Revista Brasileira de Direito Empresarial

e-ISSN: 2526-0235
DOI: 10.21902/
Organização Comitê Científico
*Double Blind Review* pelo SEER/OJS
**Recebido em:** 29.06.2015
**Aprovado em:**17.08.2015

# ENFOQUE JURÍDICO DA DEFESA CIBERNÉTICA APLICADA ÀS SOCIEDADES EMPRESÁRIAS

## ENFOQUE LEGAL DE CIBER DEFENSA APLICADA A EMPRESAS

**[1]Ronaldo Bach da Graça**

## RESUMO

Este artigo tem por finalidade apresentar a utilidade da defesa cibernética fomentada pelo Estado em favor de sociedades empresárias, o que, em última instância, acaba por favorecer toda a comunidade e o próprio Estado. O texto segue o método de abordagem descritivo e lógico-intuitivo, abordando que a sociedade deve proteger suas empresas como forma de manutenção da própria qualidade de vida. Uma das formas de proteção, relevante no momento em que vivemos, dá-se por meio da adequada proteção oferecida pela defesa cibernética. Foi constatado que é importante para o Direito Empresarial que se aborde sobre as garantias constitucionais que podem ser apoiadas por meio de uma atuação Estatal no contexto da defesa cibernética. Hodiernamente, doutrina e jurisprudência pátrias reconhecem direitos fundamentais das pessoas jurídicas, e existe uma relação de dependência entre a comunidade e suas sociedades empresárias que desemboca em melhor qualidade de vida, emprego e renda. Para que se preserve a segurança nacional, devem receber tutela especial os bens intangíveis das empresas que estão suscetíveis a ataques cibernéticos. O artigo contribui ao debate da proteção de sociedades empresárias pela guerra cibernética, concluindo que a segurança jurídica proporcionada pela atividade de guerra cibernética em favor das empresas e à proteção de seus direitos fundamentais protege a própria comunidade e o Estado do qual faz parte. O presente trabalho fomenta a proteção cibernética às empresas pelo Estado, como espécie de autoproteção e segurança da sociedade como um todo.

**Palavras-chave:** Direito empresarial, Defesa cibernética, Direitos fundamentais, Proteção dos ativos intangíveis de sociedades empresárias

## ABSTRACT

Este trabajo tiene como objetivo presentar la utilidad de ciberdefensa promovida por el Estado en favor de las empresas comerciales; que, en última instancia beneficia a toda la comunidad y el Estado. La investigación fue realizada por el método de enfoque descriptivo y lógico-intuitivo, mencionandose que la sociedad debe proteger a sus empresas como una forma de mantener la propia calidad de vida. Una forma de protección, relevante en el momento en que vivimos, se da a través de una adecuada protección ofrecida por la defensa cibernética. Es importante para el derecho de los negocios que se ocupe de las garantías constitucionales, que pueden ser apoyadas por un Estado que actúa con la defensa cibernética. En nuestros tiempos, doctrina y jurisprudencia en Brasil reconocen los derechos fundamentales de las personas jurídicas, y existe una relación de dependencia entre la

[1] Mestrando em Direito no Centro Universitário de Brasília, UniCEUB, Brasília, DF, (Brasil). E-mail.: ronaldobach@hotmail.com

comunidad y sus empresas comerciales que desemboca en una mejor calidad de vida, empleo y ingresos. Con el fin de preservar la seguridad nacional, deben recibir protección especial los activos intangibles de las empresas que son susceptibles a los ataques cibernéticos. El artículo contribuye al debate sobre la protección por la guerra cibernética de las empresas, concluyendo que la seguridad jurídica proporcionada por la actividad de la guerra cibernética en favor de las empresas y la protección de sus derechos fundamentales protege a la comunidad y el estado al que pertenece. Este trabajo fomenta la protección cibernética a las empresas per el Estado, como una especie de auto-protección y seguridad de toda la sociedad componente del Estado.

**Keywords/Palabras-claves/Mots-clés:** Derecho comercial, Ciber defensa, Derechos fundamentales, Protección de los activos intangibles de las empresas

## INTRODUÇÃO

A Guerra Cibernética é concebida para proteger a sociedade de ataques cibernéticos de eventuais oponentes, incluindo-se hipóteses de terrorismo. Por meio da leitura da Constituição Federal de 1988, pode-se perceber que o Brasil possui vocação de defesa, e não de iniciativas de ataques de guerra. O Brasil não pretende ser um país beligerante, mas quer sempre se defender com eficácia, efetividade e eficiência.

Ataques cibernéticos podem vulnerabilizar a sociedade como um todo, pois nos dias de hoje as redes informáticas permeiam muitas formas de relacionamento e de controle humanos. Sociedades empresárias podem ser vulnerabilizadas em eventuais ataques cibernéticos pela simples negação de um serviço vital para o desempenho de sua atividade; por meio de espionagem, que pode acontecer relacionada a informações estratégicas (como dados de negociação), relacionada a conhecimentos técnicos, tecnologias vitais e em alguns casos, únicas.

A depender dos valores em risco em razão de ataques cibernéticos, eventuais vulnerabilidades podem trazer consequências nefastas até mesmo para a segurança nacional, pois podem ser informações estratégicas para o país. Por tal motivo, deve-se fomentar nas empresas o interesse em terem ao seu lado, potencializando seus investimentos privados em segurança, um Estado protetor e proativo.

Sociedades empresárias bem estruturadas normalmente já possuem investimentos relacionados à segurança de redes informáticas. No entanto, o Estado deve apoiar, para o seu próprio bem e da sociedade, tais iniciativas de maneira sinérgica.

O presente trabalho abordará, a partir de direitos constitucionais relativos a sociedades empresárias, aspectos jurídicos que possam indicar razões para a fundamentação da implementação de políticas públicas que assegurem a defesa cibernética para as empresas, visando com isso à proteção de toda a comunidade.

Trata-se de um tema pouco explorado no Brasil, mas de grande relevância. Deve ainda ser considerada a relativamente restrita difusão das informações aqui retratadas para empreendedores, que com seus objetivos usuais de lucro, têm sido aliados de uma sociedade que preza qualidade de vida por meio de empregos de qualidade, renda e desenvolvimento cognitivo. A geração de impostos por parte de sociedades empresárias, por si só, já justificariam investimentos na área por parte do Estado. Se a defesa cibernética provida pelo Estado se desenvolve adequadamente, todos tendem a se beneficiar.

Para fomentar o debate acerca do tema, o capítulo primeiro tratará de direitos fundamentais da pessoa jurídica à luz da Constituição da República de 1988, focando direitos como privacidade, liberdade, propriedade. O capítulo segundo abordará o ciberespaço e alguns riscos a ele inerentes, discorrendo sinteticamente sobre riscos do mau uso de redes informáticas, riscos cibernéticos aos empreendedores, o valor da tecnologia e do conhecimento numa sociedade empresária. No capítulo terceiro o enfoque será no direito informático e a busca pela paz social, tratando aspectos do Estado e a segurança cibernética; e a segurança jurídica numa sociedade empresária e os reflexos da guerra cibernética. O capítulo quarto analisará sinteticamente alguns casos concretos. O quinto capítulo abordará uma possível solução, terminando todo o estudo com uma breve conclusão.

## 1. DIREITOS FUNDAMENTAIS DA PESSOA JURÍDICA À LUZ DA CONSTITUIÇÃO FEDERAL DE 1988

Theodoro Júnior (1988) discorre que a jurisprudência melhor posicionada acolhe o entendimento de que o nome, o conceito social e a privacidade, são bens cabidos e tutelados pela CR/88, tanto para pessoa física, quanto para pessoa jurídica. Logo, ambas podem reclamar ressarcimento por prejuízos causados tanto ao nome comercial, conceito na praça, sigilo nos negócios. Para a presente pesquisa, ressalte-se que são bens caros a uma pessoa jurídica como uma empresa, e tutelados pela Lei Magna.

Cardoso (1999, p. 84-88) opina no sentido de que a prevenção é o melhor meio para que o ilícito seja evitado, discorrendo que os problemas sociais são resolvidos não por normas, mas por meio de instrumentos de prevenção, e concorda que a prevenção a que se refere reclama uma intervenção dinâmica e positiva que neutralize suas raízes ou causas.

Do ensinamento, pode-se extrair a mensagem de que é sempre melhor a prevenção contra ilícitos. Instrumentos de prevenção podem ser fomentados por muitos meios, sendo que um dos mais eficazes é a mediação. Quando a mediação não é suficiente, buscam-se outros meios para que, em última análise, os regramentos impostos pela sociedade sejam seguidos de forma universal dentro de certa jurisdição.

Existe ainda alguma relação com o tema o fato de haver uma tendência cada vez mais visível, em que pese tratar-se de tema ainda controverso, quando se cogita pela indenização por dano moral à pessoa jurídica. Durante período considerável, houve o entendimento de que a lesão moral seria fenômeno atinente exclusivamente à pessoa natural. Dada a evolução cognitiva já se admite na doutrina e na jurisprudência tal possibilidade (SANTINI, 2002. p. 21-26).

A Constituição da República brasileira, promulgada em 1988, consagra diversos princípios e garantias, liberdades e prerrogativas das pessoas jurídicas, que evidenciam que as referidas garantias não se restringem a princípios de Direito Econômico. Direitos Fundamentais estão, entre outros princípios e regras, assegurados também às pessoas jurídicas e sua atividade empresarial. Outros direitos assegurados pela Constituição, que também são vitais para uma empresa, dizem respeito à segurança jurídica, tais como a previsibilidade e o direito a não surpresa, dentre outros (TAVARES, 2013, p. 13-14).

A titularidade de Direitos Fundamentais por sociedades empresárias é fundamento para qualquer regime constitucional, merecendo a atenção da Ciência do Direito, pois estão vinculados à ideia de Estado Democrático de Direito (TAVARES, 2013, p. 14-18). Preliminarmente, pode-se dizer que a Constituição da República de 1988 não faz distinção quanto à titularidade de Direitos Fundamentais, e discorre, no caput do art. 5º, sobre o princípio da igualdade de todos perante a lei, sem qualquer distinção. Em poucos casos, a CR/88 faz menção expressa à titularidade de Direitos Fundamentais por pessoa jurídica, como no caso do art. 5º, XXI (caso das associações para representar seus filiados), ou no caso do art. 8º, III (hipótese de sindicatos defendendo interesses de categorias) (TAVARES, 2013, p. 23-26). Muitos dos direitos elencados na Constituição são extensíveis às pessoas jurídicas, pois em diversas hipóteses, a proteção última do indivíduo perpassa a proteção oferecida pela

norma constitucional às pessoas jurídicas (BASTOS, 2000, p. 282). As pessoas jurídicas com a referida proteção podem ser tanto as brasileiras quanto as estrangeiras que atuem no Brasil (MASSON, 2015, p. 186-187).

O STF já se manifestou no sentido de que alguns direitos fundamentais dos contribuintes elencados no art. 15º da Constituição Federal de 1988 são aplicáveis para pessoas jurídicas quando figuram no polo passivo de uma relação tributária, admitindo, ainda que minimamente, a titularidade de direitos fundamentais por pessoas jurídicas (TAVARES, 2013, p. 26-27). O recurso extraordinário (RE) 63694/RS ratifica sobre possibilidade de aplicação de direitos fundamentais em uma sociedade empresária.

São os valores relevantes para a comunidade, os assegurados na Carta Constitucional, alguns dos mais importantes são considerados valores universais. Alguns, tratados como Direitos Fundamentais pela CR/88. Talvez pela razão apresentada, a atividade empresarial é dotada de sinergia quando valores constitucionais são realmente providos pelo Estado por meio de suas instituições. Princípios constitucionais mais especificamente vinculados à atividade empreendedora dependem de certa segurança oferecida pelo Estado.

Algumas leis ordinárias oferecem suporte para que o Estado assegure para as sociedades empresárias valores como a proteção da livre concorrência, que se opõe aos abusos de poder econômico, político e outros. Por certo, as normas têm alcançado de forma cada vez mais intensa a desejada eficácia social que oferece melhor suporte para que um empreendimento cumpra sua função social, conforme mandamento constitucional previsto na Magna Carta (art. 5º, XXIII; e art. 170, III da CR/88).

## 1.1 DIREITO À PRIVACIDADE

O art.5º, X CR/88 afirma que: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. André Ramos Tavares sustenta que a titularidade dos direitos retratados no presente inciso não é restrita a pessoas físicas, mas compreende também pessoas jurídicas; e cita que a conclusão a que chegou encontra guarida no entendimento do STF, citando como argumento a Reclamação 2040-1/DF, cujo relator foi o Ministro Néri da Silveira. O referido autor cita ainda o direito à imagem de pessoas jurídicas presentes tipicamente na rede mundial de computadores, oportunidade em que se pode evidenciar a tutela constitucional da imagem para pessoas jurídicas (TAVARES, 2013, p. 80-87). Por

certo, também a imagem deve ser protegida numa rede informática, mas podem-se citar outros valores que podem ameaçar de forma muito mais significativa a atividade empresária que se utiliza de redes informáticas de maneira direta ou indireta para desempenhar sua função social, prestando qualidade de vida por meio de produtos e/ou serviços oferecidos à comunidade.

## 1.2 DIREITO À LIBERDADE

A Lei Antitruste (Lei 8884/94), por exemplo, combate a concentração econômica e abusos que quedam por comprometer a livre concorrência prevista na Constituição Federal no artigo 150, IV. Para efetivar a intenção constitucional, a Lei transforma o Conselho Administrativo de Defesa Econômica (CADE) em autarquia, modifica procedimentos administrativos de investigação e repressão a condutas anticompetitivas. O *Sherman Act*, estadunidense, que tem por finalidade, dentre outras, combater práticas de restrição ao comércio, influencia diplomas legais por todo o mundo desde sua promulgação. Da mesma forma, o Tratado de Roma, na Comunidade Europeia (SCHUARTZ, 2015, p. 9-11).

## 1.3 DIREITO À PROPRIEDADE

Trata-se de um fundamento da atividade empresarial. O direito de propriedade deixou de ser absoluto, visto que a propriedade da sociedade empresária, como qualquer outra propriedade no Brasil, deve cumprir sua função social. Se, no Brasil de outrora, a propriedade tinha característica essencialmente individualista, hoje deve harmonizar o caráter de direito individual e a função social. Se, por um lado, há um direito subjetivo de exploração de determinado bem da vida baseado no inciso XXII do art. 5º da CR/88, por outro, há o mandamento do inciso XXIII do mesmo artigo, que induz concluir que a propriedade de uma sociedade empresária tem por finalidade também assegurar para a comunidade uma existência com dignidade e justiça social (art. 170, *caput*, Constituição da República de 1988) (TAVARES, 2013, p. 62-70).

Pela dualidade apresentada, há o interesse individual e o interesse público de que a propriedade seja preservada dentro de circunstâncias que assegurem dignidade e justiça social para todos. Tal fato leva a concluir que a preservação da propriedade para que ela cumpra sua função social também é interesse de todos, amparado na razão de que, de certa forma, todos são beneficiados pelo direito de propriedade de uma sociedade empresária.

Por certo, tal preservação também passa por uma segurança cibernética, que deve ser provida pelo Estado o qual se beneficia da propriedade junto com o proprietário. É evidente que o particular pode e deve investir em segurança cibernética a fim de que seus interesses individuais sejam preservados. No entanto, a Defesa Cibernética é uma ocupação que o Estado deve tomar também para si a fim de preservar os interesses sociais que ele representa e para o que ele foi formado.

Toda a explanação aqui presente sobre a aplicabilidade de Direitos Fundamentais em empresas desemboca na proteção destes direitos, quando aplicável, para sociedades empresárias. É desejável que as empresas tenham um mínimo de proteção provida pelo estado, até para que a sociedade possa se aproveitar da presença dos empreendedores com suas obras que fomentam o bem social. Modernamente não se pode imaginar uma proteção adequada sem adentrar no espectro da segurança cibernética.

## 2. O CIBERESPAÇO E OS RISCOS INERENTES

Ataques cibernéticos podem estimular concentração econômica e abusos que acabam por comprometer a livre concorrência. Tal fato acontece pela possibilidade de espionagem numa rede informática ou outra forma potencial de ilícito que tecnicamente é possível realizar por meio de uma rede. Lembre-se que hodiernamente é possível o controle de muitas máquinas à distância, oferecendo meios para muitas atividades danosas como manipulação ou sabotagem. Exemplo recente de ameaça significativa a atividades empreendedoras pode ser materializado na oportunidade em que os Estados Unidos foram denunciados por Edward Snowden por espionarem de forma sistemática uma das maiores e mais importantes sociedades empresárias do Brasil: a Petrobrás.

Motivos para espionar a Petrobrás, certamente o Estado americano os possuía e possui. No entanto, é difícil que algumas destas razões possam ser consideradas razoáveis pelo Direito, considerando os bens jurídicos tutelados e os atores envolvidos.

É público e notório que Snowden tem advertido a sociedade para o que ele considera excesso cometido pelo seu país natal, os Estados Unidos: espionagens de todo tipo, principalmente cibernética e de tráfego telefônico, que acarretam prejuízos inclusive para empresas. Segundo Edward Snowden, a privacidade está ameaçada pela inteligência estadunidense. Com ela, outros bens jurídicos tutelados pela Carta Constitucional.

O secretário executivo da entidade que zela pela governança da internet no Brasil, o Comitê Gestor da Internet (CGI), ao explicar a pressão da sociedade global por uma gestão internacional da rede, comentou que os Estados Unidos podem desligar a internet de qualquer país a qualquer momento (BBC, 2015).

O secretário Glaser da CGI.br informou que os Estados Unidos, em parte pressionados pelo escândalo descrito por Edward Snowden, concordaram em abrir mão da tutela que exercem sobre a Corporação da Internet para Designação de Nomes e Números (ICANN), entidade que administra questões técnicas importantes para o funcionamento da rede como a distribuição de domínios (endereços eletrônicos da internet) (BBC, 2015).

Modernamente, a maior parte das grandes empresas trabalham no sentido de criar vínculos na internet, muitas vezes canais de vendas e de comunicação. Por vezes pequenos empreendedores, dada a pouca disponibilidade de recursos, utilizam-se de *sites* de terceiros – como sites de leilões ou de classificados – para expandir suas vendas. Tal fato acaba por melhorar a qualidade de vida dos empreendedores envolvidos, seus funcionários, clientes.

Ameaçar a segurança na internet pode implicar em ameaçar as próprias empresas que se utilizam da rede mundial, e naturalmente tal fato pode trazer reflexos para a sociedade em aspectos como economia e segurança. A má utilização ou a negação do serviço da rede mundial de computadores pode causar prejuízos que transcendem o que se imagina usualmente. O mau funcionamento da rede mundial de computadores pode ameaçar a economia num aspecto macro, pois por meio deste serviço são gerenciadas redes elétricas, redes logísticas e outras atividades estratégicas para uma comunidade. Tais riscos exemplificados podem ser controlados ou ao menos relativizados por meio de uma boa estrutura estatal de proteção cibernética.

## 2.1 RISCOS DO MAU USO DE REDES INFORMÁTICAS

Os riscos que podem ser reportados a partir do mau uso de redes informáticas possuem um impacto econômico gigantesco, não só na empresa como na comunidade brasileira que espera que a empresa cumpra sua função social no país da forma mais abrangente possível. Uma sociedade de economia mista como a Petrobrás deve ter como escopo o fomento tecnológico para que o país detenha tecnologias de interesse; geração de emprego de qualidade e renda; transforme seu conhecimento tecnológico em produtos que gerem recursos para a sociedade brasileira e para a companhia. Os impostos que podem ser

gerados por meio de produtos e serviços podem ser altamente relevantes para toda a sociedade.

Quando um projeto, tecnológico ou não, é espionado, é possível que haja uma perda tecnológica estratégica para a empresa e para o Estado Brasileiro, principalmente se considerarmos, no exemplo, que a Petrobrás possui tecnologia de ponta no mundo e que, por vezes, ela é a única detentora de determinadas tecnologias. A Petrobrás, na hipótese de vazamento de tecnologia ou de conhecimento associado à sua *práxis*, tem muito a perder, e com ela a sociedade que a financia e acolhe. Perde na geração de empregos, na geração de impostos, na criação potencial de novos concorrentes em razão de informações furtadas por meio de práticas como a espionagem cibernética.

## 2.2 RISCOS CIBERNÉTICOS AOS EMPREENDEDORES

A internet é formada por indivíduos inseridos em um amplo conceito, que abrange a individualização de pessoas físicas, empresas, instituições e governos. A referida rede informática elimina o conceito de corporação unidimensional, impessoal e massificada, decorrendo profunda mudança na forma como o Direito deve encarar o relacionamento entre tais atores. O Direito deve atender à sociedade digital, e o fará por meio dos instrumentos do Estado (PINHEIRO, 2007, p. 1-2). Enquanto for possível, suportará este dever por meio das boas relações sociais. Em casos de necessidade, pelo Direito, e quando não restar outra alternativa para manter a ordem legal, terá que utilizar de sua força, que no caso de redes informáticas dependem dos técnicos que atuam com o que se chama de defesa cibernética. Por ser um bem jurídico tutelado tão ímpar e estratégico, e considerando que a ameaça a este bem jurídico pode se contrapor à segurança nacional, a maior parte dos países destina recursos de todo tipo para que seja defendido pelos profissionais da guerra e, em segundo plano, pelos órgãos de segurança pública. Todos estes participam do que se chama de Defesa Cibernética.

O Direito deve equilibrar, também na internet, interesses comerciais, privacidade (PINHEIRO, 2007, p. 43), interesses de Estado (para melhor servir à sociedade). O equilíbrio, se aceito pela sociedade, deve ser fomentado por meio de vigilância e punibilidade definidos pelo próprio Direito. Empresas disputam consumidores na internet, por vezes mitigam a privacidade alheia (PINHEIRO, 2007, p. 43), mas também merecem a proteção da sociedade e do Estado para que continuem a agregar valor por meio do trabalho. Por meio da *deep web*, segurança e riscos podem ser potencializados.

Pela rede, como já foi citado, pode-se ameaçar grande parte do patrimônio de uma sociedade, ameaçando suas empresas pela possibilidade de negação de serviços de rede, mitigação da privacidade acima dos limites permitidos pela sociedade, pela espionagem por meio da rede. Esta pode ameaçar todos os conhecimentos e tecnologias disponíveis ou mesmo diminuir o seu valor no mercado de forma significativa.

## 2.3 O VALOR DA TECNOLOGIA E DO CONHECIMENTO NUMA SOCIEDADE EMPRESÁRIA

A consciência da importância do valor da tecnologia e do conhecimento acaba por justificar investimentos estatais na atividade.

Para que se possa mensurar de forma mais precisa o prejuízo de um furto de tecnologia de ponta, pode-se constatar que se estão analisando hipóteses de tecnologias por vezes caríssimas, mas que perdem valor de forma intensa quando são difundidas ou ao menos deixam de ser segredo. O tempo também pode desvalorizar tecnologias dominadas, porém este processo tende a se acelerar em virtude da espionagem cibernética.

A maior parte dos países em desenvolvimento tem tentado agregar valor à sua economia industrializando produtos localmente, mas grande parte não fez progressos significativos. Apenas alguns poucos avançaram em processos como *catching-up*. O desenvolvimento tecnológico tem se mostrado fator fundamental para o desenvolvimento econômico de sociedades empresárias. Em economias centrais, mais da metade do desenvolvimento econômico de longo prazo são originados em mudanças tecnológicas que alimentam a produtividade, melhorando o desenvolvimento de novos produtos, processos e novos ramos de atividades (KIM, 2005, p 13-16). Tais atividades devem ser fomentadas e protegidas pela sociedade que destas atividades se aproveita.

A aptidão tecnológica se refere à condição de fazer uso efetivo de conhecimento tecnológico quando se deseja assimilar, utilizar, adaptar ou mudar tecnologias em uso. Inclui a capacidade de assimilar conhecimento e, a partir deste, gerar novo conhecimento. Compreende a produção, o investimento, a inovação. O acúmulo de aptidões tecnológicas, ao longo do tempo, pode fomentar uma industrialização mais célere, com o consequente desenvolvimento socioeconômico na hipótese de o fenômeno acontecer em regiões menos desenvolvidas (KIM, 2005, p 16-18). Se as atividades de defesa cibernética fomentadas pelo

Estado podem proteger tais valores que geram desenvolvimento sinérgico para toda a comunidade, o Estado deve, para seu próprio bem, fazê-lo.

A industrialização pode ser acelerada por meio da imitação, o que não implica necessariamente em falsificação ou clonagem de mercadorias importadas. A imitação pode ser uma atividade legal, que não envolve violação de patentes nem violação de propriedade intelectual (KIM, 2005, p. 27). Se a imitação é precedida de invasões cibernéticas alienígenas com foco em espionagem industrial, pode trazer grandes prejuízos para empresas, para a sociedade, para o ambiente acadêmico e para o governo que foram vítimas de tal atividade. A depender do tamanho do prejuízo socioeconômico, pode até mesmo ameaçar a segurança nacional. Deve-se ter sempre em mente que quando as empresas são ameaçadas, junto com elas é ameaçado o desenvolvimento social que geram, aí incluídos empregos e renda gerados e os impostos arrecadados que a sociedade espera receber delas. A proteção das sociedades empresárias contra ataques cibernéticos pode até ser realizada por uma atividade privada, mas o Estado pode e deve adotar políticas públicas que protejam as empresas deste tipo de vulnerabilidade, pois, mesmo em uma visão egoística, estaria, em última análise, protegendo a si próprio. Este raciocínio é evidenciado, inclusive, pelo cumprimento da função social da sociedade empresária: a empresa favorece a sociedade, e esta deve tomar medidas para fomentá-la e preservá-la.

A capacitação tecnológica é algo complexo, influenciado pelo ambiente de trabalho e de tecnologia, pelas políticas públicas, pela educação formal, pelo viés sociocultural e pela estrutura organizacional. As fontes do aprendizado tecnológico podem ser os esforços internos das sociedades empresárias, a comunidade nacional e a comunidade internacional (KIM, 2005, p. 145).

Das fontes apresentadas, a comunidade internacional constitui, por vezes, a mais relevante para sociedades empresárias em processo de *catching-up*, pois, quando mudanças tecnológicas são implementadas em países desenvolvidos, são criadas oportunidades favoráveis em países que tentam recuperar seu atraso tecnológico. Empresas que desenvolvem uma rede ampla e ativa com a comunidade internacional fortalecem sua própria capacidade tecnológica (KIM, 2005, p. 145-146), no entanto carecem ainda mais de proteção, porque por vezes lidam também com patrimônio de terceiros estrangeiros. A distância induz ao uso de redes informáticas para o trânsito de informações, e o prejuízo potencial para o Estado e a sociedade pode ser agravado pela possibilidade de indenização a empresas estrangeiras por eventual vazamento de informações estratégicas, obrigando o Estado a perder divisas para

pagamento de relevantes indenizações em hipóteses de pouca segurança no trânsito de informações. Mesmo em hipóteses de culpa concorrente, o prejuízo existe e deve ser evitado. Além do patrimônio do empreendedor em jogo, estão seus reflexos no bem e no desenvolvimento da sociedade acarretado pela empresa que busca inovação e desenvolvimento em sua produção, gerando emprego e renda no país.

Vale muito a pena para a sociedade investir nas sociedades empresárias. E a segurança cibernética é mais uma forma de investimento que favorece a todos, inclusive as empresas. Trata-se de um investimento que deve ser feito de toda forma. Quando se usa em favor de empresas, protege-se também a economia, pela consequente potencialização de segurança no trânsito de informações por redes informáticas. Para constatar tal assertiva, veja-se o exemplo estadunidense.

## 3. O DIREITO INFORMÁTICO E A BUSCA PELA PAZ SOCIAL

A preservação de tecnologias que geram desenvolvimento socioeconômico também é de interesse da sociedade, que pode contribuir com as empresas por meio do Estado. Uma das grandes vulnerabilidades de vazamentos de dados sobre a tecnologia agregada e que gera valor às empresas pode se dar por meio de redes informáticas, as quais podem ser mais bem protegidas com investimentos sistêmicos em Defesa Cibernética.

Pode-se, inicialmente, pensar que os riscos inerentes à internet atinentes a sociedades empresárias estariam restritos a ameaças contra empresas virtuais; provedores de acesso, de serviços e de conteúdos; comércio eletrônico e *e-Business*; propriedade intelectual e direito autoral em novas mídias; proteção de conteúdos; finanças virtuais; *internet banking*, *home broker*, *mobile banking* etc. Acontece que as ameaças potenciais são muito mais expressivas, sem querer diminuir a importância do que já foi citado para as empresas e para a comunidade em geral.

O Direito Informático tem raízes nos princípios fundamentais retratados na Carta Constitucional, mas está presente nas mais diversas áreas do Direito, tais como no Direito Empresarial, Direito Civil, Direito Autoral, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Internacional, entre outros ramos. O Direito Informático é subsidiado por princípios existentes no Direito há muito tempo. A norma antiga é, em grande parte, aplicável

a hipóteses em que se utilizam novas tecnologias. O que pode acontecer é uma análise mais aprofundada da norma por parte de quem interpreta e por conta de quem aplica as referidas normas. Novas tecnologias agregam ao mundo jurídico novas peculiaridades e desafios. Tal fato advém de novos comportamentos massificados em razão das novas formas de interagir em sociedade: das peculiaridades atinentes às novas tecnologias. Trata-se de novos procedimentos que devem ser regulados pelo Direito. Considere-se que a norma possui limitação temporal, como também possui uma atuação limitada em razão do espaço (territorialidade). A velocidade das transformações, por vezes, se mostra como barreira à normatização de determinadas condutas atinentes às novas tecnologias (PINHEIRO, 2007, p. 29-35).

O Direito Informático atende a uma sociedade marcada pela mudança de comportamentos em razão de novas tecnologias. A mudança comportamental é evidente nos negócios e nas relações entre indivíduos. Patrícia Peck cita a adoção cada vez mais frequente de um "Regime de Coopetição" (cooperação adicionado a competição), caracterizado pela necessidade cada vez maior das empresas em buscar a sobrevivência em um contexto de ambiente competitivo, globalizado e, principalmente, conectado. Na análise da autora, "empresas isoladas tendem a naufragar" (PINHEIRO, 2007, p. 55-56). Assim sendo, aumenta a importância da segurança e defesa cibernética. É para o bem da empresa que se pode prover esta segurança, mas é para o bem da comunidade e do Estado que esta proteção seja efetiva. Num mundo onde os bens intangíveis são valiosos para toda a sociedade e muitos deles circulam na rede, a segurança passa a ser requisito para a sobrevivência, principalmente das empresas.

O ciberespaço é o teatro de operações para a Guerra Cibernética, que perpassa as dimensões tradicionais da guerra, visto que possui correlação com atividades de defesa em terra, no mar, no ar e no espaço. O domínio cibernético tem a característica de interseção nos demais domínios (VENTRE, 2012, p. 35). A internet é um dos principais propulsores da era da informação, porém, os modernos meios tecnológicos, quando quebram barreiras territoriais, podem mitigar os conceitos de soberania e de Estado, dificultando o êxito de alguns procedimentos judiciais que culminariam com a tutela de bens jurídicos protegidos pela norma legal. Com isso, a Guerra Cibernética aparece como uma poderosa arma de alcance transnacional. Em razão de tal realidade, é necessária a cooperação entre os diversos atores do Direito Internacional (ÁLVARES, 2014, p. 101-102). Quando esta cooperação não é

possível, resta a técnica e as tecnologias utilizadas na Guerra Cibernética para proteger a soberania do Estado em ambiente virtual. E esta soberania, que seria relativizada sem a ação da defesa cibernética que visa proteger as empresas e a sociedade presentes em determinado território em cujo Estado pretende tutelar bens jurídicos independente de acordos internacionais.

## 3.1 O ESTADO E A SEGURANÇA CIBERNÉTICA

Com relação a estas hipóteses, o Estado pode prover a chamada Segurança Cibernética, que pode ser somada a iniciativas privadas de proteção, potencializando a segurança. Os atores envolvidos – Estado e sociedades empresárias que dominam informações relevantes sobre tecnologias, mercados etc – devem perceber que agindo de forma sinérgica tendem a potencializar os resultados obtidos numa relação de "ganha-ganha": ganham a empresa, o Estado e a sociedade. Preservam-se empregos, tecnologias, conhecimento, dados de gestão de projetos complexos, e evita-se concorrência desleal, por vezes predatória.

Na hipótese de algum agente deter um poder econômico desproporcional com relação a seus concorrentes, o mercado tende a concentrar poder e gerar desequilíbrio entre concorrentes. Por vezes o fenômeno da concentração econômica é lícito e desejável, quando, *v.g.*, se deseja fortalecer sociedades empresárias por meio de fusão, participação, aquisição (TAVARES, 2013, p. 48-51). Algumas das hipóteses apresentadas podem ser até fomentadas por um Estado que deseja fortalecer sua indústria, mas definitivamente a espionagem cibernética nunca comporá o presente rol com justiça social.

Ressalte-se, sobre o tema, que o poder econômico pode ser entendido como a detenção dos meios de produção, podendo estar concentrado até mesmo em uma única pessoa (MAGALHÃES, 1975, p. 16). Tais meios, na posse ou propriedade de uma sociedade empresária, são constitucionais e permitidos. O legítimo uso do poder econômico não sofre quaisquer restrições, sendo essencial para o desenvolvimento social (TAVARES, 2006, p. 261-262). Gera empregos de qualidade, renda; eventualmente nacionaliza ou desenvolve tecnologias, produtos, serviços, conhecimentos laborais.

## 3.2 SEGURANÇA JURÍDICA NUMA SOCIEDADE EMPRESÁRIA E OS REFLEXOS DA GUERRA CIBERNÉTICA

Arrolada no art. 5º da CR/88, a segurança jurídica é um direito relevante quando se trata de atividade empresarial. A previsibilidade é um dos indícios de segurança jurídica (TAVARES, 2013, p. 78-79). A manutenção do Direito em ambiente virtual não depende apenas de normas que amparem relações sociais em uma rede informática, o que pode ser constatado pelo fato de que o conceito de territorialidade, altamente atrelado ao conceito clássico de jurisdição é relativizado num teatro de operações típico de combate cibernético. Por vezes, o ataque é realizado a partir de um país distante e se utilizando de meios que podem estar espalhados pelo mundo.

Tendo em vista que o Direito sozinho não consegue garantir a lei e a ordem em ambiente virtual, verifica-se a importância da supremacia ou ao menos superioridade no ambiente virtual.

Neste ponto convém diferenciar a supremacia da superioridade técnica quando se trata de combates virtuais. Em síntese, pode-se afirmar que uma força possui supremacia técnica (ou, no caso, cibernética) quando consegue aniquilar facilmente seu oponente; enquanto que terá apenas superioridade nas técnicas de cibernética se sua força integrada tiver um poder combativo maior do que a força adversa, porém não terá facilidade para assegurar o tráfego efetivo e seguro nas redes informáticas nas quais presta seu serviço.

A desejável supremacia técnica ou a possível superioridade não pode ser oferecida sem investimento sistêmico e esforço social materializado em políticas públicas oferecidas por meio de regulamentação e regulação adequadas para a realização da atividade. Tal fato pode ser constatado por meio de um simples exercício de raciocínio: via de regra, os profissionais que oferecem serviços de Defesa Cibernética, assim como todos os profissionais, desejam saber exatamente o risco inerente do exercício de sua profissão para que possam cumprir suas atribuições de forma segura e à medida que a sociedade deseja. Isto partindo do pressuposto de que a sociedade deve decidir o que é melhor pra si, e não o profissional que presta o serviço de defesa cibernética. Em outras palavras, o profissional de defesa cibernética tem a comunidade em que vive como cliente, e somente ela pode oferecer a melhor representação do que deseja, assumindo as consequências de sua opção.

A Defesa cibernética pode prover segurança jurídica pela implementação de técnicas de defesa para que o direito se faça valer onde a decisão judicial sozinha não consegue assegurar direitos. No entanto cobra-se um preço: a relativização de alguns direitos fundamentais, como a privacidade. Os limites da atuação destes profissionais devem ser

oferecidos pela sociedade organizada, que deve ainda considerar que não é seguro para nenhuma comunidade que a referida atividade seja utilizada com fins políticos. Por este motivo, sugere-se que a solução ofertada pela comunidade passe ao largo do controle da classe política. Ademais, o Estado Administrativo, segundo entendimento do Professor Marcio Iorio Aranha, possui a virtude de tornar convergentes noções de profissionalismo e expertise tradicionalmente aplicadas aos negócios privados, para que sejam aplicadas no contexto da atividade de governar com a conotação de permanência, treinamento, especialização de funções (ARANHA, 2014. p. 11-15). Trata-se de uma forma de reconhecimento de que as empresas têm muito que ensinar ao Estado para que ele sirva à sociedade de forma eficaz. E complementa o professor, num contexto de Direitos Fundamentais objetivados e Estado Regulador, que o adensamento do conteúdo dos direitos fundamentais pode ser auxiliado de forma relevante pela regulação (ARANHA, 2014. p. 9-11). Pode-se aduzir deste entendimento que o Estado que se utiliza dos préstimos de sociedades empresárias pode ainda prestar um melhor serviço para pessoas físicas e jurídicas, por meio de adequada regulação. Na hipótese em análise, regulação do setor cibernético com treinamento compatível, especialização de funções; o que pode ser alcançado por meio de políticas públicas de Estado, preferencialmente materializadas em leis.

Um controle político das atividades de defesa cibernética poderia deixar a sociedade refém de um governo mal intencionado que desejasse se utilizar de dados coletados em favor de um controle sobre a população, quando, em verdade, um Estado democrático deve servir à comunidade, e não que seja servido por ela.

Um autor que retrata muito bem o que uma sociedade democrática espera do Estado é o professor Carlos Ayres Britto (2012, p. 116). O referido autor ressalta que "[...] o judiciário não tem do governo a função, mas tem do governo a força. A força de impedir o desgoverno, que será tanto pior quanto resultante do desrespeito à Constituição." E sugere o autor que a governabilidade, tornada uma práxis, corresponderá ao clímax do humanismo e da democracia. Pode-se concluir que todos devem respeitar os limites ditados pela Constituição para que o Estado seja o que a sociedade deseja. Destarte, por meio de adequada regulação que passe ao largo do controle político, a sociedade poderá mensurar os investimentos e procedimentos que são úteis para que a comunidade alcance os objetivos os quais deseja.

## 4. CASOS CONCRETOS

Os Estados Unidos envolveram-se maciçamente assumindo riscos de empreendedorismo para estimular a inovação. Em tal contexto, podem-se citar exemplos de êxito como o da Agência de Projetos de Pesquisa Avançada de Defesa do governo estadunidense (DARPA), o Programa de Pesquisa para a Inovação em Pequenas Empresas (SBIR), o *Orphan Drug Act* e a *National Nanothecnology Initiative* (Iniciativa Nacional de Nanotecnologia). Todos estes exemplos representam uma abordagem proativa do Estado americano com escopo de moldar um mercado que impulsionasse a inovação naquele país. É o Estado desempenhando um papel de empreendedor em áreas inovadoras do conhecimento. Trata-se de políticas públicas adotadas com visão estratégica em atividades altamente inovadoras com pesquisas de risco que o Estado tomou pra si (MAZZUCATO, 2014, p. 109-125) com foco no desenvolvimento socioeconômico. Por certo, utilizaria empresas para alcançar seus objetivos estratégicos.

Ainda para ilustrar os casos de êxito para o país quando o poder público assume investimentos e riscos, destaca-se o caso da Apple com o iPhone. Produtos revolucionários como iPhone, iPad e iPod possuem tecnologias básicas incorporadas que são resultantes de décadas de apoio federal em inovação. Grande parte da tecnologia incorporada a tais produtos foi desenvolvida por meio de esforços de pesquisa e apoio financeiro do governo e das Forças Armadas estadunidenses (MAZZUCATO, 2014, p. 126-129).

O Estado pode e deve, dentro de suas possibilidades, investir em inovação e tecnologia. Tais investimentos por certo auxiliarão o desenvolvimento socioeconômico e, por consequência, o desenvolvimento do Estado. Com o mesmo empenho que o Estado deve agir sinergicamente com o meio acadêmico e com as empresas gerando emprego e renda, deve zelar pela manutenção destas conquistas da sociedade que o sustenta. Uma das formas é investindo em defesa cibernética e oferecendo tal proteção para a sociedade de forma estratégica, inclusive protegendo as empresas que geram desenvolvimento e renda por meio de impostos e outros investimentos na comunidade.

Mesmo sem espionagens, ainda que eventualmente precedidos destas, ataques cibernéticos podem causar grandes transtornos para empresas e para a comunidade que se utiliza de seus serviços. Recentemente foi noticiado que a Bolsa de Valores de Nova Iorque (NYSE), a companhia aérea United Airlines e o jornal estadunidense *Wall Street Journal* (WSJ) teriam sido vítimas de falhas técnicas em suas redes informáticas. A bolsa de Nova Iorque ficou fechada por quase quatro horas no dia 8 de julho de 2015. No mesmo dia, a americana United Airlines ficou por duas horas sem operar qualquer voo em todo o mundo, e

o WSJ ficou com sua página fora do ar por alguns momentos e instável por período mais longo. Ainda que tenha sido desmentido pelo próprio FBI (agência que compõe a inteligência estadunidense) (VALOR ECONÔMICO, 2015), sites internacionais indicaram um possível ataque *hacker* direcionado para grandes instituições corporativas dos Estados Unidos (CARVALHO, 2015).

Percebe-se dos casos citados uma pequena amostra do potencial de ataques cibernéticos, pois, ainda que o FBI tenha afirmado que os supostos defeitos da rede não tenham sido ataques as falhas poderiam ter sido consequências de ataques, e, para o presente estudo, vale apenas a hipótese de que as falhas tenham sido consequências de ataques cibernéticos. Trata-se de casos que certamente causaram grande transtorno e prejuízo, mas que representam muito pouco em face do potencial de ataques cibernéticos. A sociedade, incluindo as empresas, precisa de proteção contra tais ameaças. O Estado pode fomentar tal proteção de forma bastante eficaz se conseguir investir na Defesa de forma sistêmica, planejada e responsável; mas tudo na medida em que a comunidade, por meio de um debate social, considere adequado. A sociedade diz o que prefere e assume as consequências de suas opções políticas.

Os profissionais que lidam com ataques que envolvam tecnologia precisam de treinamento contínuo e específico, sob pena de serem ineficazes. Afinal, tecnologias podem ser superadas em períodos bastante pequenos.

Julian Assange, do sítio WikiLeaks, recluso há alguns anos na Embaixada do Equador em Londres, opina sobre o prejuízo que a sociedade brasileira, podendo-se incluir suas empresas, podem ter com eventual inércia do governo brasileiro em não se defender de supostos ataques de espionagem que podem se dar também por meio de procedimentos cibernéticos:

> Se a presidente Dilma Rousseff quer ver mais investimentos dos EUA no Brasil na esteira de sua recente viagem ao país, como ela afirma, como ela pode assegurar às empresas brasileiras que as companhias norte-americanas não têm uma vantagem proporcionada por esta vigilância. Até que ponto ela pode realmente garantir que a espionagem foi encerrada - não apenas sobre ela, mas sobre todas as questões brasileiras (GLOBONEWS, 2015).

Tal assertiva evidencia possibilidade de prejuízos significativos às empresas nacionais como também para toda a sociedade brasileira até que a espionagem contra cidadãos e empresas possa, ao menos, ser identificada tecnicamente. Incluem-se ainda nesse risco a possibilidade de sabotagem e outras técnicas prejudiciais à comunidade brasileira.

## 5. UMA POSSÍVEL SOLUÇÃO

A solução para a proteção cibernética passa necessariamente pelo tratamento dos dados de vigilância cibernética, além de acordos transnacionais. A comunidade internacional tem agido de forma cada vez mais colaborativa. Um acordo global diminuiria o risco de beligerância, melhorando as relações (GRAÇA, 2014). A matéria referente a tratamento de dados tem merecido regulamentação, como ocorre na Itália desde 2003. Este país publicou importante norma relacionada ao tema "tratamento de dados pessoais": o Decreto Legislativo 196, de 30 de junho de 2003.

Já no art. 1º, a norma supracitada declara que todos têm o direito à proteção de dados pessoais que lhe digam respeito. Pelas razões já elencadas, entende-se que essa proteção valeria, no Brasil, também para pessoas jurídicas. A proteção assegura, no art. 2º, o respeito aos direitos e às liberdades fundamentais, o respeito à dignidade, dentre outras garantias.

A referida norma tem a preocupação de ditar as pessoas competentes para tratamento de dados, diferenciando o titular do tratamento, o responsável (designado facultativamente pelo titular) e os encarregados pelo tratamento, medidas de segurança dos dados e dos sistemas. O referido diploma legal destaca o que se consideram medidas mínimas de segurança, regulamenta a transferência de dados ao exterior, e possui ainda um título que trata especificamente dos serviços de comunicação eletrônica:

> TITOLO X - COMUNICAZIONI ELETTRONICHE
> CAPO I - SERVIZI DI COMUNICAZIONE ELETTRONICA
> Art. 121 (Servizi interessati)
> 1. Le disposizioni del presente titolo si applicano al tratamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni.
> Art. 122 (Informazioni raccolte nei riguardi dell'abbonato o dell'utente)
> 1. Salvo quanto previsto dal comma 2, è vietato l'uso di uma rete di comunicazione elettronica per accedere a informazioniarchiviate nell'a pparecchio terminale di un abbonato o di um utente, per archiviare informazioni o per monitorare le operazioni dell'utente.
> 2. Il codice di deontologia di cui all'articolo 133 individua i presupposti e i limiti entro i quali l'uso della rete nei modi di cui al comma 1, per determinati scopi legittimi relativi ala memorizzazione tecnica per il tempo strettamente necessário alla trasmissione della comunicazione o a fornire uno specifico servizio richiesto dall'abbonato o dall'utente, è consentito al fornitore del servizio di comunicazione elettronica nei riguardi dell'abbonato e dell'utente che abbiano espresso il consenso sulla base di una previa informativa ai sensi dell'articolo 13 che indichi analiticamente, in modo chiaro e preciso, le finalità e la durata del trattamento.
> Art. 123 (Dati relativi al traffico)
> 1. I dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più

> necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei commi 2, 3 e 5.
> 2. Il trattamento dei dati relativi al traffico strettamente necessari a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessária per effetto di una contestazione anche in sede giudiziale.
> 3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico può trattare i dati di cui al comma 2 nella misura e per la durata necessarie a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, solo se l'abbonato o l'utente cui i dati si riferiscono hanno manifestato il próprio consenso, che è revocabile in ogni momento.
> 4. Nel fornire l'informativa di cui all'articolo 13 il fornitore del servizio informa l'abbonato o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del medesimo trattamento ai fini di cui ai commi 2 e 3.
> 5. Il trattamento dei dati personali relativi al traffico è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'articolo 30 sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni e che si occupano della fatturazione o della gestione del traffico, di analisi per conto di clienti, dell'accertamento di frodi, o della commercializzazione dei servizi di comunicazione elettronica o della prestazione dei servizi a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessário per lo svolgimento di tali attività e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata. 6. L'Autorità per le garanzie nelle comunicazioni può ottenere i dati relativi alla fatturazione o al traffico necessari ai fini della risoluzione di controversie attinenti, in particolare, all'interconnessione o alla fatturazione.
> (...)
> Art. 132 (Conservazione di dati di traffico per altre finalità)
> 1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico sono conservati dal fornitore per trenta mesi, per finalità di accertamento e repressione di reati, secondo le modalità individuate con decreto del Ministro della giustizia, di concerto con i Ministri dell'interno e delle comunicazioni, e su conforme parere del Garante (ITALIA, 2003).

O art. 132 do Decreto Legislativo ora referenciado trata sobre coleta de dados e tratamento de dados dentro do respeito às medidas e meios de garantia do interessado. Numa análise sistemática da norma, conclui-se que ela abrange, inclusive, comunicações telefônicas. Deve-se destacar que parte das comunicações telefônicas existentes hoje no Brasil e no mundo acontece tecnicamente na internet, por meio de tecnologias como voz sobre IP (VOIP), ou por outras formas de trânsito de dados. Do exposto, pode-se concluir que também esta forma de comunicação depende da proteção cibernética, até porque, mesmo quando a comunicação não se dá por meio de redes informáticas, estas normalmente são utilizadas no gerenciamento de comunicações telefônicas "tradicionais". Existem normas europeias sobre o

assunto, tais como a Diretiva 95/46/CE – referente à proteção das pessoas no que diz respeito ao tratamento de dados pessoais e à livre circulação dos mesmos dados – e a Convenção 108, a qual regulamenta a proteção das pessoas em relação ao tratamento automatizado de dados pessoais.

Se os instrumentos normativos mencionados fossem tomados como parâmetro, certamente protegeriam também pessoas jurídicas, consoante doutrina e jurisprudência brasileiras apresentadas no presente trabalho. Seria, ao mesmo tempo, um limite das atividades empresariais e uma proteção contra os excessos das mesmas atividades. É público e notório que a França adotou recentemente uma legislação que permite uma postura bastante intrusiva nos dados que circulam na internet com a finalidade de uma maior proteção contra o terrorismo. O mesmo acontece nos Estados Unidos, mesmo sem a reedição do *Patriotc Act*, fato amplamente divulgado pela imprensa mundial. Pode-se, ainda, citar como instrumento transnacional que trata do tema as Linhas Diretrizes da OCDE (Organização para a Cooperação e Desenvolvimento Econômicos), altamente ligada ao direito empresarial e à realidade no Brasil, pois, desde 2013, o governo brasileiro cria formas de implementar tais diretrizes em empreendimentos sob jurisdição brasileira (PALMA, 2013).

## CONCLUSÃO

Muitos são, em potencial, os riscos que empresas podem correr em razão de superioridade ou supremacia de oponentes no ciberespaço. Por certo, empresas de maior expressão podem arcar com elevados gastos de segurança de redes informáticas. No entanto, nem sempre se pode considerar razoável o aludido investimento, a depender do contexto.

Pode-se dizer que a sociedade depende de suas empresas para alcançar maior bem-estar social. Por vezes, a ameaça cibernética a uma sociedade empresária pode trazer caos a empresas prestadoras de serviços de quase todos os setores, inclusive serviços públicos, como os de geração de energia, controle de trânsito, abastecimento de água e luz, dentre outros. Destaca-se que estes e outros serviços públicos, ainda que essenciais, muitas vezes são prestados por empresas privadas.

Quando a sociedade protege suas empresas, protege a si mesma, sua economia, seus empregos. Em algumas hipóteses até mesmo a vida de alguém pode estar ameaçada por causa de ameaças cibernéticas, como ocorre numa simplória hipótese de interrupção no fornecimento de energia elétrica numa região onde se encontra um hospital.

Ao optar por atuar na segurança cibernética em favor também de empresas que geram serviços, produtos, empregos, e impostos para o país, o Estado protege a si mesmo e à sociedade que dele se serve. Mesmo o regular funcionamento de simples transações bancárias, *v.g.*, é essencial para o equilíbrio social.

O debate social deve considerar os direitos, inclusive os fundamentais, que a CR/88 e as normas infraconstitucionais asseguram às empresas. A tecnologia e o conhecimento agregados, a partir de pesquisas, a produtos e serviços devem ser vistos pelo Estado e pela sociedade como algo estratégico e que pode ser preservado por meio da defesa cibernética, pois ela pode ser usada como instrumento ou técnica para que a lei seja cumprida dentro da jurisdição nacional. É um fazer cumprir por meios técnicos na dimensão onde o Direito, por si só, teria dificuldades de atuar de forma eficiente.

Políticas públicas, preferencialmente implementadas a partir de leis, podem auxiliar a sociedade neste processo de maturação, para que o Estado possa ser cada vez mais eficaz. Meios de Guerra Cibernética podem proteger até mesmo contra o terrorismo cibernético, assim como auxiliar muitas investigações estratégicas para uma nação.

Os Estados que possuem melhores condições costumam investir recursos com foco no desenvolvimento de tecnologias e estratégias de negócios que serão utilizadas inclusive em transações privadas. O bem-estar social, quando puder ser ameaçado por meio de redes informáticas, deve ser preservado com o mesmo esmero com que foi conquistado.

Mitigando o mau uso de redes informáticas, quer pela educação e pelo Direito quando isso for possível, quer por técnicas de defesa cibernética para fazer valer a norma quando for necessário, o Estado contribuirá com a sociedade no sentido de preservar a paz social e outros valores. O risco do negócio em uma sociedade empresária pode aumentar relevantemente se o gerenciamento e a comunicação proporcionados por redes informáticas não forem seguros.

Snowden já mostrou que a espionagem que acontece por meio de redes informáticas pode ser desastrosa para a sociedade. E frise-se que o ex-agente da NSA focou sua delação em espionagem realizada pelo Estado Americano, sem comentar sobre a ameaça vinda por concorrentes, risco mitigável pela defesa cibernética e prática proibida pela norma brasileira.

A defesa cibernética, que protege a eficácia da norma para uma melhor garantia dos Direitos aplicáveis às empresas e à sociedade como um todo, também depende da norma, estimulando e implementando condutas de interesse no campo da defesa cibernética. Neste contexto o Estado pode apoiar para que se conviva em uma sociedade mais justa e próspera.

## REFERÊNCIAS

ÁLVARES, João Gabriel. **Territorialidade e Guerra Cibernética.** *In:* Segurança e Defesa Cibernética: Da Fronteira Física aos Muros Virtuais. Org. Oscar Medeiros Filho *et al.* Recife: Ed. UFPE, 2014. p. 101-102.

ARANHA, Marcio Iorio. **Manual de Direito Regulatório: Fundamentos de Direito Regulatório.** 2ª Ed. rev. ampl. Coleford, UK: Laccademia Publishing, 2014. p. 9-11.

BASTOS, Celso Ribeiro Bastos. **Curso de Direito Constitucional.** 21ª ed. São Paulo: Saraiva, 2000, p. 282.

BBC. **EUA podem desligar a internet de qualquer pais, diz comitê brasileiro.** Disponível em: <http://g1.globo.com/tecnologia/noticia/2015/07/eua-podem-desligar-internet-de-qualquer-pais-diz-comite-brasileiro.html>. Acesso em: 11/07/2015.

BRITTO, Carlos Ayres. **O Humanismo Como Categoria Constitucional.** 1ª ed. 2ª reimp. Belo Horizonte: Fórum, 2012. p. 116.

CARDOSO, Atinoel Luiz. **Das Pessoas Jurídicas e Seus Aspectos Legais: Sucessão Comercial, Fundações e Associações, Direito Público e Direito Privado, Capacidade e Vontade Jurídica, Sociedade Anônima e Holding, Instituições e Vontade Social, Extinção da Pessoa Jurídica.** AEA Edições Jurídicas, 1999: São Paulo. P. 84-88.

CARVALHO, Caio. **Erro de computador afeta sistemas da Bolsa de Nova York, United Airlines e WSJ**. Disponível em: <http://canaltech.com.br/noticia/seguranca/erro-de-computador-afeta-sistemas-da-bolsa-de-nova-york-united-airlines-e-wsj-44789/>. Acesso em: 09/07/2015.

GLOBONEWS. **EUA grampearam Dilma, ex-ministros e avião presidencial, revela WikiLeaks.** Disponível em: <http://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html>. Acesso em: 11/07/2015.

GRAÇA. Ronaldo Bach da. **Regulação da Guerra Cibernética e o Estado Democrático de Direito no Brasil.** Disponível em: <http://www.ndsr.org/SEER/index.php?journal=rdet&page=article&op=view&path%5B%5D=93&path%5B%5D=78>. Acesso em: 11/07/2015.

ITALIA. **Decreto legislativo 30 giugno 2003, n. 196**. Codice in matéria di protezione dei dati personali. Disponível em: <http://www.camera.it/parlam/leggi/deleghe/03196dl.htm>. Acesso em: 11/07/2015.

KIM, Linsu. **Da imitação à inovação: a dinâmica do aprendizado tecnológico da Coréia.** Campinas:Editora Unicamp, 2005. p 13-16.

MAGALHÃES, Guilherme A. Canedo de. **O Abuso do Poder Econômico: apuração e repressão.** Rio de Janeiro: Artenova, 1975. p. 16.

MASSON, Nathalia. **Manual de Direito Constitucional** - 3a ed.: Revista, ampliada e atualizada. Salvador: Juspodivm, 2015, p. 186-187.

MAZZUCATO, Mariana. **O Estado Empreendedor: Desmascarando o Mito do Setor Público vs. Setor Privado.** Trad. Elvira Serapicos. 1ª Ed. São Paulo: Portifolio-Penguin, 2014. p. 126-129.

PALMA, Gabriel. **Governo cria Grupo de Trabalho para Implementar Diretrizes da OCDE para multinacionais.** Disponível em: <http://memoria.ebc.com.br/agenciabrasil/noticia/2013-02-20/governo-cria-grupo-de-trabalho-para-implementar-diretrizes-da-ocde-para-multinacionais>. Acesso em: 11/07/2015.

PINHEIRO, Patrícia Peck. **Direito Digital.** 2ª ed. rev., atual. e ampl. São Paulo: Saraiva, 2007. p. 1-2

SANTINI, José Raffaelli. **Dano Moral.** Campinas: millennium, 2002. P. 21-26.

SCHUARTZ, Luis Fernando, et al. **Direito da Concorrência.** Nota de Aula do Curso LLM-5 de Direito Empresarial. Rio de Janeiro: FGV, 2015, p. 9-11.

TAVARES, André Ramos. **Direito Constitucional Econômico.** 3ª Ed. São Paulo: Método, 2006, v. 1. p. 261-262.

TAVARES, André Ramos. **Direito Constitucional da Empresa.** Rio de Janeiro: Forense, 2013, p. 23-26.

THEODORO JÚNIOR, Humberto. **Dano Moral.** 1ª ed., São Paulo: Oliveira Mendes, 1988.

VALOR ECONÔMICO. **FBI não encontra Indício de Ataque Cibernético em Falha na Bolsa de NY**. Disponível em: <http://www.valor.com.br/financas/4127214/fbi-nao-encontra-indicio-de-ataque-cibernetico-em-falha-na-bolsa-de-ny>. Acesso em: 09/07/2015.

VENTRE, Daniel. **Ciberguerra.** *In:* XIX Curso Internacional de Defensa, 2011. Seguridad Global y Potencias Emergentes em um Mundo Multipolar. Zaragoza: Imprenta Ministerio de Defesa, 2012. p. 35.