QUALIFICAÇÃO DO AUTOR

Luiz Fabricio Thaumaturgo Vergueiro, Doutor em Direito Internacional pela Faculdade de Direito da Universidade de São Paulo, Pós-Doutor em Sistemas Complexos pela Escola de Ciências, Artes e Humanidades da Universidade de São Paulo, Pós-Doutor em Políticas de Segurança e Defesa Nacional pelo Colégio Interamericano de Defesa (Washington/DC). Advogado da União, ex-Consultor Jurídico da Amazônia Azul Tecnologias de Defesa S/A, empresa pública federal vinculada ao Ministério da Defesa, responsável pelo desenvolvimento programa de submarinos da Marinha do Brasil (Prosub) e do Programa Nuclear Brasileiro (PNB). Professor da Escola Superior da Advocacia-Geral da União (ESAGU).
Telefone (cel.): (11) 98560-8092, e-mail: luizfabriciovergueiro@gmail.com

MARCO CIVIL DA INTERNET E GUERRA CIBERNÉTICA: ANÁLISE COMPARATIVA À LUZ DO MANUAL DE TALIN SOBRE OS PRINCÍPIOS DO DIREITO INTERNACIONAL APLICÁVEIS À GUERRA CIBERNÉTICA

INTERNET CIVIL FRAMEWORK AND CYBERWARFARE: COMPARATIVE ANALYSIS IN LIGHT OF THE TALIN MANUAL ON THE PRINCIPLES OF INTERNATIONAL LAW APPLICABLE TO CYBERWARFARE

RESUMO

O novo Marco Civil da Internet, introduzido no ordenamento jurídico brasileiro pela Lei nº 12.965, de 23 de abril de 2014, representa inovação paradigmática tanto para os operadores de Direito brasileiros, quanto para a comunidade jurídica internacional, que vem debatendo continuamente os reflexos da rede mundial de computadores no enorme plexo de relações que se estabelecem por seu intermédio, ou em função de sua existência, e que demandam regulação adequada às finalidades e princípios da rede, mas tendo em mente princípios jurídicos fundamentais para a espécie humana. Nesse contexto, surge iniciativa de âmbito internacional que busca adaptar parcela relevante do Direito Internacional Público ao uso da Internet como arma e cenário em conflitos entre nações. Desse esforço acadêmico institucional surgiu o "Manual de Talin sobre o Direito Internacional Aplicável à Guerra Cibernética", cujas proposições podem servir de guia ao operador de Direito brasileiro que se veja confrontado com o exame do fenômeno da Guerra Cibernética à luz da já vigente legislação nacional.

Palavras-chave: Marco Civil. Internet. Guerra Cibernética. Manual de Talin

ABSTRACT

The new Internet Civil Rights Framework, introduced into Brazilian legal system by Law No. 12,965 of April 23, 2014, represents a paradigmatic innovation for both Brazilian legal operators and for the international legal community, which has been continuously debating the effects of the World Wide Web on the enormous plexus of relationships that are established through it, or due to its existence, and that require appropriate regulation to the purposes and principles of the network, but having in mind legal principles that are fundamental to the human species. In this context, an international initiative arises that seeks to adapt a relevant portion of Public International Law to the use of the Internet as a weapon and scenario in conflicts between nations. This institutional academic effort gave rise to the "Tallinn Manual on the International Law Applicable to Cyber Operations," whose proposals may serve as a guide to the Brazilian legal practitioner who is faced with examining the phenomenon of cyber warfare in light of the already existing national legislation.

Keywords: Civil Rights Framework. Internet. Cyber Warfare. Tallinn Manual

1. Introdução

Antes de tudo, este trabalho é fruto do laborioso projeto de contínuos estudos sobre Direito e Internet, mantido sob a emblemática liderança dos estimados professores Newton De Lucca e Adalberto Simão Filho, a quem agradeço, sensibilizado, pela nova oportunidade de colaborar com o terceiro volume da série dedicada ao tema. Ambos os mestres notabilizaram-se como precursores no estudo dos reflexos jurídicos da Internet, em solo brasileiro, e servem de exemplo a gerações de advogados, acadêmicos, magistrados e demais operadores de Direito que se devotam ao complexo estudo das relações que se estabelecem no mundo cibernético, sem dúvida uma das fronteiras da ciência jurídica no século XXI.

Visando a preparar o espírito do leitor que gentilmente se debruçará nas próximas linhas, esclareço que este trabalho destina-se a,brevemente, estabelecer um paralelo entre a regulação positiva estabelecida no Brasil pelo Marco Civil da Internet, editado sob a forma da Lei nº 12.965, de 23 de abril de 2014, e o percuciente estudo desenvolvido por alguns dos maiores especialistas do mundo dedicados ao Direito Internacional Público, que resultou na afirmação dos Princípios de Talin sobre o Direito Internacional Aplicável à Guerra Cibernética, consolidados na publicação de manual homônimo adotado pelo Centro de Excelência em Defesa Cibernética Cooperativa, da Organização para o Tratado do Atlântico Norte (*NATO Cooperative Cyber Defence Center ofExcellence – NATO/CCD/COE*), sediado na capital da República da Estônia.

Conforme teremos oportunidade de detalhar nos tópicos seguintes, o "Manual de Talin" não se traduz em norma internacional, per se, e nem é vinculante sequer para os países integrantes da OTAN sob cujos auspícios foi publicado, entretanto, ele representa a visão de alguns dos maiores especialistas da atualidade, acerca da aplicabilidade de normas já vigentes no Direito Internacional Público, sejam de natureza costumeira (e aplicáveis, portanto, a todas as nações), sejam de natureza convencional, vinculantes para os países que tenham aderido aos respectivos tratados, relativamente ao uso da internet como arma de guerra, ambiente de operações militares, ou alvo destas[1].

[1] Recentíssima repercussão jurídica de ação classificada como "guerra cibernética", foi a instauração de processo penal, pela Justiça Federal dos EUA, contra militares da República Popular da China, formalmente acusados de acessar, subtrair e danificar sistemas de informações militares estadunidenses. Vide: **EUA indiciam hackers militares chineses por espionagem: É a primeira vez que o governo americano processa judicialmente 'hackers estatais', que trabalham comandados pelo Exército da China**. São Paulo: Revista Veja, 19 mai. 2014. Disponível em: http://veja.abril.com.br/noticia/mundo/eua-vao-indiciar-hackers-militares-chineses-por-espionagem. Acesso: 19 ago. 2014.

Desnecessário frisar que, também o Brasil, por integrar o rol de nações que se pretende respeitador do Direito Internacional, terá que observar as prescrições deste ramo jurídico ao regular em seu território o uso da Internet, o que exigirá a adequação dos esforços interpretativos de seu novo Marco Civil com o restante do ordenamento jurídico aplicável.

Longe de se revestir de esboço com pretensões meramente acadêmicas, o estudo das regras aplicáveis à Guerra Cibernética constitui matéria de efetivas cogitações práticas, num cenário mundial em que se desenvolvem atividades classificáveis como Guerra Cibernética, que tanto se dirigem contra o Brasil, quanto se utilizam de pessoas e meios técnicos localizados em seu território.

Vale destacar, a esse respeito, notória e escandalosa violação da soberania brasileira, noticiada pela mídia nacional e internacional em período imediatamente anterior à promulgação do Marco Civil da Internet[2] (e que foi, em parte, um dos impulsos para a edição da nova Lei), a qual, por sua vez, gerou repercussões efetivas no Direito Internacional, decorrentes de pronunciamento formal da Assembleia-Geral das Nações Unidas, provocado por manifestação expressa da República Federativa do Brasil[3].

Outra fonte normativa brasileira considerada, no contexto da presente análise comparativa, é o Decreto nº 6.703, de 18 dez. 2008, que aprova a Estratégia Nacional de Defesa, documento oficial que baliza os esforços de defesa do Estado brasileiro, que estabelece como meta a ser perseguida pela sociedade e pelo Estado, dentre outras: "(...) *aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, que permitam seu pronto restabelecimento, a cargo da Casa Civil da Presidência da República, dos Ministérios da Defesa, das Comunicações e da Ciência e Tecnologia, e do GSI-PR; (...)*

Pois bem, definido o escopo de nossas considerações, passo a brevemente apresentar a estrutura do novo Marco Civil da Internet brasileira, na parte em que nos interessa

---

[2]BRASIL. Senado Federal. Relatório da Comissão Parlamentar de Inquérito composta por onze membros titulares e sete suplentes, com a finalidade de, no prazo de 180 dias, investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar emails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal. Brasília, DF, 09 abr. 2014. **Diário do Senado Federal**. Brasília, 17 abr. 2014. Suplemento "C".

[3]ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração do Terceiro Comitê da Assembléia-Geral das Nações Unidas: **Direito à Privacidade na Era Digital**. GA/SHC/4094. Nova York, 26 nov. 2013.

ao Estudo. Certamente, análises dogmáticas e principiológicas muito mais aprofundadas poderão ser localizadas nos demais artigos que compõem esta obra coletiva, às quais desde já me reporto.

Tomo apenas a liberdade, nessa exposição, de indicar as (poucas) fontes similares localizadas no Direito Comparado, objetivando realçar o caráter inovador da lei brasileira, que certamente será utilizada por operadores do Direito de outras nações, como fonte interpretativa e de consulta.

2. O Marco Civil da Internet brasileira

A norma a que se denomina Marco Civil da Internet brasileira foi positivada por meio da Lei nº 12.965, promulgada pela Presidenta da República em 23 de abril de 2014, data de sua publicação no Diário Oficial da União. É dotada, portanto, da força normativa de lei ordinária federal editada pela União no exercício de sua competência para legislar privativamente sobre Direito Civil, Comercial, Penal e Processual, bem como sobre informática, telecomunicações e radiodifusão, todas essas reservadas ao ente nacional pelo art. 22, I e IV, da Constituição Federal.

Cuida-se, assim, de verdadeira lei nacional[4] de observância vinculante por todas as esferas de governo (federal, estadual e municipal), pelos três poderes (executivo, legislativo e judiciário), bem como por todas as pessoas físicas e jurídicas em território nacional, independentemente de sua nacionalidade, observado o Princípio da Legalidade inscrito no art. 5º, II, da Constituição Federal.

Este introito, aparentemente óbvio para o meio jurídico, explica-se pela preexistência de inúmeras outras normas que, conquanto pretendessem regular diversos aspectos da internet, careciam justamente da força normativa atribuída no sistema brasileiro exclusivamente à lei, em sentido formal, limitando-se a gerar efeitos para a própria Administração Pública (Decretos, Instruções Normativas, Portarias, etc.), e, ainda assim, restritas às respectivas esferas de governo, ou de cada poder constituído.

Atento à multiplicação de questões jurídicas atinentes à internet, que deram ensejo às mais variadas tentativas de regulamentação no vácuo legislativo que se formara, o

[4] "*(...) a distinção entre leis nacionais e leis federais. Aquelas são relativas à atribuição legislativa da União como ente que congrega todas as pessoas políticas, estabelecendo normas a eles comuns (p. ex., direito penal, normas gerais tributárias). As leis federais referem-se à regulamentação de situações que envolvem exclusivamente a União, como pessoa pública equiparada às demais (v.g., estatuto de seus servidores, criação de imposto federal)".* PEREIRA, Helio do Valle. **Manual da Fazenda Pública em Juízo** – 2ª ed. Rio de Janeiro: Renovar, 2006.

Poder Executivo, através da Secretaria de Assuntos Legislativos do Ministério da Justiça (SAL/MJ), elaborou anteprojeto de lei que seria, posteriormente, remetido ao Congresso Nacional pela Presidência da República, na forma do Projeto de Lei nº 2.126/2011[5].

O pensamento do Executivo, àquela altura, pode ser identificado na Exposição de Motivos nº EMI 0086, de 25 de abril de 2011[6], subscrita em conjunto pelos então Ministros de Estado da Justiça; Comunicações; Ciência e Tecnologia; e Planejamento, Orçamento e Gestão, sintetizada nos parágrafos seguintes.

A Secretaria de Assuntos Legislativos do Ministério da Justiça - SAL/MJ, em parceria com o Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas do Rio de Janeiro, desenvolveu a iniciativa denominada Marco Civil da Internet no Brasil, a fim de construir, de forma colaborativa, um anteprojeto de lei que estabelecesse princípios, garantias e direitos dos usuários de Internet.

A proposta delimitava deveres e responsabilidades a serem exigidos dos prestadores de serviços e define o papel a ser exercido pelo poder público em relação ao desenvolvimento do potencial social da rede.

Com vistas ao diálogo entre normas jurídicas e a rede mundial de computadores, partiu-se de duas óbvias inspirações: o texto constitucional e o conjunto de recomendações apresentadas pelo Comitê Gestor da Internet no Brasil - CGI.br - no documento "Princípios para a governança e uso da Internet" (Resolução CGI.br/RES/2009/003/P). Uma discussão ampla foi realizada com a sociedade pela própria Internet, entre outubro de 2009 e maio de 2010, por meio de um blog hospedado na plataforma Cultura Digital (uma rede social mantida pelo Ministério da Cultura e pela Rede Nacional de Ensino e Pesquisa - RNP).

Resultado desse processo, o anteprojeto foi estruturado em cinco capítulos: disposições preliminares, direitos e garantias do usuário, provisão de conexão e de aplicações de Internet, atuação do poder público e disposições finais.

No primeiro capítulo foram indicados os fundamentos, princípios e objetivos do marco civil da internet, além da definição de conceitos e de regras de interpretação. Entre os fundamentos, enumerou-se elementos da casuística que serviram de pressupostos para a proposta. Entre os princípios figuraram os pontos norteadores que entendia o Governo deveriam sempre informar a aplicação do direito em relação à matéria. Já no âmbito dos objetivos,

---

[5] CONTRERA, Carla; ORTEGA, Dulcina. **O Comércio Eletrônico e o Código de Defesa do Consumidor**: Disciplina jurídica, aplicabilidade e evolução. Trabalho de Conclusão de Curso São Paulo: 2013, p. 29.

[6] BRASIL. Casa Civil da Presidência da República/Subchefia de Assuntos Parlamentares. Exposição de Motivos nº EMI Nº 00086 - MJ/MP/MCT/MC. Brasília: 25 abr. 2011.

apontou-se as finalidades a serem perseguidas de forma permanente, não apenas pelo Estado, mas por toda a sociedade.

No capítulo sobre os direitos e garantias do usuário, o acesso à internet seria reconhecido como um direito essencial ao exercício da cidadania. Foram apontados direitos específicos a serem observados, tais como a inviolabilidade e o sigilo das comunicações pela internet e a não suspensão da conexão.

No terceiro capítulo, ao tratar da provisão de conexão e de aplicações de internet, o anteprojeto buscou regulamentar legalmente, pela primeira vez, questões como: tráfego de dados, guarda de registros de conexão à Internet, guarda de registro de acesso a aplicações na rede, responsabilidade por danos decorrentes de conteúdo gerado por terceiros e requisição judicial de registros.

Privilegiou-se a responsabilização subjetiva, como forma de preservar as conquistas para a liberdade de expressão decorrentes da chamada Web 2.0, que se caracteriza pela ampla liberdade de produção de conteúdo pelos próprios usuários, sem a necessidade de aprovação prévia pelos intermediários. O anteprojeto pressupôs usos legítimos, protegendo a privacidade dos usuários e a liberdade de expressão, adotando como baliza o princípio da presunção de inocência, ao tratar abusos como eventos excepcionais.

No capítulo referente às atribuições do Poder Público, fixou diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da Internet no Brasil, além de regras para os sítios públicos, para a Educação, para o fomento cultural e para a avaliação constante do resultado das políticas públicas. Confere-se à Administração Pública um parâmetro para o melhor cumprimento dos objetivos do Marco Civil.

Finalmente, no último capítulo previu expressamente a possibilidade de que a defesa dos interesses e direitos pertinentes ao uso da Internet seja exercida de forma individual ou coletiva, na forma da Lei.

Naquele momento, o anteprojeto representou um primeiro passo no caminho legislativo, sob a premissa de que uma proposta legislativa transversal e convergente possibilitaria um posicionamento futuro mais adequado sobre outros importantes temas relacionados à internet que ainda carecem de harmonização, como a proteção de dados pessoais, o comércio eletrônico, os crimes cibernéticos, o direito autoral, a governança da internet e a regulação da atividade dos centros públicos de acesso à internet, entre outros.

Uma vez submetido ao Congresso, o Projeto de Lei do Executivo sofreu inúmeras propostas de emendas, culminando na apresentação de um substitutivo global

apresentado pelo relator do projeto[7], (deputado Alexandre Molon), a qual, finalmente, tornou-se o texto votado e aprovado pela Câmara dos Deputados. Chegando ao Senado Federal, o projeto aprovado pela Câmara sob o nº PLC 21/2014, foi aprovado sem alterações, após intenso trabalho do relator naquela casa (senador Ricardo Ferraço), seguindo para promulgação pela Presidência da República.

Uma vez aprovada a Lei, o Marco Civil da Internet foi apontado como referência mundial para as legislações que devem tratar da rede mundial dos computadores, durante o NetMundial – Encontro Multissetorial Global Sobre o Futuro da Governança da Internet, que reuniu governos, empresas, especialistas e ativistas em discussões sobre o futuro da rede[8].

Os princípios da lei – especialmente a garantia da neutralidade de rede, da liberdade de expressão e da privacidade dos usuários – foram estabelecidos para manter o caráter aberto da internet[9].

A neutralidade de rede prevê que o tráfego de qualquer dado deve ser feito com a mesma qualidade e velocidade, sem discriminação, sejam dados, vídeos, etc. Se essa neutralidade não fosse garantida, a internet poderia funcionar como uma TV a cabo: os cidadãos pagariam determinado valor para acessar redes sociais e outro para acessar redes e vídeos, por exemplo.

Outro princípio é a garantia da liberdade de expressão, em virtude do que o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as

---

[7]Em consequência, ficaram prejudicados a proposição inicial; as Emendas apresentadas; o Substitutivo apresentado pelo Relator da Comissão Especial; e os Projetos de Lei nºs 3.016/00, 3.303/00, 3.891/00, 4.972/01, 5.403/01, 5.977/01, 6.557/02, 7.461/02, 18/03, 480/03, 1.256/03, 2.196/03, 3.301/04, 4.144/04, 4.562/04, 5.009/05, 169/07, 2.957/08, 4.424/08, 5.185/09, 5.298/09, 6.357/09, 6.527/09, 7.131/10, 7.270/10, 7.311/10, 642/11, 1.172/11,1.468/11, 1.880/11, 1.961/11, 2.552/11, 2.690/11, 3.033/11, 3.095/12, 3.124/12, 3.175/12, 3.761/12, 4.565/12, 4.666/12, 5.475/13 e 6.375/13, apensados. Disponível em http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255, acesso: 10 set. 2014.

[8] MARTINS, Helena. **Entenda os três princípios do Marco Civil da Internet**. Disponível em: http://www.jcnet.com.br/Geral/2014/04/entenda-os-tres-principios-do-marco-civil-da-internet.html, acesso 11 set. 2014.

[9]"***Os princípios da disciplina do uso da internet no Brasil estão indicados no artigo 3o da nova lei. O primeiro deles é a "garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal***" *(inciso I). A referência ao texto constitucional seria desnecessária, porque óbvia a conformação desses princípios ao quanto disposto nos artigos 5o, inciso IX, e 220 da Constituição, continente do que a doutrina alemã denomina genericamente de liberdades comunicativas. Independentemente do caráter expletivo desse inciso, é compreensível que o legislador haja pretendido enfatizar seu compromisso com a proteção dos conteúdos jurídicos ali enunciados.* ***Os incisos II e III também formulam princípios constitucionais, ainda que em linguagem um tanto diversa, como o da "proteção da privacidade" e da "proteção dos dados pessoais, na forma da lei".*** *A conexão com o artigo 5o, incisos X (inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas) e XII (inviolabilidade do sigilo de dados) é também facilmente assimilável*. RODRIGUES JUNIOR, Otávio Luiz. **Liberdades comunicativas e privacidade no Marco Civil**. Disponível em: http://www.conjur.com.br/2014-mai-07/direito-comparado-liberdades-comunicativa-vida-privada-marco-civil, acesso: 11 set. 2014.

providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

O marco também garante a privacidade dos usuários da internet, ao estabelecer que informações pessoais e registros de acesso só poderão ser vendidos se o usuário autorizar expressamente a operação comercial. Tornou-se, desse modo, ilegal o uso de dados pessoais por grandes empresas para obter mais receitas publicitárias, privilegiadas pelo acesso a detalhes sobre as preferências e opções dos internautas[10].

Além dos princípios da internet no Brasil, outros direitos foram consagrados pela "Constituição da Internet", como passou a ser chamada a regra. A inviolabilidade da intimidade e da vida privada e indenização em caso de violação; a não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização; a manutenção da qualidade contratada da conexão à internet são alguns dos direitos dos usuários.

Os internautas deverão, ainda de acordo com a lei, ter informações claras e completas sobre os contratos de prestação de serviços e coleta, uso, armazenamento, tratamento e proteção de dados pessoais[11], bem como ter garantida a acessibilidade, levando em conta as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário.

Além desses três princípios apontados por toda a (recente) doutrina que se dispõe a comentar as inovações do Marco Civil da Internet, outro princípio, cuja conjugação com as normas sobre Guerra Cibernética pode trazer especial dificuldade, é a denominada "Inimputabilidade da Rede".

Segundo este princípio, que teria sido estabelecido pelo art. 15, da Lei nº 12.965/2014, o combate a ilícitos perpetrados por intermédio da rede deve atingir especificamente os responsáveis finais, aqueles que, de fato, cometeram um crime, e não

---

[10] "*A exclusão digital, em seu aspecto positivo, percorre os mesmos embates e lutas enfrentados pela inclusão. Aliás, o direito à exclusão digital é interligado à inclusão digital. É um modo de se utilizar da inclusão digital, para que, dentro dela ou ao mesmo tempo que ela, o ser humano possa exercitar o direito à exclusão digital.* ***A exclusão digital é um direito que funciona conjuntamente aos direitos à privacidade, à intimidade, à vida privada e neles se complementa, completa e funciona.*** *Pode-se afirmar que o direito à exclusão digital é a tática dos seres humanos à implementação destes direitos . É a exclusão digital atuando estruturalmente na formação dos discursos, saberes e poderes que, na sociedade tecnológica, se formam sem o consentimento do usuário. Neste sentido, a exclusão digital, positivamente, implementa a dignidade da pessoa humana ao trazer o empoderamento para o sujeito decidir por querer ou não ser incluído*." GONÇALVES, Victor Hugo Pereira. **Direito Fundamental à Exclusão Digital**. Disponível em: https://www.academia.edu/4783856/Exclusao_Digital_como_Direito_Fundamental, acesso: 12 set. 2014.

[11] DE LUCCA, Newton. **Contratación Informática y Telemática**. Bogotá: Javeriana, 2012, p. 6.

aqueles que operam os meios utilizados para o funcionamento da rede, isto é, em última análise, as empresas que proveem a infraestrutura, e os seus administradores e técnicos[12].

Para o Comitê Gestor da Internet no Brasil (CGI.br)[13], a positivação do princípio da inimputabilidade da rede é essencial porque: i) promove transparência e confiança no uso da Internet e nas atividades de provimento da própria Internet; ii) estabelece princípios básicos e garante a aplicação do devido processo legal, quando necessário; coíbe acordos privados para o combate a ilícitos, suscetíveis a critérios arbitrários e suspeitos; iii) assegura a liberdade de expressão e a privacidade, ao mesmo tempo em que coíbe abusos; iv) preserva o livre fluxo de comunicações globais; e v) preserva a estrutura da rede mundial, responsabilizando aqueles que utilizam seus recursos indevidamente, e não a cadeia que suporta o funcionamento da Internet, em si.

Trata-se de verdadeira garantia instrumental, que pretende resguardar a própria existência do "espaço virtual", tornado efetivo pelo trabalho ininterrupto de milhares de empresas e profissionais[14], cuja eventual responsabilização decorrente do abuso por terceiros,

---

[12] O CGI.br e o Marco Civil da Internet: **Defesa da privacidade de todos que utilizam a Internet**; Neutralidade da rede; Inimputabilidade da rede. Disponível em: https://pimentalab.milharal.org/files/2013/09/CGI-e-o-Marco-Civil.pdf, acesso 12 set. 2014.

[13]Sobre a natureza jurídica do Comitê Gestor da Internet no Brasil, didática explanação retirada da jurisprudência do Tribunal Regional Federal da 3ª Região: *"(...) o Comitê Gestor da Internet no Brasil - CGI.br é composto por membros do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica. Foi criado pela Portaria Interministerial MC/MCT nº 147/95, posteriormente ratificada e alterada pelo Decreto Presidencial nº 4.829/2003. Dentre as atribuições, estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil; estabelecer diretrizes para a organização das relações entre o Governo e a sociedade na execução do registro de Nomes de Domínio, na alocação de Endereço IP (Internet Protocol) e na administração pertinente ao Domínio de Primeiro Nível (ccTLD - country codeTopelLevel Domain), .br, no interesse do desenvolvimento da Internet no País (artigo 1º, incisos I e II, fl. 137). Até dezembro de 2005, o registro de nomes de domínio, sob o sufixo .br, era realizado pela equipe de voluntários ligados à rede acadêmica e sediados na FAPESP (Resolução CGI.br nº 002/98). Com o crescimento do número de registros e dos recursos deles decorrentes, optou-se pela constituição de uma entidade jurídica apta a assumir as funções técnicas historicamente executadas pelo grupo de pesquisadores da FAPESP. Veja-se, ainda, os esclarecimentos de fls. 154 verso/155: Por conta disso, foi criado o NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR - NIC.br. Esta, a entidade da qual o Comitê gestor da Internet no Brasil - CGI.br passou a se valer, em substituição à FAPESP, para cumprir as atribuições descritas na Portaria Interministerial MC/MCT nº 147/95, confirmadas e alargadas pelo Decreto 4.829, de 3 de setembro de 2003.* ***Vale ressaltar que o Comitê Gestor da Internet no Brasil - CGI.br não é órgão integrante da administração pública, posto que a Portaria Interministerial MC/MCT nº 147/95 e o Decreto Presidencial nº 4.829, de 03 de setembro de 2003, que o criou, apenas formou a união de membros dos Ministérios de Estado, representantes da sociedade civil e de áreas ligadas à Internet, visando estabelecer diretrizes relacionadas ao uso e desenvolvimento da Internet no Brasil. A criação de qualquer comitê com base no artigo 84, inciso VI, alínea a, da Carta Magna não o qualifica como unidade do Poder Público, transformando-se em órgão público****. Assim, com fundamento no artigo 10 do Decreto nº 4.829/2003, que permite seja atribuída à entidade privada sem fins lucrativos a execução do registro de nomes de domínio, dentre outras atividades, o Comitê Gestor da Internet no Brasil procedeu à delegação por meio da Resolução nº 001/05 (...)"* (3ª Vara Cível Federal de São Paulo. Processo nº 0005316-22.2011.4.03.6100. j. 30 set. 2011).

[14] "*Este ciberespaço é autônomo, no sentido de que funciona segundo as regras de um sistema autorreferenciado, conforme assinalamos. É pós-orgânico, já que não está formado por átomos, nem segue as regras de funcionamento e localização do mundo orgânico: trata-se de bits. Tem uma natureza não territorial e comunicativa, um espaço-movimento, no qual tudo muda a respeito de tudo, isto é, o "espaço virtual" não é*

pressupõe a lei, colocaria em risco esta conquista da humanidade no Século XXI, que é a rede mundial de computadores.

A título comparativo, pode ser mencionada a legislação russa sobre a matéria, aprovada na forma de Lei Federal nº 149-FZ, de 27 jul. 2006, alterada pelas Leis Federais números 139-FZ, de 28 jul. 2012, e 398-FZ, de 28 dez. 2013, aprovada pelo Parlamento ("Duma"), e pelo Conselho da Federação Russa, sob o nomen juris de "*Lei sobre a Informação, Tecnologias da Informação, e Proteção da Informação e sobre os Procedimentos para Estabelecer, Bloquear, Desenvolver e Manter o Sistema Uniforme Automatizado de Lista Negra da Internet Russa*"

O diploma russo, contrariamente ao que estabeleceu a legislação brasileira, expressamente consignou como princípios da internet a serem observados no território daquele país: i) o controle e supervisão do tráfego de internet por parte de autoridades reguladoras (no caso, a Agência de Imprensa e das Comunicações de Massa da Federação Russa - *Федеральноеагентствопопечати и массовымкоммуникациям России*); ii) a possibilidade de supressão do conteúdo considerado impróprio mediante notificação da autoridade reguladora (e não do Poder Judiciário); iii) identificação do provedor de serviço e do responsável pelo conteúdo impróprio; iv) registro e armazenamento de informações sobre os dados considerados impróprios, de seus autores e dos provedores de serviço utilizados; e v) responsabilidade solidária do provedor do serviço, pelo compartilhamento de conteúdos impróprios.

Critica publicada à época pelo Conselho para o Desenvolvimento das Instituições da Sociedade Civil e dos Direitos Humanos chamou atenção para os principais problemas da legislação russa, sintetizados em alguns pontos. Para o Conselho, a criação do registro (a "lista negra") do conteúdo proibido para a Internet, e a introdução de procedimentos para o bloqueio de recursos da Internet, introduziu uma lista de recursos a ser bloqueado é muito ampla e incluiu, além da pornografia infantil, uma série de categorias de avaliação subjetiva.

Um bloqueio generalizado de nomes de domínio e endereços IP (em vez de bloqueios pontuais sobre os sinais universais de páginas da Web URL) poderia resultar no fechamento em massa de recursos de boa-fé também hospedados nos mesmo domínios e endereços de rede. Adicionalmente, devido ao fato de que o sistema de filtragem ter que ler todos os materiais que são passados em web-protocolos, incluindo criptografados, aumenta a

---

sequer assemelhado ao espaço real, porque não está fixo, não se pode localizar mediante provas empíricas, como, por exemplo, o tato." LORENZETTI, Ricardo Luis. **Comércio eletrônico**. Trad. Fabiano Menke. São Paulo: RT, 2004, p. 13.

probabilidade de acesso não autorizado a dados confidenciais do governo e os dados pessoais dos usuários russos a Internet.

Ademais, a introdução de filtragem nos principais provedores, implicou diminuição geral da taxa de tráfego de Internet na Rússia, pondo em risco a estabilidade do sistema, e impondo consequências extremamente negativas para o desenvolvimento do *e-commerce* e transações *online* (incluindo pagamentos eletrônicos e *internet banking*). De acordo com o Center for New Media, Nova Escola de Economia, haveria uma relação direta entre o desempenho econômico e a velocidade de transmissão de dados na Internet, de tal modo que uma diminuição da taxa da rede em 20% (o esperado declínio com a introdução de filtragem), resultaria num declínio estimadode até 5% do PIB nacional.

Finalmente, estimou-se que a lei imporia um ônus financeiro para a implementação do bloqueio, que seria muito elevado para os jogadores menores no mercado. De acordo com os cálculos dos operadores, o custo do equipamento adicional poderia chegar a até 10 bilhões de rublos, que seriam repassados para os usuários, afetandonegativamente a quantidade deconsumidores russos.

Mesmo diante dessa grande quantidade de críticas, especificamente dirigidas ao modelo russo, não se pode dizer que este seja uma exceção. Pelo contrário, em muito se assemelha ao marco regulatório estabelecido na Turquia pela Lei nº 6.518, de 06 fev. 2014[15].

Tal legislação permite à Autoridade de Telecomunicações da Turquia (*Telekomünikasyon İletişim Başkanlığı*– TIB), o bloqueio de páginas da internet sem prévia ordem judicial, caso lhe seja apresentada uma reclamação por desrespeito à privacidade das pessoas. Uma vez apresentada a reclamação, o ente regulador pode ordenar ao provedor de serviços o bloqueio da URL, que deverá cumprir a determinação em até quatro horas. Uma vez efetuado o bloqueio, o interessado deve buscar uma ordem judicial, mas a página permanecerá fora do ar até que seja julgado o processo.

A autoridade reguladora pode, ainda, determinar o bloqueio *ex officio*, quando entender que os potenciais ofendidos sejam hipossuficientes, ou que a demora no bloqueio possa gerar conseqüências irreversíveis. Os provedores são obrigados a armazenar todos os dados relativos às suas atividades de hospedagem por até dois anos, e torna-los disponíveis à

[15] Altera a Lei nº 5.651/2007, que dispõe sobre o Regulamento de Publicações na Internet e o Combate aos Crimes Cometidos por Intermédio dessas Publicações. Mencionada lei, antes mesmo das alterações que a tornaram mais rígidas, já havia sido considerada abusiva pela Corte Europeia de Direitos Humanos (CEDH), em dezembro de 2012, no julgamento do caso Ahmet Yildirim v. Turquia. A CEDH considerou violado o artigo 10 da Convenção Europeia de Direitos Humanos.

autoridade reguladora quando solicitados, bem como a atender quaisquer medidas solicitadas pela TIB[16].

Como se vê, a tendência mais recente dos ordenamentos jurídicos de países possuidores de quadros político-social muito similar ao brasileiro tem apontado para marcos regulatórios da Internet informados por valores bastante distintos da legislação brasileira, o que, se pode servir de alívio ao operador do Direito nacional, deve ser visto como indicativo de risco a ser avaliado em eventuais propostas de alteração do Marco Civil da Internet.

Feitas essas breves remissões aos conceitos básicos introduzidos no ordenamento jurídico brasileiro pelo Marco Civil da Internet, passamos a analisar os Princípios de Talin, objeto principal de nosso trabalho.

3. Manual de Talin sobre o Direito Internacional Aplicável à Guerra Cibernética

Em 2009, o Centro de Excelência em Defesa Cibernética Cooperativa, da Organização para o Tratado do Atlântico Norte, organização militar internacional sediada em Talin, capital da Estônia, convidou um grupo independente de especialistas para discutir o fenômeno e produzir um manual sobre o Direito aplicável à guerra cibernética. Seguia, com isto, caminho que já fora trilhado anteriormente quando da elaboração do Manual de San Remo Aplicável aos Conflitos Armados no Mar, pelo Instituto Internacional de Direito Humanitário; e do Manual sobre o Direito Internacional Aplicável à Guerra Aérea e de Mísseis, sob os auspícios do Programa de Pesquisa sobre Conflitos e Política Humanitária, da Universidade de Harvard[17].

Operações militares cibernéticas começaram a chamar a atenção da comunidade jurídica internacional a partir do fim da década de 90 do Século XX, mas a primeira onda reconhecida de "hackativismo" maciço contra um Estado foi detectada em 2007, contra a Estônia, e 2008, contra a Geórgia, "coincidentemente" quando esses países entraram em conflito direto ou indireto com a Federação Russa. Outro episódio internacionalmente

---

[16] Library of the Congress. **Turkey: Law on Internet Publications Amended**. Disponível em: http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403875_text , acesso 12 set. 2014.

[17] SCHMITT, Michael N. **Tallin Manual on the International Law Applicable to Cyber Warfare**: Prepared by the International Group of Experts at the Invitation of the Nato Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press, 2013.

reconhecido como uso militar de ferramentas da internet foi o ataque ao projeto nuclear iraniano, mediante utilização do vírus *Stuxnet*, em 2010.

Esses e outros eventos levaram Estados a dedicarem maior atenção ao mundo virtual, concebendo-o efetivamente como espaço de operações militares. No mesmo ano de 2010 o Reino Unido inseriu um tópico sobre segurança cibernética em sua Estratégia de Segurança Nacional[18]; o Canadá lançou sua Estratégia de Segurança Cibernética[19], e a Rússia publicou sua Visão Conceitual sobre Atividades das Forças Armadas da Federação Russa no Espaço Informacional[20].

Seguindo a tendência, e ainda com maior ênfase, os EUA incluíram em sua Estratégia de Segurança Nacional, de 2010, menção preocupante sobre graves riscos decorrentes de ataques de natureza cibernética, logo seguida pela ativação de uma nova grande unidade do Comando Estratégico dos Estados Unidos (*USSTRACOM*): O Comando Cibernético dos Estados Unidos (*USCYBERCOM*).

No Brasil, a Estratégia Nacional de Defesa, de 2008, já apontava como um de seus eixos prioritários o reforço à área cibernética, posteriormente consolidada na publicação do Livro Branco de Defesa Nacional[21], que alocou a missão principal deste segmento ao Exército Brasileiro, sem desconsiderar, contudo, as especificidades e capacidades próprias das demais Forças Armadas. Seguiu-se ao aparato normativo a ativação do primeiro Centro de Defesa Cibernética (CDCiber), do Comando do Exército, sediado em Brasília, com jurisdição sobre todo o território nacional[22].

Um dos principais desafios enfrentados pelos Estados no ambiente cibernético é a definição sobre o escopo de aplicabilidade do Direito Internacional às operações cibernéticas, sejam ofensivas ou defensivas, já que, ao tempo em que foram produzidos os principais textos legais internacionais, sobre normas costumeiras ou convencionais, a tecnologia cibernética nem sequer se punha no horizonte[23].

---

[18] HM Government. **A Strong Britain in na Age of Uncertainty**: The National Security Strategy 11 (2010).
[19] Government of Canada. **Canada's Cyber Security Strategy** (Outubro de 2010).
[20] Ministério da Defesa da Federação Russa. **Russian Federation Armed Forces' Information Space Activities Concept**. Disponível em: < http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle>, acesso: 12 set. 2014.
[21] BRASIL. **Livro Branco de Defesa Nacional**. Ministério da Defesa: Brasília, 2012, p. 69.
[22] BRASIL. Portaria nº 666, de 04 ago. 2010 – Cria o Centro de Defesa Cibernética do Exército. Ministério da Defesa/Comando do Exército: Brasília, **Boletim do Exército nº 31**, de 06 ago. 2010.
[23] "*Bearing in mind that international law is an inter-state legal system in which there is no central govenrment, only those rules that are accepted by States can be part of international law. The same, to a certain extent, can hold true for certain rules that are not strictly, or originally, based on State consent, but which are inherent in the very nature of international law as a legal system. Such a factor of inherency is essentially different form the desirability or social acceptability of the relevant rule. It is one thing to say that the rule must be seen as part of international law because it is indispensable to its structural underpinnings. It is another thing to argue that a*

No limite, questiona-se mesmo se existe alguma aplicabilidade do Direito vigente às questões cibernéticas. Opiniões dissonantes sobre o tema vão desde a aplicação integral do marco regulatório internacional sobre conflitos armados, sob o enfoque generalista de precedentes da Corte Internacional de Justiça, até o da não-aplicabilidade completa, seguindo antigo postulado da extinta Corte Permanente de Justiça Internacional, segundo o qual atos que não sejam expressamente proibidos pelo Direito Internacional estejam genericamente permitidos.

Neste contexto de incertezas, o Manual de Talin procurou examinar o Direito Internacional aplicável tanto ao *jus ad bellum* – isto é, o "Direito à Guerra", tal como compreendido no século XXI; quanto *ao jus in bello*, que regula os meios e métodos de combate internacionalmente aceitáveis, uma vez iniciadas as hostilidades.

O Manual de Talin parte de um enfoque especificamente dedicado à "Guerra Cibernética", com ênfase nas operações puramente cibernéticas, ou seja, não se debruça, senão incidentalmente, sobre o que se convencionou chamar "Operações Cinéticas", caracterizadas como operações militares no mundo físico ("real"), dirigidas contra instalações civis ou militares das quais dependa o funcionamento da rede, essenciais à sua infraestrutura[24].

Não é um manual sobre segurança cibernética, inerente ao dia-a-dia do funcionamento de particulares, assim como de empresas e entidades públicas, e nem se dirige, propriamente, a estudar os casos de "Ciber-Espionagem", levadas a efeito cotidianamente por agências de inteligência civis e militares, exceto quando estas possam ser de tal vulto ou gravidade, a ponto de já se enquadrarem no conceito de "uso da força", regulado pelo Direito Internacional sob o paradigma do *jus ad bellum*.

O Manual analisa, por fim, tanto os conflitos armados internacionais quanto, acompanhando, neste ponto, as definições clássicas do Direito Internacional dos Conflitos Armados.

3.1 – Afirmação da Aplicabilidade do Direito Internacional Costumeiro e Convencional à Guerra Cibernética

certain substantive regulation is part of international law because it is a desirable or sound regulation, even though State consent does not support it." ORAKHELASHVILI, Alexander. **The Interpretation of Acts and Rules in Public International Law**. Oxford: Oxford University Press, 2008, p. 60.

[24] SCHMITT, Michael N. Op. Cit.

No item precedente mencionamos que uma das primeiras especulações do Grupo de Especialistas que se reuniu em Talin, dizia respeito à própria aplicabilidade de um conjunto de regras jurídicas consagradas muito antes da criação da Internet, ao conceito de "Guerra Cibernética"[25].

Sinteticamente, concluiu o Manual de Talin que também essa nova modalidade de conflito armado está regulada pelo Direito Internacional, e, para tanto, cunharam a expressão "Direito Internacional da Segurança Cibernética" (*International Cyber Security Law*), fundamentada nos argumentos que se seguem, já articulados na forma de Princípios[26].

Tendo em mente a limitação de espaço inerente ao escopo deste trabalho, procurar-se-á articular as proposições principiológicas dos Manual de Talin com aquelas anteriormente detalhadas para o Marco Civil da Internet brasileira, à medida em que surjam os postulados respectivos.

3.1.1 – Soberania – Um Estado pode exercer o controle sobre infraestrutura e as atividades cibernéticas no interior de seu território soberano.

Já de início encontramos proposição que pode contrariar (ao menos parcialmente), valores e conceitos adotados pelo Marco Civil da Internet brasileira. Com efeito, o art. 2º, I, da Lei nº 12.965/2014, ao afirmar que a disciplina do uso da Internet no Brasil parte do pressuposto de sua escala mundial, pode ser interpretado como uma restrição genérica ao controle do Estado sobre as atividades cibernéticas em seu território[27].

Enquanto isso, segundo o Grupo de Especialistas em Direito Internacional, conquanto nenhum Estado possa reivindicar soberania sobre o ciberespaço, *per se*, os Estados podem exercer prerrogativas de soberania a respeito de qualquer porção da infraestrutura

---

[25] Interessante notar que, apesar das críticas dirigidas à legislação da Federação Russa, sobre regulação da Internet, o texto básico que especifica a doutrina de guerra cibernética naquele país, referida em passagem anterior, ao contrário das normas similares de outros países, que em geral silenciam sobre o tema, faz consignar expressamente em seu item 2.1 que as operações no espaço informacional serão desenvolvidas com aderência ao Princípio da Legalidade, decorrentes das leis do país, bem como das normas de Direito Internacional aplicáveis, com destaque para aquelas deduzidas da Carta das Nações Unidas e do Direito Internacional Humanitário.

[26] "*Os princípios do Direito Internacional estão consagrados em vários documentos produzidos internacionalmente, que foram resultado do amadurecimento da sociedade internacional, a partir de suas experiências, ainda que essa individualização não permita obter uma visão simplista, ou mesmo uma perspectiva estanque e isolada sobre o tema*." MENEZES, Wagner. **Os Princípios no Direito Internacional** *in* CASELLA, Paulo Borba; RAMOS, André de Carvalho (org.). **Direito Internacional**: Homenagem a Adherbal Meira Mattos. São Paulo, Quartier Latin, , 2009, p. 696.

[27] Art. 2o A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como: I - **o reconhecimento da escala mundial da rede**; (...)

cibernética que se localize fisicamente em seu território, bem como sobre as atividades associadas àquela infraestrutura[28].

Esta assertiva é dedutível do precedente firmado pela Corte Permanente de Justiça Internacional no laudo arbitral sobre a Ilha de Palmas, de 1928[29]. Neste precedente clássico, que reconheceu o Direito Internacional Costumeiro vigente, definiu-se que a soberania na relação entre os Estados significa independência. Independência em relação a determinada porção do globo terrestre é o direito de exercer nela, com exclusão de qualquer outro Estado, as funções de governo.

Soberania implica que o Estado possa controlar toda a infra-estrutura as atividades cibernéticas que se desenvolvam na porção terrestre de seu território, em suas águas interiores, no mar territorial (incluído o leito oceânico e seu subsolo), arquipélagos e no espaço aéreo subjacente. Conseqüência da soberania do Estado sobre a infraestrutura cibernética é que esta deve submeter-se ao controle legislativo e regulamentar do Estado, mas também que compete ao Estado a proteção desta infraestrutura, seja ela de propriedade privada ou pública.

Desse modo, para o Direito Internacional, uma operação cibernética que seja lançada de seu território contra a infra-estrutura cibernética localizada no território de outro Estado pode ser considerada uma violação da soberania deste, induzindo responsabilidade internacional. Se tais operações tiverem por objetivo coagir um determinado governo, estas incidirão na proibição geral de "intervenção nos negócios internos de um país", ou ao "uso da força", prevista pela Carta das Nações Unidas, apta a provocar represálias ou contramedidas, bem como ao acionamento do Conselho de Segurança das Nações Unidas.

No contexto cibernético, o princípio da soberania permite que um Estado restrinja ou proteja, no todo ou em parte, o acesso à Internet, sem prejuízo das demais normas de Direito Internacional e Direitos Humanos aplicáveis. O simples fato de que a infra-estrutura cibernética de um Estado se conecte com redes globais de telecomunicações, não serve para afastar os direitos de soberania sobre aquela infra-estrutura.

Da mesma forma, a soberania exercida por um Estado sobre o leito de seu mar territorial outorga-lhe total controle sobre a colocação de cabos submarinos, o que representa um fator crucial de controle, na medida em que a porção mais maciça de dados da Internet

---

[28] SCHMITT, Michael N. Op. Cit.

[29] "*Sovereignty in the relation between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State. The development of the national organisation of States during the last few centuries and, as a corollary, the development of international law, have established this principle of the exclusive competence of the State in regard to its own territory in such a way as to make it the point of departure in settling most questions that concern international relations*." Scott, Hague Court Reports 2d 83 (1932) (Perm. Ct. 4rb. 1928), 2 U.N. Rep. Intl. 4rb. Awards 829.

atualmente seja suportada por cabos submarinos. Em relação aos cabos submarinos que se estendam além do mar territorial, o art. 79 da Convenção sobre o Direito do Mar limita os direitos de interferência de um Estado aos cabos submarinos depositados sobre a sua plataforma continental.

Este princípio, consolidado pelo Manual de Talin pode parecer, num primeiro momento, contrário também aos postulados de neutralidade e inimputabilidade da rede, consagrados pelos artigos 3º e 15, do Marco Civil da Internet brasileira, mas, num segundo exame, podemos perceber que o legislador brasileiro não se exonerou de toda e qualquer autoridade sobre a rede, e sua infraestrutura, dispondo inclusive sobre medidas governamentais destinadas à proteção e desenvolvimento da rede, que pressupõem a asserção de sua soberania, nos exatos moldes acima expostos.

Enfrentando a tensão aparente entre o conceito tradicional de soberania – adotado pelo Manual – e os novos paradigmas postos pelo ciberespaço, a célebre cientista política Saskia Sassen ensina que, embora a idéia da Internet como rede de redes descentralizada tenha contribuído para a noção de sua autonomia intrínseca com relação ao poder estatal, o núcleo da Internet está conformado por uma série de elementos de infraestrutura: os pontos de interconexão (IXP), os *backbones* ou troncos nacionais, as redes regionais e as redes locais, que, em geral, se encontram sob a propriedade de entidades privadas, de tal modo que seu grau de abertura e sua tecnologia contém em si elementos com potencial de controle indireto[30].

3.1.2 – Jurisdição – Sem prejuízo das obrigações internacionais aplicáveis, um Estado pode exercer sua jurisdição: a) sobre pessoas envolvidas em atividades cibernéticas no seu território; b) sobre a infra-estrutura cibernética localizada em seu território; e c) extraterritorialmente, de acordo com o Direito Internacional

[30] "*Por un lado, se encuentra un conjunto de ideas generalizadas, con su origen en las primeras etapas de Internet, que conciben a la red como un espacio descentralizado en el que no se puede instituir ninguna estrutura de autoridad. Por otro lado, hay un corpus creciente de textos técnicos, estimulado en gran parte por el aumento de la importancia de las cuestiones relativas a las direcciones web y a la vigilancia de la actividad en la red, con las correspondientes problemáticas jurídicas y políticas asociadas con este fenómeno*." SASSEN, Saskia. **Territorio, autoridad y derechos**: de los ensemblajes medievales a los ensenblajes globales. Buenos Aires: Katz Editores, 2013, p. 414.

Diretamente decorrente do conceito de soberania, surge o de jurisdição, entendido como a prerrogativa do Estado de prescrever normas jurídicas, aplicá-las, e adjudicar situações em que estas sejam violadas.

A principal base para o exercício da jurisdição pelo Estado é a presença física de uma pessoa (*in personam*), ou de uma coisa (*in rem*), no interior de seu território. Por este pressuposto, o Estado pode legislar e fazer cumprir leis sobre as atividades cibernéticas de indivíduos em seu território. Pode ainda regular o funcionamento de empresas privadas inscritas em seus registros de comércio, ainda que fisicamente instaladas em outros territórios (por exemplo, provedores de internet – ISP), bem como regulamentar a construção e instalação de elementos da infra-estrutura da Internet nos espaços em que exerça soberania.

A jurisdição baseada na territorialidade leva em consideração que, apesar de utilizarem sistemas interconectados por "nuvens" ou "grades" baseados além de suas fronteiras, os indivíduos têm que se valer de algum equipamento, e estar fisicamente presentes em algum local, de tal forma que qualquer Estado de onde um indivíduo tenha operado os equipamentos que acessam a Internet, desfrutam de jurisdição sobre os atos ali perpetrados.

Ainda considerando o aspecto territorial da jurisdição, esta pode ter natureza subjetiva – atos perpetrados a partir de seu território, mas sem conseqüências nele –, ou objetiva – atos iniciados em outro local, mas que gerem efeitos num determinado território.

Os artigos 22 e 23 do Marco Civil da Internet brasileira atribuem ao Poder Judiciário competências para determinar a guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de Internet, para fins de instrução probatória, civil ou criminal, inclusive a pedido das autoridades policiais ou do Ministério Público (art. 13, § 2º), mas não o faz com o propósito de garantir a própria existência da rede, ou de diminuir ou prevenir danos causados pelo uso abusivo da rede.

Eventual pedido com esta finalidade teria que se basear, genericamente, na disposição principiologia estabelecida pelo art. 3º, V, da mesma Lei. É desnecessário frisar, contudo, que o tempo e a burocracia naturalmente associados à tramitação judicial de qualquer feito no Brasil (em autos físicos e no horário do expediente), dificilmente permitirão prevenir ou mesmo neutralizar graves atividades ilícitas detectadas na rede, o que, na prática, imporia uma inaceitável omissão do aparato de defesa em caso de ataque cibernético contra o Brasil, ou direcionado contra outro país a partir do território brasileiro, ou, de outro lado, cobriria sob o manto da ilegalidade iniciativas constitucionais de defesa do Estado, quiçá resguardadas somente por uma residual causa extralegal de exclusão da ilicitude: a inexigibilidade de conduta diversa.

Para o Direito Internacional, em ambos os casos haverá hipótese de jurisdição sobre os indivíduos que conduziram as operações, sendo até mais comuns os casos de jurisdição objetiva, uma vez que as operações de "Guerra Cibernética", em geral, produzirão resultados num Estado-Alvo, que deterá o interesse em responsabilizar os autores do ataque.

No aspecto extraterritorial, são consagrados, inclusive pelo Direito brasileiro[31], os princípios da personalidade ativa (leva em conta a nacionalidade do autor); da personalidade passiva (leva em conta a nacionalidade da vítima); da proteção (toma em consideração a defesa da segurança nacional do Estado atingido); e, finalmente, da jurisdição universal (violações a normas cogentes de Direito Internacional, como Crimes de Guerra).

Observe-se, finalmente, que o destaque dado para as obrigações decorrentes do Direito Internacional se referem, no Manual, ao reconhecimento de circunstâncias que afastam a jurisdição de um Estado, como a proteção ao pessoal e instalações diplomáticas, e o estatuto do combatente, que preserva os militares regularmente engajados por seus países em combate, do processo e julgamento pelas missões que venham a cumprir[32].

3.1.3 – Responsabilidade pelo Controle da Infraestrutura Cibernética – Um Estado não pode conscientemente permitir que a infraestrutura cibernética localizada em seu território seja usada para causar danos ou afetar ilegalmente outros Estados

Quiçá o princípio mais complexo cristalizado pelo Manual de Talin, este postulado estabelece um standard internacional, segundo o qual deve o Estado velar pelo controle, seja de qualquer infraestrutura cibernética (publica ou privada), localizada em seu território; seja de qualquer infraestrutura fática ou juridicamente sob sua jurisdição, de forma a impedir que estas sejam empregadas para causar danos a pessoas ou ao patrimônio situado no território de outros países.

Esta opinião do Grupo de Especialistas baseia-se em dois precedentes essenciais da Corte Internacional de Justiça a qual, declarando o Direito Internacional Costumeiro, assentou que o respeito à integridade territorial dos Estados é um fundamento essencial das

---

[31] "*A solução de problemas relacionados com a vigência espacial da lei penal se resolve de acordo com as normas de direito positivo, aí compreendidos os tratados e as convenções internacionais, bem como certos princípios aceitos, em doutrina, sem muita variação. São esses princípios: o da territorialidade, o do pavilhão (ou bandeira), o da personalidade (ou nacionalidade), o da defesa (ou real), e da universalidade (ou da justiça universal).*" TOLEDO, Francisco de Assis. Princípios Básicos de Direito Penal – 5ª ed. São Paulo: Saraiva, 2000, p. 45.

[32] SWINARSKI, Cristophe. **Direito Internacional Humanitário**: Como sistema de proteção internacional da pessoa humana. São Paulo: RT, 1990.

relações internacionais (Caso Atividades Paramilitares na Nicarágua); e que nenhum Estado pode, conscientemente, permitir que seu território seja usado para a prática de atos contra outros Estados (Caso Canal de Corfu).

Se um Estado falha ao adotar medidas apropriadas para impedir que seu território seja usado para causar danos a outro Estado, poderá responder pelos prejuízos de acordo com as regras do Direito Internacional, que podem variar desde a aplicação de sanções comerciais, até o legítimo uso da força armada em legítima defesa, com amparo no art. 51 da Carta das Nações Unidas[33].

Nos domínios do Espaço Cibernético, um ilícito internacional pode consistir, como seu viu, de uma violação à Carta das Nações Unidas, ou ao Direito Internacional dos Conflitos Armados (por exemplo, um ataque direcionado à população de país vizinho conflagrado por situação caracterizada como Conflito Armado Não-Internacional, de acordo com o Segundo Protocolo Adicional à Convenção de Genebra.

Este princípio de Direito Internacional induz, certamente, a dificuldades na aplicação do Marco Civil da Internet brasileira, que garante ampla liberdade ao uso da Internet em território nacional, adotando uma postura reativa, de repressão judicial individualizada aos eventuais abusos, *a posteriori*, em detrimento de condutas preventivas a cargo dos órgãos de regulação das comunicações, situados, naturalmente, no âmbito do Poder Executivo.

Imprescindível lembrar que, para fins de responsabilidade internacional do Estado, é irrelevante que suas autoridades se omitam do dever de controle que lhes incumbe, invocando alegada limitação imposta por legislação interna, considerada um mero fato pelo Direito Internacional, uma vez que a nenhum Estado é concedida a prerrogativa de aprovar leis que o induzam a violar obrigações decorrentes do Direito Internacional Público[34].

---

[33] "*Portanto, o Estado possui a faculdade jurídica de reagir a uma violação do Direito Internacional de diversas formas, tanto coercitivas como substitutivas. Podem ser tomadas medidas de coerção para que o Estado ofensor seja coagido a reparar o dano ou podem ser tomadas medidas de execução forçada, de caráter substitutivo. Além disso, podem Estados-terceiros serem legitimados a efetuar tais medidas contra o Estado violador, observadas certas condições. A violação de regra de Direito Internacional, por ação ou omissão atribuída a um Estado, cria relações jurídicas novas entre o Estado ao qual a conduta foi atribuída e outro, ou mesmo outros Estados da comunidade internacional, destinatários da regra violada.*" RAMOS, André de Carvalho. **Responsabilidade Internacional por Violação de Direitos Humanos**: Seus elementos, a reparação devida e sanções possíveis. Teoria e Prática do Direito Internacional. Rio de Janeiro: Renovar, 2004, p. 83.

[34] "*Logo, para o Direito Internacional, os atos normativos internos (leis, atos administrativos e mesmo decisões judiciais), são expressões da vontade de um Estado, que devem ser compatíveis com seus engajamentos internacionais anteriores, sob pena de ser um Estado responsabilizado internacionalmente. Conseqüentemente, um Estado não poderá justificar o descumprimento de uma obrigação internacional em virtude de mandamento interno, podendo ser coagido (com base na contemporânea teoria da responsabilidade internacional do Estado), a reparar os danos causados".* RAMOS, André de Carvalho. Op. Cit. p. 132.

Talvez imbuído desta percepção é que tenha o legislador inserido, de maneira excessivamente genérica, a previsão constante da parte final do art. 3º, parágrafo único, da Lei nº 12.965/2014, que ressalva a necessidade de observância aos princípios constantes de tratados internacionais de que faça parte a República Federativa do Brasil.

4. Conclusões

Procurou esta simplória exposição demonstrar que o Marco Civil da Internet brasileira, legislação inovadora em caráter mundial, não somente em virtude do fenômeno que se propõe a regular, mas também por força dos valores progressistas que buscou consolidar.

Vimos que, longe de se constituir na tendência predominante sobre a regulação da Internet, o Marco Civil brasileiro marcha, em realidade, no sentido oposto ao de países que enfrentam desafios sociais e políticos muito parecidos com os do Brasil, ainda a meio-caminho na jornada em direção ao tão desejado desenvolvimento econômico.

Verificamos, por outro lado, que a Internet surge como mais um campo de batalha possível, na complexa arena das relações internacionais do início do Século XXI, sujeitando-se, por isso, a normas de Direito Internacional sobre os Conflitos Armados que, não obstante prontificadas para um cenário bélico muito diferente, são ainda capazes de limitar a conduta dos Estados, seja no uso da força entre si (*jus ad bellum*), seja no curso de hostilidades já conflagradas (*jus in bello*).

O operador do Direito brasileiro precisará, contudo, compatibilizar diretrizes que por vezes tendem a se excluir mutuamente, umas decorrentes da Lei nº 12.965/2014, e outras derivadas do Direito Internacional Costumeiro, e dos tratados a que aderiu a República Federativa do Brasil, sob pena de, em dando prevalência somente às primeiras, induzir à responsabilização internacional do país, sobretudo em caso de omissão quanto aos deveres de controle das infraestruturas cibernéticas localizadas em seu território, que venham a ser utilizadas – mesmo que involuntariamente – para o desencadeamento de operações de "Guerra Cibernética" contra outros Estados.

REFERÊNCIA BIBLIOGRÁFICA

BRASIL. Portaria nº 666, de 04 ago. 2010 – Cria o Centro de Defesa Cibernética do Exército. Ministério da Defesa/Comando do Exército: Brasília, **Boletim do Exército nº 31**, de 06 ago. 2010.

BRASIL. Casa Civil da Presidência da República/Subchefia de Assuntos Parlamentares. **Exposição de Motivos nº EMI Nº 00086 - MJ/MP/MCT/MC**. Brasília: 25 abr. 2011.

BRASIL. **Livro Branco de Defesa Nacional**. Ministério da Defesa: Brasília, 2012.

BRASIL. **Relatório da Comissão Parlamentar de Inquérito** composta por onze membros titulares e sete suplentes, com a finalidade de, no prazo de 180 dias, investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar emails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal. Brasília, Senado Federal, 09 abr. 2014. Diário do Senado Federal. Brasília, 17 abr. 2014. Suplemento "C".

COMITÊ GESTOR DA INTERNET. **O CGI.br e o Marco Civil da Internet**: Defesa da privacidade de todos que utilizam a Internet; Neutralidade da rede; Inimputabilidade da rede. Disponível em: https://pimentalab.milharal.org/files/2013/09/CGI-e-o-Marco-Civil.pdf, acesso 12 set. 2014.

CONTRERA, Carla; ORTEGA, Dulcina. **O Comércio Eletrônico e o Código de Defesa do Consumidor**: Disciplina jurídica, aplicabilidade e evolução. Trabalho de Conclusão de Curso. São Paulo: 2013.

DE LUCCA, Newton. **Contratación Informática y Telemática**. Bogotá: Javeriana, 2012.

FEDERAÇÃO RUSSA. **Russian Federation Armed Forces' Information Space Activities Concept**. Disponível em: http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle, acesso: 12 set. 2014.

GONÇALVES, Victor Hugo Pereira. **Direito Fundamental à Exclusão Digital**. Disponível em: https://www.academia.edu/4783856/Exclusao_Digital_como_Direito_Fundamental, acesso: 12 set. 2014.

LIBRARY OF THE CONGRESS. **Turkey: Law on Internet Publications Amended**. Disponível em: http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403875_text , acesso 12 set. 2014.

LORENZETTI, Ricardo Luis. **Comércio eletrônico**. Trad. Fabiano Menke. São Paulo: RT, 2004.

MARTINS, Helena. **Entenda os três princípios do Marco Civil da Internet**. Disponível em: http://www.jcnet.com.br/Geral/2014/04/entenda-os-tres-principios-do-marco-civil-da-internet.html, acesso 11 set. 2014.

MENEZES, Wagner. **Os Princípios no Direito Internacional** *in* CASELLA, Paulo Borba; RAMOS, André de Carvalho (org.). **Direito Internacional**: Homenagem a Adherbal Meira Mattos. São Paulo, Quartier Latin, 2009.

ORAKHELASHVILI, Alexander. **The Interpretation of Acts and Rules in Public International Law**. Oxford: Oxford University Press, 2008.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração do Terceiro Comitê da Assembleia-Geral das Nações Unidas**: Direito à Privacidade na Era Digital. GA/SHC/4094. Nova York, 26 nov. 2013.

PEREIRA, Helio do Valle. Manual da Fazenda Pública em Juízo – 2ª ed. Rio de Janeiro: Renovar, 2006.

RAMOS, André de Carvalho. **Responsabilidade Internacional por Violação de Direitos Humanos**: Seus elementos, a reparação devida e sanções possíveis. Teoria e Prática do Direito Internacional. Rio de Janeiro: Renovar, 2004.

RODRIGUES JUNIOR, Otávio Luiz. **Liberdades comunicativas e privacidade no Marco Civil**. Disponível em: http://www.conjur.com.br/2014-mai-07/direito-comparado-liberdades-comunicativa-vida-privada-marco-civil, acesso: 11 set. 2014.

ROSSINI, Augusto Eduardo de Souza. Informática, telemática e Direito Penal. São Paulo: Memória Jurídica, 2004.

SASSEN, Saskia. **Territorio, autoridad y derechos**: de los ensemblajes medievales a los ensenblajes globales. Buenos Aires: Katz Editores, 2013.

SCHMITT, Michael N. **Tallin Manual on the International Law Applicable to Cyber Warfare**: Prepared by the International Group of Experts at the Invitation of the Nato Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press, 2013.

SCOTT, **Hague Court Reports 2d 83** (1932) (Perm. Ct. 4rb. 1928), 2 U.N. Rep. Intl. 4rb. Awards 829.

SWINARSKI, Cristophe. **Direito Internacional Humanitário**: Como sistema de proteção internacional da pessoa humana. São Paulo: RT, 1990.