sentido à ciência de *Comando e Controle*, talvez mais sutil, porém não necessariamente menos efetivo (Ferreira 2009, 33). Para Chevallier (*apud* Ferreira 2009, 42), o Estado Regulador se torna um Estado estrategista que harmoniza interesses viabilizando a prestação dos serviços de forma conveniente.

Considere-se ainda, conforme afirma Aguillar (1999) numa análise sistêmica de seus ensinamentos, o fato de que uma regulação exitosa em Estados centrais pode não ser um modelo sujeito à importação por Estados periféricos: ele sugere que devemos adaptar a regulação às circunstâncias, à realidade fática do local onde ela será implementada e efetivada. Diferentes realidades sociais e diferentes circunstâncias influenciam na implementação de uma regulação adequada.

A regulação das tecnologias de informação e comunicação (TICs) contemporâneas, em especial a comunicação realizada por meio de redes de computadores, esbarra na peculiaridade de que o serviço tornou-se essencial para a vida em sociedade. Ademais, as TICs são de difícil controle por parte de qualquer Estado, face às peculiaridades que podem tornar ineficazes quaisquer tentativas de regulação legal: a Internet não respeita o conceito clássico de territorialidade, primordial para a soberania de um Estado. Em outras palavras, a Internet tem mitigado a soberania de todos os Estados. Um agente paquistanês pode cometer uma conduta considerada ilícita pelo Brasil na China, utilizando-se de um servidor no Brasil, causando prejuízos nos Estados Unidos, por meio de um provedor indiano. Quem poderá impor sua regulação ao paquistanês, supondo sua conduta ser considerada lícita apenas no Paquistão? O mesmo raciocínio pode ser utilizado para condutas consideradas criminosas por quaisquer dos Estados envolvidos.

A conclusão a que se chega é de que possivelmente será considerada ineficaz qualquer tentativa de regulação jurídica da Internet que não seja

ratificada por outros atores internacionais. Nessa hipótese, a supremacia técnica em guerra cibernética é uma alternativa para manter tutelados os bens jurídicos que o Estado brasileiro pretende proteger.

Wimmer, Pieranti e Aranha (2009) entendem que a comunicação de massa deve ser regulada por quatro razões não excludentes. A primeira razão seria a força política dos meios de comunicação de massa, que podem se tornar uma ameaça para a sociedade e para o *status quo* vigente. Tais meios de comunicação podem induzir uma nação a caminhos e descaminhos. Em virtude de tais características não seria recomendável aplicar as regras naturais de regulação aos meios de comunicação.

Segundo os autores supracitados, a segunda razão para justificar a regulação do setor seria o fato de que a não-regulação poderia gerar prejuízos a direitos fundamentais. Seria necessário que os meios de comunicação garantissem a liberdade de expressão, representando toda a sociedade.

Outra razão seria o fato de que a atuação livre dos meios poderia *impactar a defesa nacional, na medida em que expõe o país a um ideário nem sempre amigável do ponto de vista da diplomacia*. Os autores explicam que meios que já proporcionavam emissões em longas distâncias, como rádios em ondas curtas, foram utilizados como suporte à propaganda e contrapropaganda, e aduz que as emissões em ondas curtas guardam uma interessante similaridade com meios como a Internet pelo fato de ignorarem fronteiras físicas e cruzarem nações, sendo veículos que difundem ideias originadas em outros Estados. E cita: *No caso das ondas curtas, isso não significou um abandono da regulação por parte do Estado, mas o estudo de alternativas à regulação tradicional; no caso da internet, tampouco devem ser abandonados os mecanismos regulatórios, ora submetidos a um novo enfoque.*

A quarta razão que justificaria a regulação do setor é a escassez de recursos. Os autores enfatizam o fato do espectro eletromagnético ser limitado. No caso da radiodifusão, a regulação técnica se justificaria com relativa tranquilidade sob o argumento de que o espectro eletromagnético comporta um número limitado de transmissores em razão da largura de banda no padrão técnico adotado pelo Estado, porém quando se fala de Internet, este argumento é mitigado: mesmo quando se imagina uma

DOI: https://doi.org/10.26512/lstr.v6i1.21550

limitação quantitativa de nomes de domínio ou de endereços IP, aparece uma solução técnica implementável para que a quantidade possível aumente substancialmente. Um exemplo na telefonia é o acréscimo de um número no telefone que possibilita uma quantidade maior de assinantes. Esta técnica foi utilizada recentemente na telefonia celular dos estados de SP, RJ e ES, multiplicando a disponibilidade de linhas telefônicas (Anatel 2012). Mesmo uma transmissão analógica de radiodifusão utiliza uma largura de banda consideravelmente maior que uma transmissão em quaisquer dos padrões de transmissão digital contemporâneos. Em outras palavras: pela inovação tecnológica, é possível transmitir-se uma maior quantidade de dados em uma mesma faixa de frequência.

O século XX pode ser considerado o período em que se consolidaram conquistas atinentes a garantias constitucionais de direitos fundamentais. É entendido como o *século de apresentação do Estado como um componente essencial na definição do conteúdo dos direitos fundamentais mediante enraizamento do conceito de serviço público e da ampliação concreta do rol de direitos dos cidadãos.* Desde então, os direitos fundamentais devem ser assegurados pelo Estado regulador, por meio de intervenção, quer seja pelo *exercício do poder de polícia, atividades de fomento e prestações positivas tradicionais de índole concreta e normativa* (Wimmer *et al.* 2009, 3).

Quando se fala em regulação em um ambiente globalizado, deve-se considerar a exigência de um ordenamento jurídico adaptado, considerando a necessidade de viabilidade das relações internacionais, sendo desejável um acordo global, o que facilitaria a interação entre os Estados (Sundfeld e Vieira 1999, 157-168) e reforçaria o poder de controle. Um acordo global diminuiria o risco de beligerância entre atores internacionais e, de forma concomitante, potencializaria o regramento interno que ratifica um eventual acordo internacional.

Atualmente a comunidade internacional tem atuado cada vez mais de forma colaborativa. Para que se tenha uma ideia das possibilidades de acordo e cooperação internacional, a Interpol está hoje presente em 190 Estados do mundo (Interpol 2013). Dependendo do bem jurídico a ser tutelado pela regulação internacional, a possibilidade de que as regras sejam cumpridas por Estados e cidadãos aumenta significativamente. Para bens

jurídicos tão caros a uma sociedade a ponto de serem tutelados pela legislação penal, a possibilidade de acordo tende a aumentar. Afinal todos os Estados querem preservar direitos que são caros a sua sociedade, e muitas vezes são encontrados valores comuns em culturas distintas. Este fato possibilita uma regulação potencialmente mais eficiente.

Quando se fala de regulação de guerra cibernética, percebe-se, de um lado, a necessidade de o Estado prover a própria segurança, por meio do agente público; e, de outro, direitos fundamentais que também são constitucionalmente assegurados. A relação existe na medida em que a proteção do Estado será tão mais efetiva quanto maior forem as informações disponíveis sobre as ameaças em potencial. Em tese, a criação deste banco de dados pode ameaçar parte da privacidade dos atores envolvidos, visto que uma ameaça precisa ser conhecida para ser melhor combatida. Em regra o operador da guerra cibernética, como o da guerra eletrônica, estaria sujeito a necessidade de norma autorizativa de sua conduta, e este fato tem sido um problema para essa espécie de atividade militar no Brasil. A interpretação sistêmica da norma brasileira sobre o tema pode se mostrar polêmica.

Com relação à efetiva ação de um dos mais relevantes Estados centrais, relacionada ao tema de guerra cibernética, o ex-líder do programa de segurança digital dos EUA, Howard Schmidt, especialista em segurança na internet e ex-coordenador de cibersegurança do governo Barack Obama, ensina que *faz parte da responsabilidade de toda nação proteger os seus cidadãos contra a coleta de dados por sistemas de inteligência.* Schmidt sugere atenção às normas internacionais, estabelecendo limites do aceitável. Declarou que se preocupa com a militarização da internet, descrevendo que 27 Estados criaram organizações militares especializadas em explorar vulnerabilidades das redes de computadores e criar formas de destruir a infraestrutura de oponentes em potencial. Ele também sinalizou com a *necessidade* de que sejam criadas normas para o ciberespaço sugerindo o modelo multissetorial para a regulação, adotado por órgãos como a ICANN (Corporação da Internet para Atribuição de Nomes e Números). Ao fim, ele adverte que os usuários comuns não imaginam os riscos que a internet pode oferecer (Aguilhar 2013).

DOI: https://doi.org/10.26512/lstr.v6i1.21550

Sérgio Pagliusi afirma que, em uma escala de 0 a 10, o Brasil estaria com nota entre 3 e 4 no quesito segurança da informação. Segundo ele, "estamos começando a acordar para o problema. Nessa história de espionagem corporativa, temos muita lição a fazer. Falta consciência institucional e um longo aprendizado. A sociedade como um todo caiu em si e viu que é uma coisa que nos afeta" (Agência Brasil 2013). Tal assertiva nos leva a inferir que a guerra cibernética influi na vida de toda a sociedade. A ameaça é tão real que a espionagem já tem cancelado projetos de computação em nuvem (Grossmann 2013). Acerca da possibilidade de tecnologia brasileira eficaz para a necessária segurança, Rafael Moreira, conselheiro do Comitê Gestor da Internet (CGI), afirma que "há uma massa de conhecimento dentro das universidades e em empresas inovadoras que podem contribuir propondo medidas para que possamos mudar isso [falta de segurança] no longo prazo" (Agência Brasil 2013). Portanto o Estado brasileiro possui as ferramentas necessárias para atuar com guerra cibernética.

Para Pinheiro (2000), quando não existe um contrato entre partes com interesses antagônicos, a precariedade na definição de normas será um fator para potencializar a imprevisibilidade de eventual decisão judicial na relação entre as partes, com a consequente insegurança jurídica inerente às circunstâncias apresentadas. Para esse mesmo autor, um sistema justo seria aquele no qual a probabilidade da vitória do certo tende a cem por cento.

Guerra cibernética no Brasil

O desenvolvimento científico influencia a forma como a humanidade faz guerra, pelo desenvolvimento dos armamentos e das técnicas de combate. As ações de guerra demandam estratégias planejadas e recursos investidos em longo prazo para não se ter que contar com a sorte.

Porém, antes de adentrar nos pormenores das atividades de guerra cibernética, cabe uma diferenciação entre guerra eletrônica e guerra cibernética. A guerra eletrônica é "o conjunto de atividades que visam desenvolver e assegurar a capacidade de emprego eficiente das emissões eletromagnéticas próprias, ao mesmo tempo em que buscam impedir, dificultar ou tirar proveito das emissões inimigas" (Brasil 2008). Desta

DOI: https://doi.org/10.26512/lstr.v6i1.21550

definição se conclui que a guerra eletrônica se relaciona com a propagação de radiofrequência no espectro eletromagnético.

Recentemente foi noticiado que, por meio de um equipamento móvel de escuta específico para telefonia celular francês e de escutas ambientais, foram realizadas escutas telefônicas e ambientais de comunicações de ministros do Supremo Tribunal Federal (Bonin 2013, 74-80). De acordo com os conceitos apresentados *supra*, casos como estas supostas escutas demonstram possibilidades de atuação da guerra eletrônica, porque foram dados coletados sem o uso de rede de computadores.

A guerra cibernética está relacionada com o uso de computadores em rede. Para o Ministério da Defesa brasileiro,

> é o conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informações e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil.

Este tema estaria ligado, *v.g.*, ao fato afirmado pela empresa estadunidense de segurança eletrônica FireEye de que a China teria *hackeado* computadores de chanceleres europeus que iriam participar dias depois da reunião de setembro de 2013 do G20, o que foi negado e condenado pelo governo chinês (Folha de São Paulo 2013).

Das redes de computadores existentes, a mais significativa para o contexto da guerra cibernética é a internet. Definições existentes para o termo em análise são inúmeras, e quase sempre sem consenso. O setor cibernético é considerado pelo Decreto 6.703/2008 (Estratégia Nacional de Defesa - END) essencial para a defesa nacional. Neste contexto, a guerra cibernética visa a assegurar a capacidade para atuar em rede de computadores.

A END prossegue determinando que, no setor cibernético, deve ser constituída uma organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar. Espera-se que a preparação para a guerra cibernética auxilie no aperfeiçoamento dos dispositivos e

procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos.

A Portaria 3.028/2012, do Ministério da Defesa (MD), em seu art. 1º, atribui a responsabilidade pela coordenação e integração das atividades de Defesa Cibernética ao Exército Brasileiro (EB) no âmbito das Forças Armadas do Brasil. Assim sendo, o maior centro de doutrina do MD está no Exército Brasileiro. Hoje, a organização encarregada de desenvolver a capacitação cibernética no âmbito do Ministério da Defesa é o Centro de Defesa Cibernética. Subordinado ao Departamento de Ciência e Tecnologia do Exército Brasileiro, esse centro tem recebido investimentos do Governo Federal com escopo na capacitação de pessoal que possa fazer frente a um possível ataque cibernético.

Para o Centro de Defesa Cibernética, Guerra Cibernética em sentido estrito diz respeito a um nível de decisão operacional ou tático. Em nível estratégico, denomina-se Defesa Cibernética. No nível de decisão política, convencionou-se chamar de Segurança Cibernética. Esta é a terminologia adotada pelo Ministério da Defesa (MD). Neste artigo, convencionou-se adotar a expressão guerra cibernética qualquer que seja o nível de decisão. Conceitos de segurança cibernética, inteligência cibernética e pesquisa cibernética estão atrelados ao tema.

O MD, em 2012, editou a Política Cibernética de Defesa (MD31-P-02) por meio da Portaria Normativa nº 3.389/MD. Fruto das diretrizes traçadas, foram implementados produtos como o antivírus nacional e o Simulador de Operações Cibernéticas, *software* que utiliza a doutrina brasileira para treinar os "Guerreiros Cibernéticos" formados no Exército. A capacitação de recursos humanos em guerra cibernética é feita, no âmbito do Exército, no Centro de Instrução de Guerra Eletrônica (CIGE), instituição de ensino superior que capacita também especialistas em guerra eletrônica.

O CIGE é uma organização militar diretamente subordinada ao Centro de Comunicações e Guerra Eletrônica do Exército (CCOMGEX). Por isso, compete ao Comandante de Comunicações e Guerra Eletrônica do Exército nortear não só as atividades de ensino de guerra cibernética no Exército, mas também as de guerra eletrônica e de comunicações, em sua vertente bélica (trânsito de informações de interesse militar).

DOI: https://doi.org/10.26512/lstr.v6i1.21550

A estrutura ora apresentada oferece sinergia para a defesa externa do Estado brasileiro, pois facilita a atuação conjunta de diversas áreas ligadas ao *Comando e Controle* em uma operação militar terrestre. Este contexto sugere que se pode realizar uma análise sistêmica dos vetores ora apresentados quando se tem a segurança no trânsito das informações com o objetivo a ser perseguido.

O Centro de Defesa Cibernética tem participado de grandes eventos realizados no Brasil, como a Rio +20, a Jornada Mundial da Juventude e a Copa das Confederações, possuindo uma Central de Monitoração Cibernética. A intenção é de que participe também da Copa do Mundo 2014 e das Olimpíadas em 2016.

A Doutrina de Guerra Cibernética ainda é incipiente se comparada à Doutrina de Guerra Eletrônica (GE). Logo, como possuem muito em comum, vale uma análise de alguns conceitos de GE para que se antecipar conclusões sobre a guerra cibernética.

A GE está representada nas Forças Armadas brasileiras desde os anos 1980. Já possui no Brasil doutrina consolidada, e está presente nas três forças armadas brasileiras. Está em curso, em razão de um acordo de compensação do Exército Brasileiro, o desenvolvimento em parceria de *hardwares* de sensores eletromagnéticos brasileiros com tecnologia alemã e brasileira. Trata-se de conhecimento industrial bastante restrito e importante para potencializar os esforços de segurança.

A doutrina de guerra eletrônica mundial destaca a atividade de inteligência do sinal (nível estratégico) como a principal atividade de GE. Trata-se de uma atividade que busca formas de se preparar para a guerra, a partir da coleta constante de informações em tempo de paz. Sun Tzu, autor do clássico *A Arte da Guerra*, já ensinava que, para se obter sucesso em batalhas, é imperioso conhecer a si mesmo e ao seu oponente. A atividade de inteligência do sinal busca apoiar o combate pelo conhecimento do potencial oponente e das vulnerabilidades próprias. No nível tático, busca-se obter dados a partir da aquisição de sinais eletromagnéticos. A finalidade de interceptar, identificar emissões determinadas e localizar o emissor de radiofrequência é o reconhecimento imediato da ameaça (Brasil 2008).

Existem outros ramos de atividades não menos importantes, porém praticadas somente em casos específicos. São executadas normalmente no

DOI: https://doi.org/10.26512/lstr.v6i1.21550

nível tático, ou, em uma linguagem mais simples, em efetivo combate. Uma delas visa a impedir ou reduzir o emprego eficiente do espectro eletromagnético pelo oponente: o que for possível e mais conveniente e/ou oportuno. Outra visa a assegurar a utilização eficiente do espectro eletromagnético, a despeito das tentativas do oponente em dificultar ou impedir as nossas transmissões e de obter dados a partir da aquisição de sinais eletromagnéticos (Brasil 2008).

Analogamente pode-se aduzir a importância, num contexto de guerra cibernética, de se saber o que se passa consigo e com o potencial oponente para que realmente se chegue a uma percepção útil para utilização na atividade de guerra cibernética. Além disso, deve-se utilizar toda a informação obtida com o propósito de impedir ou dificultar o uso regular de uma rede de computadores quando necessário, e, ao mesmo tempo, assegurar que a própria rede de computadores funcione adequadamente.

Ainda que a doutrina militar brasileira não privilegie o ataque – mas a reação ao ataque –, deve-se ter em conta que o preparo para operações de ataque ou de defesa é necessário. Com isso pode-se concluir que uma boa preparação na área da guerra cibernética deve buscar conhecimento das próprias vulnerabilidades e assegurar a segurança no uso das redes de computadores próprias. Ademais, deve-se ter capacidade para interceptação e ataque. Com esta filosofia, o Estado brasileiro tem privilegiado técnicas de autodefesa e a defesa ativa, conforme declaração do General José Carlos dos Santos (Motta 2011).

No entendimento de Davi Ottenheimer, especialista em segurança da informação, é desejável que, em caso de ataques cibernéticos, realizem-se contra-ataques com escopo na prevenção contra novos ataques, de forma comissiva, reforçando o conceito de defesa ativa (V CONSEGI 2012).

Consolide-se a informação de que, no mundo todo, para que haja preparação adequada para a guerra cibernética, é necessária a constante busca de dados por meio da rede: tanto vulnerabilidades próprias quando vulnerabilidades de oponentes em potencial. Ela funciona como um agente de segurança ostensiva, que cumpre sua função mais adequadamente se souber quem está a sua volta, no ambiente onde se propõe a manter a ordem.

DOI: https://doi.org/10.26512/lstr.v6i1.21550

A busca de dados ora referida deve acontecer não só por meios eletrônicos, mas por todos os meios disponíveis. Dados como os disponibilizadas pelo delator do suposto sistema governamental estadunidense de espionagem Edward Snowden (Redação G1 2013) devem ser confirmados ou ao menos ter sua probabilidade de veracidade escalonada para compor mais um subsídio nas análises de dados voltadas para a Defesa Cibernética.

Edward Snowden foi o técnico da CIA acusado pelo governo americano de espionagem por vazar informações sigilosas de segurança dos Estados Unidos e revelar em detalhes alguns dos supostos programas de vigilância daquele país contra estadunidenses, europeus e latino americanos.

Sem considerar aspectos políticos, a oitiva de pessoas com acesso a informações de espionagem estatais dispostas a falar sobre o assunto é sempre um complemento desejável para confirmar ou não dados coletados eletronicamente, mas tais declarações devem ser analisadas com cautela, a fim de evitar a manipulação por meio de dados falsos divulgados. A descrição apresentada aqui não é necessariamente o que o Brasil adota, mas como é desenvolvida a atividade no meio militar, no contexto dos países centrais. Importante frisar a necessidade do desenvolvimento técnico nesta área do conhecimento na medida em que, neste campo, a supremacia técnica pode tutelar bens jurídicos que o direito, sem auxílio técnico e cooperação internacional, não conseguiria proteger.

Guerra cibernética e direito digital

Algo que não se pode olvidar quando se reporta à guerra cibernética são alguns dos conceitos recorrentes em direito digital. O direito busca tutelar bens jurídicos com a finalidade de tornar possível o bom convívio social. A sociedade da informação adveio de um longo processo que pode ter seu início vinculado à própria Revolução Industrial (Crespo 2011, 32).

Da Revolução Industrial para os dias de hoje, houve avanços econômicos e valorização de bens imateriais, que têm sido tutelados até mesmo pelo direito penal da maior parte dos Estados centrais. Assim também ocorre no Brasil. Cada vez mais tutelam-se bens imateriais, tais como a imagem, a integridade, a dignidade, a privacidade. A valorização

desses bens pode ser inferida de disposições constitucionais e penais no Brasil, acompanhando uma tendência global. Grande parte destes bens imateriais possuem vínculo com redes de computadores, e em especial com a internet (Crespo 2011, 32-37).

Sistemas de defesa (militares ou não); centrais de energia, inclusive nuclear; controle de tráfego, inclusive aéreo e metroviário; centrais telefônicas; sistemas de saúde; enfim, todas as infraestruturas críticas dos Estados contemporâneos estão, de alguma forma, ligadas às redes de computadores.

Na medida em que sistemas críticos passam a depender das informações trafegadas em rede de computadores, surge uma nova arma de combate: a manipulação das informações que trafegam em rede. A guerra cibernética vem ganhando importância em razão da gama de ameaças que podem ser, por meio dela, combatidas.

O uso indevido das informações que trafegam em uma rede de computadores pode dar azo a consideráveis prejuízos. Cabe ao Estado oferecer a segurança necessária para a vida em sociedade. Para que tal segurança seja maximizada, torna-se imprescindível a montagem de bancos de dados referentes a potenciais ameaças à segurança do país. Se o Estado for surpreendido, as chances de uma resposta militar ser ineficiente aumentam exponencialmente.

Os conceitos de soberania e de territorialidade são mitigados quando se trata de guerra cibernética: meios tecnológicos modernos quebram barreiras territoriais dificultando em alguns casos a eficácia de demandas judiciais. Um agente indiano no Paquistão pode, a mando de um terceiro Estado, causar danos no Brasil, utilizando-se de um provedor americano. Ainda que o agente seja condenado no Brasil, dificilmente será uma condenação eficaz, salvo hipótese de cooperação internacional que possibilite implementar eventual condenação. Em razão disto, a defesa deve ser baseada também em tecnologia que evite o dano. Como o "território virtual" não respeita fronteiras físicas, pode não haver outra alternativa viável, posto que a soberania se efetiva pelo domínio do território.

Debates atinentes a iniciativas legislativas, como o Marco Civil da Internet, em tramitação no Congresso Nacional brasileiro quando da elaboração deste estudo, influenciam a regulação da guerra cibernética no

Brasil. O Projeto de Lei em pauta valoriza a privacidade, a neutralidade da rede e define como imputar condutas indesejáveis a indivíduos. São temas que devem ser valorizados quando da apreciação dos limites de atuação da Guerra Cibernética, enquanto instrumento do Estado. Porém, o Marco Civil possui aspectos muito polêmicos e grandes divergências a serem pacificadas.

Como sugere o Projeto de Lei do Marco Civil da Internet, atenção especial merece a privacidade quando se está ligado a uma rede de computadores. O desrespeito à privacidade pode ter por consequência, inclusive, grandes tragédias pessoais. Tal fato não pode ser ignorado. Existe atualmente uma sensação de que os limites da privacidade estão cada vez mais exíguos. O acontecimento privado, se divulgado na Internet, passa a ser acessível a qualquer um que tenha acesso à rede. E o que fazer quando a informação disponível diz respeito a momento delicado da vida de alguém que se pretendia manter sob reserva? Dentre outros bens tutelados, a indigência de uma pessoa exposta na rede mundial de computadores pode se tornar uma tragédia de difícil reparação. Observe-se que se trata aqui de exposição pessoal involuntária.

Por outro lado, o respeito excessivo à privacidade pode ser encarado como uma conduta omissiva do Estado preocupado com a segurança: quando se anda por uma rua bem policiada, há uma maior sensação de segurança porque se percebe que o Estado, por meio de seus agentes, está naquele local monitorando condutas. Se a polícia não age proativamente, de forma preventiva, o resultado de sua atuação tende a permanecer aquém do desejável pela sociedade. Na hipótese de uma conduta considerada anormal, algum agente público poderá perceber com menor lapso temporal, suficiente para neutralizar ou mesmo mitigar um risco que, às vezes, não seria tão evidente para agentes sem treinamento. Analogamente, pode-se considerar que o mesmo ocorre no que tange ao contexto da guerra cibernética.

O cuidado na seleção dos policiais da situação hipotética descrita *supra* também deve ser trazido para o recrutamento de profissionais que atuam com guerra cibernética. Da mesma forma que um mau policial pode trazer um grande prejuízo para a sociedade onde ele se encontra inserido, o mesmo acontecerá com qualquer agente de segurança que não possua

adjetivos necessários, principalmente quando se trata de Segurança Nacional.

Quando se aborda guerra cibernética ou mesmo defesa cibernética, deve-se ter em conta que essas são atividades planejadas e executadas pelo Poder Executivo. Pela teoria apresentada por North (1993), o judiciário, nesta hipótese, teria um papel coercitivo em uma relação entre outros dois agentes com interesses diversos: o Estado e o detentor de informação que deseja protegê-la.

Durante as manifestações populares ocorridas no Brasil em junho de 2013 contra atos de governo, vários protestos foram organizados por meio de redes sociais. Nessa ocasião, o Exército monitorou a rede com uma técnica semelhante à utilizada pela Agência de Segurança Nacional dos Estados Unidos (NSA). Isto se deu por meio de um *software* que filtra as informações disponibilizadas nas redes sociais. Desta forma, o Exército poderia identificar aqueles que assumiram o comando dos protestos. As informações foram repassadas para a Polícia Federal e para a Secretaria de Segurança Pública dos estados nos quais ocorreram tais manifestações (Sassine 2013).

A um grupo de cinquenta militares foi atribuída a responsabilidade pela identificação dos líderes das manifestações, pontos de potencial conflito e organização de atos de vandalismo. Agentes e delegados da Polícia Federal atuaram em conjunto com o Exército. Segundo o General José Carlos, a atividade foi desempenhada dentro da legalidade, visto que o acompanhamento é necessário por envolver questões ligadas a Segurança Nacional, o que legitimaria e justificaria esta ação. O *software* utilizado para a realização desta operação é de fabricação nacional, desenvolvido pela Dígitro, sociedade empresária sediada em Florianópolis, que comercializa a solução para órgãos de segurança pública em geral.

O Exército cessou o monitoramento com o fim da Copa das Confederações. Segundo o General Santos, em nenhum momento o Exército filtrou dados que não fossem informações públicas, divulgadas nas redes sociais pelos ativistas. Segundo o General, por meio de filtros, consegue-se localizar as informações de interesse.

DOI: https://doi.org/10.26512/lstr.v6i1.21550

> É uma técnica de filtragem que a própria espionagem deve utilizar racionalmente. Os americanos monitoram 2,3 bilhões de e-mails e telefonemas. Se não houver essa técnica, não é possível gerar inteligência sobre isso. O próprio embaixador americano (no Brasil), Thomas Shannon, indica que essa é a técnica utilizada pela NSA. É um processo semelhante. A grande diferença é que nós nos baseamos só em informações de domínio público. (Sassine 2013)

Percebe-se que as informações que trafegam na rede podem ser de grande repercussão para a segurança de um Estado, refletindo em sua população e instituições. A preservação da segurança nacional não deve ser negligenciada, até porque a estabilidade atrai investimentos, facilitando a vida em sociedade.

Fadi Chehardé, representando o ICANN, residente nos Estados Unidos, apresentou à presidente brasileira Dilma Rousseff a intenção de reunir no Brasil representantes de setores da sociedade com o escopo de redigir uma carta de princípios que o órgão pretende que seja base para regulação do ambiente virtual. Além de garantir a liberdade de expressão na internet, a Corporação pretende evitar o *great firewall*, uma espécie de censura governamental na internet. Sobre a recente espionagem realizada pela Agência Nacional de Segurança dos Estados Unidos contra Estados como o Brasil, ele opina que espiões são necessários, mas que se pode deixar claro o que os países podem e o que não podem fazer na internet. A entidade teme que a espionagem afete a confiança dos usuários comuns de guardar dados "na nuvem" (Vilicic 2013, 114-115).

O direito à privacidade é assegurado pela Constituição Federal de 1988, em seu art. 5º, X. Ele engloba a tutela a informações pessoais do indivíduo, as quais são protegidas do uso de outros – inclusive do próprio Estado.

A Lei 9.296/1996, em seu artigo 10, dispõe que constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática sem autorização judicial ou com objetivos não autorizados em lei. A Lei 12.527/2011, em seu art. 32, IV, dispõe que constitui ilícito divulgar ou permitir a divulgação, acessar ou permitir acesso indevido a informação sigilosa ou informação pessoal. A Lei 12.737/2012 introduziu no Código Penal (art. 154-A) a seguinte tipificação criminosa: devassar dispositivo

DOI: https://doi.org/10.26512/lstr.v6i1.21550

informático alheio, conectado ou não na rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo.

Por outro lado, as Forças Armadas possuem uma atribuição constitucional de defender a pátria, garantindo a lei e a ordem (art. 142, Constituição Federal de 1988).

Cabe ao agente público que labora com a guerra cibernética conciliar, em tempo de paz, as suas atividades típicas com as garantias oferecidas pelo ordenamento jurídico brasileiro.

Observe-se que, mesmo em ambiente empresarial, convém, sob pretexto de que às pessoas seja oferecida segurança na internet, derrubar "serviços, sites e redes ligadas ao crime virtual" (Exame 2013) – como está previsto no Centro de Combate a Crimes Cibernéticos da Microsoft. Acontece que, para que este objetivo seja alcançado, é necessária uma investigação prévia a partir da monitoração da rede mundial de computadores. Pode-se questionar até que ponto uma investigação como essa, anunciada por uma empresa privada na imprensa mundial, pode ferir a privacidade dos usuários da rede mundial de computadores.

Em se tratando do direito à privacidade, sabe-se que esse é um dos direitos fundamentais tutelados pela Constituição Federal de 1988. Todavia, sabe-se que direitos, ainda que fundamentais não são absolutos; possuem caráter relativo. Norberto Bobbio entende que raros são os direitos fundamentais que não entram em concorrência com outros direitos (Bobbio 1992, 40). Pinheiro (2007, 29) entende que o direito digital consiste na evolução do próprio direito, abrangendo princípios e institutos vigentes e introduzindo novos institutos e elementos para o pensamento jurídico. A velocidade das transformações tecnológicas tem sido uma barreira à legislação quando se trata de direito digital.

Os Estados Unidos supostamente teriam desenvolvido com Israel um vírus com o objetivo de afetar usinas nucleares iranianas. O resultado esperado do ataque seria a interrupção no funcionamento de centrífugas iranianas (Defesanet 2013). Mesmo sem a confirmação dos agentes envolvidos sobre este episódio publicado no *The New York Time* (Grego 2013), o caso exemplifica o dano potencial do ataque de um vírus na rede.

O objetivo, se diverso, poderia gerar grande destruição, inclusive entre civis.

Destarte, mesmo sem pólvora, esta atividade deve ser respeitada. Negligenciá-la pode colocar em risco não só a economia de um Estado, mas também a integridade física de seus habitantes.

Em razão do exposto, constatam-se algumas necessidades. É imperiosa ao Estado e à população uma preparação e atuação em guerra cibernética com qualidade, mesmo em tempo de paz. A segurança nacional deve ser preservada. Direitos fundamentais, como o direito à privacidade, devem ser assegurados, porém eventualmente mitigados em razão da necessidade de uma efetiva defesa cibernética. Tecnicamente, é necessária a formação de um banco de dados para a implementação da atividade, e este deve ser autorizado pelo Estado para que a atividade seja bem desempenhada.

Em razão da mitigação da soberania e territorialidade quando se discorre sobre rede de computadores, mesmo havendo vedação legal em alguns Estados, empreendimentos privados realizam a monitoração da internet sob o pretexto de resguardar os usuários de ameaças potenciais e reais, como foi citado o caso da Microsoft.

Em uma análise sumária do que já foi apresentado, ao que parece, as Forças Armadas brasileiras têm adotado a política de monitoração das informações públicas disponibilizadas nas redes de computadores, ao menos quando se fala de segurança em grandes eventos. Seria desejável uma lei que autorizasse expressamente atuação mais livre dos órgãos públicos competentes, para que o gestor público possa desenvolver a atividade a ele confiada de maneira mais consciente, maximizando a segurança e respeitando a privacidade nos limites estabelecidos. No cenário atual, em face da incipiência de julgados sobre o tema e a escassez de doutrinadores que o abordam, falta ao gestor e aos agentes públicos segurança jurídica no desempenho da atividade. Isso decorre, também, da pouca regulação. Lembre-se que a conduta dos agentes públicos se funda no princípio da legalidade estrita, que permite que se faça apenas o que é expressamente determinado por Lei.

Bill Clinton, ex-presidente dos Estados Unidos, diz que, em seu país, o governo pode monitorar ligações e *e-mails*, desde que em busca de padrões. O conteúdo é violado nas hipóteses em que se percebem conexões regulares

DOI: https://doi.org/10.26512/lstr.v6i1.21550

com suspeitos de terrorismo. Disso decorre que, mesmo nestes casos, o governo necessita de requerimento a tribunal para acessar a comunicação. Apesar destas medidas de precaução, ele admite que bons técnicos são capazes de quebrar qualquer segurança na rede, citando exemplos públicos de quem já realizou este tipo de conduta. Opina, ainda, que o governo americano não deveria levantar informações econômicas de aliados sob pretexto de segurança (Dória e Rodrigues 2013). A par desta exceção, o ex-presidente afirma que, para a realidade americana, seria razoável levantar algumas informações não econômicas de aliados, informações – inclusive econômicas – de não aliados e informações consideradas sensíveis, que, no, caso americano, seriam contra o terrorismo. De fato, poder levantar e armazenar informações facilita a atuação do Estado na guerra cibernética.

Um risco que deve ser considerado, no que diz respeito a levantamento e armazenagem de informações, é o fato de que, dependendo do tipo de informações que estejam sob posse de governos totalitários, essas podem se tornar uma grande ameaça à liberdade de cidadãos, a ponto de a Constituição portuguesa proibir expressamente sequer a atribuição de número nacional único aos seus cidadãos em seu artigo 35.

Conclusão

A guerra cibernética se reveste de grande importância social, inclusive regulatória. Nas oportunidades em que a norma, por qualquer motivo, não conseguir produzir, por si só, os efeitos esperados, as técnicas de guerra cibernética poderão assegurar a tutela de bens jurídicos. Sendo um importante instrumento técnico a serviço do Estado para dar efetividade à lei, a esta deve se sujeitar. Trata-se de um instituto que se apresenta como manifestação de vácuo regulatório normativo, mas também como manifestação regulatória operacional, que necessita de regulação jurídica adequada. Desta forma, se promove segurança jurídica para o profissional que milita em tão sensível ramo de atividade e para a sociedade como um todo.

A sensação de segurança na vida em sociedade está intrinsecamente ligada à prestação de serviços pelo Estado, haja vista que este possui, de regra, o monopólio do uso da força. Existe uma preocupação, a qual diminui naturalmente a partir do desenvolvimento sustentado de uma democracia, de

como as forças políticas que governam o Estado usarão os dados e instrumentos a ele disponibilizados.

Com o desenvolvimento democrático em um Estado de Direito, as forças de segurança atuarão sempre em sinergia com a ordem legal, que é, em última análise, a vontade social.

Privacidade e outros direitos fundamentais devem ser preservados. A guerra cibernética deve proteger o Estado em pontos primordiais para a existência da sociedade, visto que esta pode se ver ameaçada concretamente em razão de um ataque virtual. Para tanto, deve-se investir em tecnologias, capacitação técnica de pessoal e regulação jurídica de defesa cibernética.

A regulação em pauta deve ser específica, visto que institutos como o Marco Civil da Internet possuem escopo paralelo, mas diverso da posição relativa da guerra cibernética como manifestação regulatória operacional frente à potencial regulação internacional sobre o setor.

A cooperação entre atores internacionais é importante, mas, tendo em vista que a expressão militar é um prolongamento da política que se utiliza da força das armas, deve-se considerar uma preparação adequada para um instituto necessário em situações de adversidade e crise. Para uma situação normal, que pode ser caracterizada pelo tempo de paz ou pela ausência de ações muito lesivas, basta a regulação civil de como se utilizar de computadores ligados em rede.

Frise-se que uma ameaça virtual relevante pode partir de pessoas comuns com conhecimentos adequados de rede de computadores; não necessariamente de Estados oponentes. Esta característica faz crescer a importância da guerra cibernética e sua regulação jurídica.

Sabe-se que a desregulação é uma forma de regulação, mas esta deve ser evitada. Os agentes públicos que labutam com segurança terão um resultado potencializado se souberem claramente seus limites de atuação. Quando os limites não são claros, é natural que os profissionais queiram mitigar o risco pessoal, evitando adentrar no que pode lhes ser defeso fazer. Para que a segurança cibernética seja assegurada com maior qualidade, deve ser fomentado um debate social sobre o tema.

Devem ser considerados os limites técnicos estabelecidos em países centrais, limites esses que muitas vezes são mais rígidos no Brasil em razão do ordenamento não privilegiar aspectos militares de segurança nacional.

DOI: https://doi.org/10.26512/lstr.v6i1.21550

A regulação jurídica específica pode melhorar a qualidade da proteção oferecida pela guerra cibernética brasileira, maximizar a segurança jurídica da sociedade e do profissional do ramo. Com regulação e investimentos adequados, a guerra cibernética pode oferecer para a sociedade algo que nem mesmo a norma consegue, em razão dos limites físicos da atuação do judiciário, inexistentes em ambiente virtual: a tutela a bens caros à sociedade e ao Estado brasileiro. Dessarte a democracia será reforçada e realimentada, em progresso continuado e fundamental para um importante ator global, como é o Brasil.[1]

Si vis pacem, para bellum
(Se queres a paz, prepara-te para a guerra)
Flavius Vegetius Renatus (390 D.C. - Roma)

Bibliografia

Agência Brasil. *Especialistas ouvidos por CPI alertam para baixa segurança da informação*. Brasília, 2013. Disponível em: http://www.correiobraziliense.com.br/app/noticia/politica/2013/10/22/interna_politica,394706/especialistas-ouvidos-por-cpi-alertam-para-baixa-seguranca-da-informacao.shtml, acessado em 18.11.13.

Aguillar, F.H. (1999) **Controle Social de Serviços Públicos**. São Paulo: Max Limonad.

Aguilhar, L. (2013) *A Espionagem Ultrapassou Limites*. São Paulo, Disponível em: http://blogs.estadao.com.br/link/a-espionagem-ultrapassou-limites/, acessado em 18.11.13.

Anatel. *Nono Dígito*. Brasília, 2012. Disponível em: http://www.anatel.gov.br/Portal/exibirPortalNivelDois.do?codItemCanal=1746&nomeVisao=Cidad%E3o&nomeCanal=Nono%20D%EDgito&nomeItemCanal=Nono%20D%EDgito, acessado em 19.02.14.

Bobbio, N. (1992) **A era dos direitos**. Trad. Carlos Nelson Coutinho. Rio de Janeiro: Elsevier.

Bonin, R. (2013) **O Livro Bomba**. In: *Revista Veja*, Editora Abril, São Paulo, edição 2351.

[1]Informações jornalísticas presentes neste trabalho possuem caráter meramente ilustrativo e exemplificativo, não impactando nas informações científicas aqui apresentadas.

DOI: https://doi.org/10.26512/lstr.v6i1.21550

Brasil. Câmara dos Deputados. (2013) Projeto de Lei do Marco Civil da Internet. Brasília: Câmra dos Deputados. Disponível em: http://edemocracia.camara.gov.br/web/marco-civil-da-internet/inicio, acessado em 12.12.13.

Brasil. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. (2008) **C 34-1: O Emprego da Guerra Eletrônica**. Brasília: EGGCF.

Congresso Internacional. Software Livre e Governo Eletrônico (V Congresso). **A favor de uma defesa ativa contra ataques cibernéticos**. Belém. Disponível em https://gestao.consegi.serpro.gov.br/cobertura/noticias/a-favor-de-uma-defesa-ativa-contra-ataques-ciberneticos, acessado em 16.02.14.

Crespo. M.X.F. (2011) Crimes digitais, Editora Saraiva, São Paulo.

Dória, P. e Rodrigues L. (2013) *Segurança não justifica espionagem econômica*. O Globo. Rio de Janeiro. Disponível em: http://oglobo.globo.com/pais/exercito-monitorou-lideres-de-atos-pelas-redes-sociais-9063915, acessado em 09.12.13.

Ferreira, R.S.P. (2009) **A (In)adequação dos Mecanismos Regulatórios Setoriais aos Institutos Jurídicos de Índole Constitucional do Mercado e da Universalização de Serviços Públicos**. Brasília: Universidade de Brasília.

Folha de São Paulo. *China é acusada de hackear reunião do G20* (2013), São Paulo. Disponível em: http://www1.folha.uol.com.br/fsp/mundo/143297-china-e-acusada-de-hackear-reuniao-do-g20.shtml, acessado em 12.12.13.

Grego. M. (2013) *Obama ordenou ataque ao Irã com Stuxnet, diz NYT*. Disponível em: http://exame.abril.com.br/tecnologia/noticias/obama-ordenou-ataque-ao-ira-com-stuxnet-diz-nyt, acessado em 08.12.13.

Grossmann L.O. (2013) *Espionagem dos EUA já cancela projetos de computação em nuvem*. São Paulo: Convergência Digital. Disponível em: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=34377#.UoqGqxrrzQs, acessado em 18.11.13.

INTERPOL. *A Global Presence*. Disponível em: http://www.interpol.int/Member-countries/World, acessado em 19.11.13.

Machado, H. B. (2008) **Curso de Direito Tributário**. Malheiros Editores, São Paulo.

Motta, S., *CDCIBER - Na Guerra Cibernética, Brasil adota estratégia do contra-ataque, Defesanet*. Redação do Portal IG, Brasília. Disponível em: http://www.defesanet.com.br/cyberwar/noticia/1632/cdciber---na-guerra-cibernetica--brasil-adota-estrategia-do-contra-ataque, acessado em 16.02.14.

Pinheiro, A.C. (2000) **Judiciário e Economia no Brasil**. São Paulo: Editora Sumaré.

Pinheiro, P.P. (2007) **Direito Digital**. São Paulo: Saraiva.

Redação G1 / Globo.com (2014) *Entenda o caso de Edward Snowden, que revelou espiongem dos EUA*. São Paulo: G1 Mundo. Disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html, acessado em 16.02.14.

Redação Info (2013) *Microsoft abre centro para combater crimes cibernéticos*. São Paulo: Info Exame. Disponível em: http://info.abril.com.br/noticias/internet/2013/11/microsoft-abre-centro-para-combater-crimes-ciberneticos.shtml, acessado em 08.12.13.

Rossi, G. (1995) ***Pubblico e Privatto nell'Economia di Fini Secolo. Le Trasformazioni del Diritto Amministrativo***. Milano: Giuffrè Editore.

Sassine. V. (2013) *Exército monitorou líderes de atos pelas redes sociais*. Rio de Janeiro: O Globo. Disponível em: http://oglobo.globo.com/pais/exercito-monitorou-lideres-de-atos-pelas-redes-sociais-9063915, acessado em 08.12.13.

Stuxnet. *Obama ordenou os ataques ao Irã*. (2013) Defesanet. Disponível em: http://www.defesanet.com.br/cyberwar/noticia/6262/stuxnet---obama-ordenou-os-ataques-ao-ira, acessado em 08.12.13.

Sundfeld, C. A. e Vieira, O. V. (1999) **Direito global**. São Paulo: Max Limonad.

Vilicic, F. (2013) *Por uma Web Sem Censura*. Revista Veja, edição 2351, Editora Abril, São Paulo.

Wimmer, M., Pieranti, O.P. e Aranha, M.I. (2009) *O paradoxo da internet regulada: a desregulação dos serviços de valor adicionado no Brasil*. In: ***Revista de Economía Política de las Tecnologías de la Información y Comunicación***. Vol. XI, n. 3, setembro-dezembro/2009.

DOI: https://doi.org/10.26512/lstr.v6i1.21550