CIBERSEGURANÇA

ANO
XV
2014

4

# Cadernos Adenauer

# CIBERSEGURANÇA

Konrad
Adenauer
Stiftung

EDITOR RESPONSÁVEL
Felix Dane

CONSELHO EDITORIAL
Estevão de Rezende Martins
Fátima Anastasia
Humberto Dantas
José Álvaro Moisés
José Mario Brasiliense Carneiro
Lúcia Avelar
Silvana Krause

COORDENAÇÃO EDITORIAL
Reinaldo J. Themoteo

REVISÃO
Reinaldo J. Themoteo

CAPA, PROJETO GRÁFICO E DIAGRAMAÇÃO
Cacau Mendes

IMPRESSÃO
Stamppa

---

ISSN 1519-0951

Cadernos Adenauer XV (2014), nº4
*Cibersegurança*
Rio de Janeiro: Fundação Konrad Adenauer, junho 2015.
ISBN 978-85-7504-191-8

---



FUNDAÇÃO KONRAD ADENAUER
Representação no Brasil: Rua Guilhermina Guinle, 163 · Botafogo
Rio de Janeiro · RJ · 22270-060
Tel.: 0055-21-2220-5441 · Telefax: 0055-21-2220-5448
adenauer-brasil@kas.de · www.kas.de/brasil
Impresso no Brasil

# Sumário

# Apresentação

■ Do mesmo modo vertiginoso como os avanços nas novas tecnologias chegam, influenciando vidas de indivíduos e de sociedades inteiras, produzindo novos hábitos e sendo substituídos por tecnologias ainda mais recentes, na atualidade temos que lidar a cada dia com grandes volumes de informação, todo este conjunto de tecnologias, conhecimento e interações se traduzindo também numa série de implicações em termos de segurança, em diversos níveis. Esta edição da série Cadernos Adenauer é dedicada ao tema da cibersegurança, com o objetivo de promover o debate sobre cinco tópicos: vazamento de informações, regulamentação da internet, o *soft power* das novas mídias, cyberterrorismo e operações cibernéticas militares.

No primeiro capítulo Heloisa Pait e Ruan Sales de Paula Pinheiro abordam um dos temas mais polêmicos na atualidade, nos debates sobre cibersegurança: o vazamento de informações. Tomando como ponto de partida uma análise sobre o papel dos vazamentos de informações em sociedades democráticas, os autores exploram os vazamentos no Brasil e nos estados Unidos, explicitando os aspectos fundamentais para a sua compreensão, e culminam com uma análise do vazamento de informações na época da internet, englobando os principais acontecimentos mais recentes.

Patrícia Peck Pinheiro investiga a cibersegurança em sua feição jurídica. Em seu capítulo, sobre a regulamentação da internet, são explicitados os principais tópicos envolvidos nesta temática, facultando uma visão geral que nos mostra a grande complexidade na construção de normas que englobem de modo pertinente as variadas situações que se apresentam na realidade brasileira quanto ao uso da internet, articulando as questões teóricas com fatos objetivos, como a lei Carolina Dieckman e o Marco Civil da Internet.

Rafael Santos de Oliveira reflete sobre como o *soft power* das novas mídias permeia as Relações Internacionais. Nesta empreitada o autor investiga como o conceito de *soft power* é construído conceitualmente e as suas implicações na mídia em nível global, bem como o *soft power* e as novas mídias no âmbito dos fluxos de informação, no âmbito do paradoxo da informação.

Robert Muggah, Misha Glenn e Gustavo Diniz apresentam um estudo sobre cibersegurança no Brasil, investigando as iniciativas governamentais desenvolvidas de modo a impulsionar a arquitetura nacional de cibersegurança, buscando robustecer sua posição enquanto potência emergente. Partindo da caracterização do ciberespaço e da exposição das principais ameaças virtuais, são investigadas as estratégias desenvolvidas pelo governo brasileiro no enfrentamento das ameaças cibernéticas.

Julia Donsbusch investiga diversos aspectos das operações cibernéticas de caráter militar, a partir do enfoque da lei internacional. Um dos principais tópicos de sua análise diz respeito à necessidade dos Estados alcançarem um entendimento em comum acerca do que venha a ser soberania, bem como os elementos fundamentais da lei internacional que tipificam as ações cibernéticas. Nesta investigação são considerados diversos tipos de ações e ataques cibernéticos, assim como os desafios concernentes à soberania das nações, além das obrigações dos Estados em relação à segurança cibernética.

Esperamos que estas análises de alguma forma possam contribuir nos debates e reflexões sobre cibersegurança e o modo como este tema nos afeta a todos seja direta ou indiretamente, desejamos a todos uma boa leitura.

Reinaldo J. Themoteo
*Coordenador Editorial da Fundação Konrad Adenauer no Brasil*

# Vazamento de informações: um ritual democrático na era da comunicação em rede

HELOISA PAIT
RUAN SALES DE PAULA PINHEIRO

■ Começar esse texto com uma referência a Walter Benjamin parece adequado, pois sua morte nos Pirineus, em fuga para o oeste em 1940, está envolta em mistérios. Benjamin se matou, como nosso Stephen Zweig, diante do desastre pessoal e coletivo que se avizinhava? Foi caçado pelos nazistas, que impediram sua fuga para os Estados Unidos? Ou foi assassinado pelo serviço secreto russo, o que parece hoje plausível? Seus escritos até então foram repletos de aforismos e indagações: um homem olha um quadro e pensa sobre o tempo, outro passeia pelas ruas de Paris, um terceiro reflete sobre o papel do conto na vida moderna. Talvez os que carregasse na mala questionassem o stalinismo, é verdade, mas ainda assim, por que eliminar Benjamin? (Schwartz, 2001)

O tema recorrente do autor alemão é a perda de uma certa capacidade humana na sociedade moderna: a capacidade de dar sentido ao tempo, de contar uma história, de extrair significado das coisas, dos eventos, das pessoas. Nisso ele não se distancia dos grandes pensadores sociais das primeiras décadas do século XX, apenas trazendo um sentido de urgência apropriado ao seu próprio tempo. Num de seus escritos famosos, Benjamin descreve como a obra de arte perdeu a aura com a reprodução técnica; a fotografia ou o cinema são de fácil acesso, mas não são elementos de culto como uma escultura ou o próprio teatro. (Benjamin, 1968). Nosso artigo vai nessa toada: a quantidade massiva de informação que temos hoje, na sociedade como um todo e na esfera que nos interessa, a do Estado, roubou a aura dos vazamentos de informação, que num passado recente tinham algo de heróico, podendo ser contados em histórias e fazendo parte de um ritual arcaico ainda que no seio da sociedade moderna.

Vazamentos hoje têm um escopo global; seja pela plataforma Wikileaks, seja através de um consórcio internacional de jornais de renome, os públicos nacionais se interam dos vazamentos cada vez mais enquanto público global. Além disso, o volume dos vazamentos é algo inimaginável até décadas atrás, pela quantidade de informação produzida e armazenada, assim como pela facilidade de transmissão, que está ao dispor de qualquer cidadão de um país desenvolvido. Isso tudo altera algo na relação que temos com essa informação, assim como nossa relação com uma pintura é distinta da que temos com uma fotografia, por mais valiosa que seja. O que não quer dizer que o significado do vazamento se perca completamente e que estejamos tratando hoje da simples dispersão aleatória de bits; apenas que temos que repensar os vazamentos e compreender seu significado transformador mais geral, que é o objetivo desse artigo. Seguindo a trilha de Benjamin, oxalá evitando os Pirineus, vamos pensar o que são vazamentos de segredos na era da informação em rede.

O artigo começa resgatando a reflexão sobre o segredo de Georg Simmel, ao que adicionaremos, inspirados pelo autor, um tipo social que congrega nele mesmo as tensões entre segredo e publicidade, que chamamos de alardeador. A partir dessa reflexão, buscaremos compreender o papel do vazamento em sociedades democráticas, que é o de refazer um laço entre sociedade e Estado, laço esse que por alguma razão se esgarçou. Contrastamos esse importante papel com aquele dos vazamentos em sociedades patrimoniais ou totalitárias, ou seja, quando a distinção entre sociedade e Estado está pouco clara ou inexiste, ao menos no discurso. Numa segunda parte, tratamos da experiência americana e brasileira. Sublinhamos que existe desde o início da história dos Estados Unidos a tensão entre o interesse do governo em manter segredo e o interesse do público por abertura, além de uma disputa permanente em torno da própria definição de interesse público. No Brasil o espírito patrimonialista enseja a adesão do estamento dominante ao Estado e, consequentemente, o reforço aos seus segredos. Valores como participação, representação e transparência se afirmam tardiamente, e isso explica a relativa ausência de vazamentos no país.

A seguir, olharemos para os vazamentos como um ritual arcaico, onde o alardeador, instado a revelar os segredos cuja posse desconfortavelmente detêm, expõe-se à esfera pública, pessoalmente ou através de um patrono, e submete-se a um julgamento público e mediado, ou seja, realizado na esfera pública desenhada pelos meios de comunicação. O sucesso do vazamento, ou seja, o reencontro entre a sociedade civil autônoma e o Estado, dependerá em larga medida do desenvolvimento desse ritual de expiação. Numa quarta parte, descreveremos em

maior detalhe o impacto que as diversas mudanças no ambiente comunicativo têm sobre esse ritual. Finalmente, concluímos o texto refletindo sobre os riscos do ritual de vazamento, que não tem resultado definido, sobre o quanto seu exame pode revelar sobre as sociedades onde eles ocorrem, e sobre os desafios postos para o vazamento numa sociedade global.

## SEGREDO, SOCIEDADE E ESTADO

Pela perspectiva da sociologia do segredo inaugurada por Simmel (1906) a ocultação deliberada de certas realidades por meios "negativos ou positivos" consiste em um dos fundamentos da vida social. Para o sociólogo alemão "o segredo constitui uma das maiores conquistas da humanidade", uma vez que a situação de completa publicidade não permitiria que a vida se manifestasse em sua plenitude. Um encanto formal e uma utilidade prática levariam o homem a guardar segredo, enquanto que um "instinto de idealização", a importância exacerbada conferida por nossa fantasia àquilo que é secreto, e o temor natural diante do desconhecido despertariam nele o desejo de descobrir aquilo que lhe fosse ocultado.

Haveria também a incapacidade de se resistir por muito tempo à tensão infligida pela reserva do sigilo, reforçada pelo fato de que a sensação de "superioridade latente", associada ao conhecimento daquilo que a outros se oculta só pode ser plenamente desfrutada, justamente, no momento da revelação. Simmel (1906, p. 466) identifica, então, o puro prazer da revelação "que pode acobertar outra forma perversa e negativa de sensação de poder". Segundo o autor, justamente por isso "o segredo ocorre envolto na possibilidade e na tentação da revelação; e com o risco externo de que seja descoberto, se combina este intento de desvelá-lo que se assemelha à atração do abismo" (Simmel, 1906, p. 466).

As relações entre os homens seriam, portanto, fortemente influenciadas pela oposição entre os interesses de esconder e de descobrir, de manter e de revelar segredos. Ao mesmo tempo em que uma barreira entre os indivíduos é levantada pelo sigilo, "a tentação de romper essa barreira por indiscrição ou confissão acompanha a vida psíquica do que é secreto".

Ademais, o segredo é também tratado como instituição política, elemento fundamental da dominação e da governabilidade. Segundo Canetti (2005, p. 290) o sigilo se encontra no "mais recôndito cerne do poder", especialmente presente no campo das relações internacionais. E, de fato, os segredos da política de gabinetes e os "mistérios dos reis" foram alicerces do poder desde os primórdios do Estado moderno. Ao longo dos séculos, ocorreu a transição em direção a um

poder público, vinculado ao interesse dos cidadãos e não mais apartado da sociedade como esfera isolada de dominação, o que não representou o fim dos segredos de Estado. Há segredos dos quais governo algum pode prescindir: aqueles identificados como verdadeiros segredos de segurança nacional, justificados pela necessidade do Estado de assegurar por seus próprios meios a sua sobrevivência em um sistema internacional anárquico.

Uma definição mais precisa do que seriam tais segredos de segurança nacional é comprometida pela própria imprecisão e grande flexibilidade deste último conceito. Não obstante, é possível recorrer ao conceito de informações estratégicas e identificar aquelas informações que podem ter seu sigilo justificado uma vez que, "conhecidas por um adversário ou inimigo, aumentam nossas vulnerabilidades e fornecem uma vantagem comparativa crucial para os adversários nas interações conflitivas" (Cepik, 2003, p. 152). Nessa definição entram informações sobre sistemas de armas, pesquisa científica e tecnológica de aplicação militar e intenções em negociações de acordos internacionais, por exemplo.

O segredo acerca de fontes e métodos de inteligência também se encaixa nessa categoria. Trata-se, de fato, de informações sensíveis cuja revelação pode ter consequências realmente perversas para a segurança do Estado, de seus funcionários e cidadãos. Por isso agentes do governo americano se ressentem de o jornal *Washington Times* ter divulgado em 1998 a informação sigilosa de que a *National Security Agency* (NSA) interceptava a comunicação telefônica de Osama Bin Laden, líder da Al Qaeda, grupo terrorista que havia pouco bombardeara duas embaixadas americanas no Quênia e na Tanzânia, causando a morte de 258 pessoas, sendo 12 americanos.

A informação foi divulgada em 21 de Agosto de 1998, dia seguinte ao contra-ataque dos EUA com mísseis disparados contra bases da Al Qaeda no Afeganistão. Como consequência, Bin Laden teria parado quase imediatamente de utilizar os telefones por satélite, impedindo as interceptações da NSA, de modo que a inteligência americana perdia assim uma fonte valiosa para rastrear o terrorista. O dito vazamento foi condenado pelo relatório final da Comissão parlamentar sobre o 11 de Setembro, e também pelo então presidente dos EUA, George W. Bush.

Porém, nem todos os segredos guardados são assim tão autênticos, e transparência é uma exigência dos regimes liberais democráticos, que procuram submeter o exercício do poder ao escrutínio público de modo a legitimá-lo e controlá-lo. Como atesta Bobbio (1989, p. 29), "a democracia nasceu com a perspectiva de eliminar para sempre das sociedades humanas o poder invisível e de dar vida a um

governo cujas ações deveriam ser desenvolvidas publicamente". Por definição, em democracias liberais a publicidade dos atos públicos é a regra geral com a qual o sigilo deve contrastar na condição de exceção. Só que, como pondera o próprio Bobbio (2000, p. 206), mesmo em democracias a tendência do poder a se esconder é irresistível.

Nesse sentido, pode-se entender o vazamento de informações como tentativa de impor a abertura que o poder teima em não conceder, e de modo mais amplo, como questionamento dos termos da relação entre Estado e Sociedade. Quando não há meios formais e institucionalizados para se alcançar um equilíbrio satisfatório entre o direito do público à informação e a necessidade de proteger os segredos de Estado, ou quando esses meios falham em transmitir ao cidadão a impressão de abertura, o vazamento se apresenta como expressão de demanda por transparência, reação inflamada à supremacia do segredo, à distorção do sentido de interesse público. Se, como bem observou Arendt (1968, p. 293), aqueles que dão publicidade a segredos legítimos do Estado são tratados como traidores, por outro lado, o vazamento de segredos ilegítimos ou prescindíveis é muitas vezes encarado como ato de cidadania e até heroísmo.

Com esse sentido que estamos adotando, vazamentos de informações estatais ocorrem apenas em regimes democráticos ou naqueles em que se vislumbra a possibilidade de um caminho democrático. Essa ideia de vazamento pressupõe que há uma sociedade civil autônoma, com desejos próprios e que pode em princípio ter direito a conhecer assuntos do Estado, aquele que busca manter o monopólio de determinados fluxos de informação por meio de procedimentos de classificação, controles de acesso e punições em caso de revelação não autorizada (Cepik, 2003, p. 153). A sociedade civil que temos em vista é justamente aquela entendida como "a base da qual partem as solicitações às quais o sistema político está chamado a responder; como o campo das várias formas de mobilização, de associação e de organização das forças sociais que impelem à conquista do poder político" (Bobbio, 1999, p. 1211).

Nesse caso, as informações sigilosas que chegam ao conhecimento público sem o consentimento do Estado, não são vistas, a não ser em casos especiais, como fruto de crime de lesa pátria: elas são tidas como vazamentos, preocupando o cidadão por seu conteúdo mais do que pela infração penal em si. Por exemplo, quando vazaram os *Pentagon Papers*, o debate público deu-se mais em torno de seu conteúdo, que era a propriedade da continuação da guerra no Vietnã, do que em relação aos mecanismos de proteção de informações do governo. Se, ao contrário, temos em mente um governo totalitário, onde a sociedade se subordina

de modo completo aos interesses do Estado, há apenas lugar para a traição, e não para o vazamento; a disseminação de informação é algo contrário aos interesses do Estado e, portanto, da Nação.

Ilustremos isso com a publicação no exterior feita num momento de recrudescimento da repressão interna soviética de um livro como Arquipélago Gulag, de Alexander Solzhenitsyn, que descrevia em detalhes o horror dos campos de trabalho siberianos. Ela pode ter agradado alguns cidadãos da então União Soviética, mas o autor de um livro como esse deve ser banido, censurado, punido e de modo geral excluído de qualquer nesga de esfera pública, pois não há lugar simbólico para o vazamento numa situação de forte autoritarismo. Em uma época anterior de abertura, sob Kruchev, o mesmo autor foi louvado por oxigenar o regime com seus relatos, e fez todo o sentido que ele continuasse sua obra de revelação e denúncia desse episódio bárbaro da história russa. Note que a questão aqui é de publicação e reconhecimento, e não de conhecimento; boa parte da população, por experiência própria, tinha uma triste ideia do que acontecia nos campos de trabalhos forçados do leste russo. Uma amiga russa relata que sua avó, tendo perdido a filha e o genro para Stalin, não tocava no assunto em casa para proteger a família: até mesmo o luto privado é traidor num regime totalitário. Ou seja, num regime extremamente fechado, a revelação é neutralizada seja pelo pavor individual, seja pelo banimento da esfera pública; a assimilação da sociedade pelo Estado se dá pela força.

Por outro lado, num regime democrático onde a sociedade tem seu direito de informação plenamente atendido, de acordo com regras transparentes acordadas consensualmente, onde o segredo está restrito àqueles assuntos que foram delegados ao Estado - os segredos de Estado legítimos - também não há vazamento; apenas traição. Assim, a sociedade israelense, que entende existirem ameaças sérias e constantes à sua integridade nacional, aceita sem grandes contestações que as forças armadas designem uma censora para dar aval a publicações jornalísticas, censora essa que é respeitada e até tratada com afeto por boa parte da imprensa, ainda que em casos específicos os jornais tentem burlar a censura.

Estamos afirmando que os vazamentos existem quando a sociedade é autônoma apesar de sua arena de atuação não estar plenamente definida e acordada consensualmente. Ou seja, quando a pergunta "O que a sociedade deve saber?" tem respostas divergentes, mas a pergunta em si é vista como legítima por toda a sociedade, incluindo aí líderes e funcionários públicos. Numa situação onde a segurança nacional está em jogo, a resposta à pergunta é óbvia, o que não quer dizer, no nosso exemplo, que a sociedade israelense não debata extensivamente as

ações cotidianas do governo e mesmo decisões militares. Já quando a relação entre sociedade e Estado é patrimonial, usando a terminologia de Raymundo Faoro (Faoro, 1975), ou seja, quando a sociedade se subordina à lógica empreendedora do Estado, que lhe concede e retira autonomia de acordo com suas próprias necessidades cambiantes, há em princípio mais razões para os vazamentos, ou seja, há maiores divergências entre a moral do Estado e os desejos sociais. Entretanto, a dificuldade em articular esses desejos de modo coerente é tal que fica difícil estabelecer quais sejam essas divergências, dada a relação infantilizada que o patrimonialismo propõe aos cidadãos.

Seria interessante conhecer todas as condições que impedem que o consenso se estabeleça, abrindo então espaço para o vazamento de informações. Mudanças na orientação política do governo que não são acompanhadas pela burocracia estatal podem gerar alguma má vontade, alguma predisposição de certos funcionários públicos ao vazamento, mas essa razão seria notada no debate público. Abusos incompatíveis com a autoimagem da nação, como no caso Irã-Contras, geram belos vazamentos, com inquéritos públicos e discussões espetaculares, heróis e bandidos, catarses. De modo geral, sociedades complexas abarcam grupos sociais diversos e algum grau de dissenso é natural; deste modo, uma nova geração de funcionários no ministério das relações exteriores ou de defesa pode trazer concepções que se chocam com os hábitos vigentes; se a sociedade não acompanha as mudanças regulamentando a nova situação, ou se a burocracia não acomoda as demandas emergentes, o resultado pode ser o vazamento. Como veremos adiante, mudanças nos ambiente comunicativo também podem gerar tensões.

Ou seja, é a regra, e não a exceção, em uma sociedade democrática o vazamento periódico de informações. São esses vazamentos que ajustam expectativas com relação aos papéis da sociedade e do Estado, relembrando a sociedade de suas prerrogativas e o Estado de suas atribuições. Vazamentos são então como terremotos: colisões entre placas distintas, porém acopladas, que depois de movimentação paulatina por muito tempo de repente se reacomodam numa nova situação, liberando energia. Na parte a seguir, nos deteremos sobre a experiência de Estados Unidos e Brasil quanto ao vazamento de informações. Os vazamentos da grande potência de tradição liberal e democrática têm importância global, e seu desdobramento é acompanhado por uma audiência internacional. Já o Brasil que oscila entre a democracia e o autoritarismo desde o estabelecimento da República, e é marcado por uma cultura patrimonialista, é o contraponto que permite destacar singularidades e regularidades, contribuindo para a análise.

## VAZAMENTOS NO BRASIL E ESTADOS UNIDOS

A experiência norte-americana sustenta a ideia de que vazamentos são a regra em sociedades democráticas. Lá, segundo Cepik (2003, p. 156), na maioria dos casos divulgados corriqueiramente pela mídia do país, as informações são vazadas por membros do próprio governo interessados em "lançar balões-de-ensaio sobre políticas e projetos", "torpedear uma política da qual discordam" ou "avançar seus próprios interesses na disputa inter-burocrática". Não obstante, na história do país há casos de grande repercussão envolvendo segredos importantes referentes, principalmente, à política externa.

Isso porque nos EUA a demanda por abertura evoluiu desde muito cedo, a partir do campo simbólico, com o valor da transparência se formando primeiro entre filósofos, juristas, jornalistas, depois sendo transmitido por intermédio das instituições, como imprensa e universidades, a toda a sociedade. Essa demanda precedeu inclusive a valorização e a institucionalização do sigilo, que se deu a partir de 1917, com a entrada do país na Primeira Grande Guerra, e que se consolidou na medida em que se via constantemente ameaçado por inimigos externos e internos, encarando frequentes períodos de crise, em uma realidade na qual a alegada prioridade absoluta dos governos não era outra senão a chamada segurança nacional. Da tensão entre cultura do sigilo e demanda por transparência, entre a razão de estado e os valores de uma nação convencida de seu excepcionalismo, derivaram muitos vazamentos (Moynihan, 1998; Blanton, 2003).

Além disso, Doyle (1999, p. 4) destaca como a partir da década de 1950 a inexistência de uma legislação que garantisse o direito de acesso à informação levou a imprensa e o público norte-americano a buscar nos vazamentos uma forma de desvendar alguns dos mistérios da cada vez mais secreta política externa dos Estados Unidos. A lei de acesso seria aprovada em 1966, mas não foi suficiente para evitar um dos casos mais notáveis de vazamento de informações sigilosas da história americana. No dia 13 de junho de 1971, durante o governo Nixon, o jornal *New York Times* publicou a primeira de uma série de dez matérias sobre a história secreta da Guerra do Vietnã, revelada após o vazamento dos documentos que ficaram conhecidos como *Pentagon Papers.* Tratava-se de um estudo ultrassecreto do Departamento de Defesa que continha sete mil páginas de informações e análises sobre o envolvimento militar dos Estados Unidos no Vietnã, entre os anos de 1945 e 1967.

O responsável pelo vazamento do documento era Daniel Ellsberg, apresentado pela mídia norte-americana como um dos principais analistas políticos dos

Departamentos de Estado e de Defesa dos Estados Unidos. De fato, entre 1964 e 1965, Ellsberg trabalhou no Pentágono, com um cargo no *International Security Affairs (*ISA), alto escalão civil do Departamento de Defesa. Nesse período, ele teve acesso a importantes tomadores de decisão do governo, e a documentos, muitos deles secretos e ultrassecretos, que, segundo ele, por vezes contradiziam as próprias políticas adotadas (Ellsberg, 2003, p. 4).

No dia 1º de Outubro de 1969, iniciou o trabalhoso e demorado processo de cópia dos 47 volumes dos "Papéis do Pentágono", o estudo do Departamento de Defesa que ele inclusive havia ajudado a escrever. A ideia era dar à opinião pública e ao congresso as informações de que precisavam para concluir que a guerra era ilegítima, que havia sido baseada, desde sua origem, em mentiras deliberadas, cultivadas por cinco administrações da Casa Branca e mantidas em rigoroso sigilo. O objetivo principal era conseguir a mobilização dos norte-americanos contra a continuidade do envolvimento militar no Vietnã. Os documentos vazados tiveram repercussão primeiro no *New York Times*, depois no *Washington Post*, no *Boston Globe*, no *Chicago Sun Times*, e em outras treze organizações de mídia norte-americanas. A administração Nixon rapidamente exigiu na justiça a supressão das publicações sobre o caso, conseguindo algumas decisões favoráveis à censura. A Suprema Corte chegou mesmo a manter a proibição às publicações do *New York Times* e do *Washington Post* por algum tempo até o julgamento definitivo, mas a decisão final dos magistrados, por seis votos a três, foi favorável aos jornais que tiveram assegurado seu direito de publicar matérias sobre os "Papéis do Pentágono".

Ellsberg também foi acusado de crimes, com base principalmente na Lei de Espionagem de 1917. Ele se entregou à polícia, logo foi solto após pagamento de fiança e enfrentou o julgamento que o absolveu. Segundo a justiça dos Estados Unidos, Ellsberg era inocente. E o que mais pesou para que ele não fosse considerado um traidor foi justamente a natureza dos segredos revelados. Os documentos não haviam sido classificados para prevenir danos à segurança nacional, mas sim para que os governantes pudessem evitar constrangimentos e embaraços de qualquer natureza. Em relação à Eisenhower, a matéria do *Washington Post*[1] de 18 de Junho de 1971 tratava da revelação de que seu governo apoiara o golpe de estado de Ngo Dinh Diem e a ditadura brutal estabelecida por ele no Vietnã do Sul, temendo a possibilidade de uma vitória comunista nas eleições que segundo

1 Washington Post, 18 de junho de 1971: "*Documents Reveal U.S. Effort In '54 to Delay Viet Election*".

o Acordo de Genebra de 1954 (o acordo de paz entre França e Vietnã) deveriam ocorrer até 1956, visando à reunificação do Vietnã. Com o golpe, as eleições foram canceladas, a reunificação evitada e os opositores da ditadura passaram a ser perseguidos e mortos.

Já Kennedy teve seu papel na escalada do envolvimento militar americano na Indochina destacado pelo *Boston Globe.* As revelações desmentiram o Presidente que alegava enviar ao Vietnã somente assessores e conselheiros militares, enquanto de fato foi o primeiro a mandar tropas de combate norte-americanas àquele país. Do mesmo modo, desmentiram Lyndon Johnson, que usou como argumento para finalmente declarar a guerra um suposto atentado a navios dos Estados Unidos no Golfo de Tonquim o qual, na verdade, nunca ocorreu. Os documentos vazados por Ellsberg tornaram público ainda o fato de que a decisão de fazer a guerra já havia sido tomada mesmo antes de as eleições de 1964 elegerem Johnson como Presidente[2]. Havia uma clara fissura entre o discurso público e a ação. A política externa parecia, àquela altura, desconectada da sociedade, e o vazamento, ao expor essa ruptura, podia contribuir para uma recomposição.

No Brasil, vazamentos não são frequentes e são poucos os casos que alcançaram repercussão. A balança da tensão entre segredo e transparência pendeu muito para o lado do segredo ao longo da história do país, especialmente no que toca a política externa. Enquanto a observância normativa do princípio da publicidade só se deu com a Constituição de 1988, muitos decretos, ordens executivas e leis trataram da proteção aos segredos de Estado desde a Independência. Apesar das inúmeras contradições ensejadas pela dominação patrimonialista, a falta de autonomia das camadas subalternas da sociedade e a adesão dos estamentos dominantes ao Estado ajudam a entender a escassez de grandes vazamentos. Além disso, a afirmação da transparência como valor, princípio abstrato demandado pela esfera pública, só começou a amadurecer a partir da década de 1950.

De fato, a preocupação com o sigilo já estava presente nas primeiras leis do Brasil independente, e certamente é uma herança de Portugal, a antiga metrópole. O "1º Regimento das Legações de Sua Majestade o Imperador do Brasil", de 1834, tratava de um dito "Livro Secreto B", o qual conteria, dentre outras coisas, "quaisquer comunicações secretíssimas" e deveria ser guardado somente pelo Ministro de Estado dos Negócios Estrangeiros. Para não haver dúvida quanto à importância dos segredos para os pioneiros do Itamaraty, outro documento, o 1º

2 A manchete da matéria de capa de Neil Sheehan no *New York Times* de 14 de junho de 1971 era: "*Vietnam Archive: A Consensus To Bomb Developed Before '64 Elections, Study Says*".

Regulamento da Secretaria de Estado, de 1842, trazia em seu artigo 38 a previsão de que todos os servidores seriam : "responsáveis por faltas e omissões" no exercício de suas atribuições, mas "especialmente pelos segredos da Secretaria; sendo motivo suficiente para uma pronta demissão a divulgação deles".

Com esse artigo o regulamento formalizava a previsão de punição em caso de revelação não autorizada (vazamento) de segredos do Ministério, então chamado Secretaria. E não só: atribuía a essa infração um peso maior e um caráter mais grave do que às demais "faltas e omissões no exercício das atribuições". Posteriormente, o chamado Regulamento Paranhos, que deu nova organização à Secretaria de Estado dos Negócios Estrangeiros, em 1859, reafirmou a gravidade do delito e a severidade das medidas a serem tomadas em caso de vazamento de informações sigilosas do Itamaraty. Dos artigos 52 ao 56 o Regulamento tratou das demissões e medidas disciplinares que poderiam ser impostas aos funcionários e determinou que mesmo que os funcionários tivessem mais de 10 anos de serviço, poderiam sofrer a pena de demissão por qualquer um dos seguintes motivos: a) perpetração de qualquer crime grave; b) a revelação de segredos; c) a traição, o abuso de confiança, a insubordinação grave ou repetida e a irregularidade de conduta (Brasil, 1859).

A política externa brasileira seria fundada nos moldes da tradição europeia da diplomacia secreta, de modo que seu principal expediente, os tratados secretos, também acompanharam o país desde cedo. Um caso singular de vazamento se deu justamente quando ecos da agitação internacional contra a diplomacia secreta, acusada de ser culpada pela Primeira Guerra Mundial, chegaram ao país. O jornal "Imparcial", do Rio de Janeiro, de 12 de abril de 1919, trazia em sua segunda página um editorial intitulado "Diplomacia Secreta". Nele era narrado como Rui Barbosa em uma conferência em São Paulo havia revelado, com base em documentos secretos do Itamaraty vazados misteriosamente, uma "clara, meridiana e inconfundível" traição do então Ministro do Exterior Lauro Muller, acusado de agir secretamente contra a vontade nacional durante a Primeira Guerra Mundial em virtude de uma suposta "obstinação teutônica" e "paixão germanófila". O articulista afirmava: "O telegrama 55 é um documento esmagador da traição do Sr. Lauro Muller. Para compensar o rompimento com a Alemanha, o chanceler, germanista, procurava a todo transe um incidente desastroso com as nações aliadas"[3].

O caso do vazamento serviu para pressionar Lauro Muller que deixaria o Ministério pouco tempo depois. Naquele período, as páginas dos principais jor-

3 Imparcial, 12 de abril de.1919: "Diplomacia Secreta". Editorial, p. 2.

nais do Rio de Janeiro, capital do país à época, mostram que por um lado foram formuladas algumas condenações sofisticadas ao "segredo absoluto" e vozes se levantaram em defesa da influência da opinião pública sobre a política, muitas vezes tomando como mote algum caso concreto de segredo incômodo que atentaria contra os "princípios democráticos". Por outro lado eram também abundantes e neutralizavam qualquer pressão por abertura os textos em defesa da diplomacia secreta, da tradição diplomática, do virtuosismo da chancelaria que requereria discrição e isolamento. Um debate rico cujos termos se mantêm atuais.

Contudo, uma análise mais atenta põe em relevo o pequeno lastro social da discussão protagonizada pelos jornais. Na disputa pelos melhores argumentos os leitores eram apenas plateia e aquilo que era dito não tinha necessariamente respaldo de estratos da sociedade. O acirrado debate dos anos 1919-1920 acerca da diplomacia secreta logo arrefeceu e foi esquecido sem impacto identificável.

Em 1923, a primeira Lei de Imprensa da República, com o apoio de parte da imprensa, limitou significativamente a liberdade de expressão, prevendo inclusive penas de prisão e multas em dinheiro para "abusos" como a publicação de segredos de Estado e ofensas ao presidente. O texto da lei pretendia impedir que a imprensa tomasse parte em vazamentos de informações ao estabelecer que "a publicação de segredos do Estado é punida com a pena de prisão celular por um a quatro anos, também aplicável no caso de notícias ou informações relativas à sua força, preparação e defesa militar, se tais notícias ou informações puderem de algum modo influir sobre a sua segurança externa ou despertar rivalidades ou desconfianças, perturbadoras das boas relações internacionais".

Naquele contexto em que a maior parcela da população era rural, subalterna e sujeita às regras dos proprietários de terra, analfabeta e sem direitos políticos, a esfera pública se confundia em grande medida com o estamento dominante, que não se opunha sistematicamente ao Estado justamente por se confundir com ele. Se não bastasse, a complacência da esfera pública era conquistada também por meio de censura, repressão e subvenções, que indicam por sua vez o padrão de autoritarismo seguido pelo Estado em sua relação com a sociedade. A persistência dessa situação por muito tempo é uma das razões para a relativa escassez de relevantes vazamentos de informações sigilosas na história do Brasil.

Na década de 1950, com o fim da ditadura do Estado Novo, o quadro começaria a mudar. O Brasil vivia enfim um período de democracia de massas, a industrialização estava em marcha, empresas estrangeiras chegavam ao país, e com isso emergia o "espírito burguês". A publicidade passou a ser entendida como valiosa à iniciativa privada, demandada pelos "detentores do poder econômico não

achegados aos círculos oficiais" como forma de corrigir os vícios patrimonialistas do Estado interventor que tende a beneficiar os que "gozam de suas simpatias"[4].

Naquele novo contexto, o pragmatismo que o ex-ditador Getúlio Vargas tentou imprimir nas relações internacionais do Brasil caminhou na direção oposta à da opinião pública, mais suscetível a animosidades, melindres e simpatias. Quando o Presidente trabalhava no sentido de um acordo comercial com o governo argentino, em 1953, as reações na imprensa e no parlamento foram fortemente contrárias, "chegando ao ponto de se considerar uma traição à nação caso ele se efetuasse" (Manzur, 1999, p. 50). Vargas tentaria, então, fugir aos olhos daquela opinião opositora, negociando secretamente o Pacto ABC (Argentina, Brasil e Chile) com Juan Domingo Perón, "a fim de contrabalançar a hegemonia norte-americana no continente". Porém, a informação vazou, as negociações secretas foram denunciadas, o fato foi explorado sobremaneira pela imprensa e pela oposição, o que certamente contribuiu para o trágico fim do governo.

Nos EUA, de tradição liberal e onde a transparência se afirmou como valor social antes de o segredo ser institucionalizado como fundamento da segurança nacional, os vazamentos são mais frequentes do que no Brasil, de tradição patrimonialista, onde uma grande preocupação com o sigilo está presente desde a Independência e a demanda por transparência só avançou muito recentemente. Afora esta distinção, as experiências dos dois países, brevemente sintetizadas, convergem no que tange aos pressupostos dos vazamentos, suas causas, significados e impacto, o que nos permite interpretá-los como ritual comum às sociedades.

## UM RITUAL MEDIADO

■ Como vivemos em sociedades modernas temos certa dificuldade em enxergar nossos processos sociais como rituais. Quando muito, delegamos à cultura a manutenção do universo simbólico; na economia e na política, tendemos a ver apenas razão e interesses. A imersão entre os índios brasileiros levou os franceses Jean de Léry e, muito depois, Lévi-Strauss a rever sua própria sociedade europeia e é com esse olhar que buscamos aqui compreender o vazamento de informações na sociedade contemporânea mediada e global e seus possíveis impactos para as relações entre as nações. Os meios de comunicação são pontos privilegiados de contato entre tradição e modernidade. Bledsoe e Robey (1986) examinaram o uso mágico e secreto da escrita em sociedades tradicionais da Serra Leoa, enquanto

4 Diário Carioca, "Segredos de Estado", 11 de Maio de 1952, p. 8.

Blondheim e Liebes (2009) viram na audiência contemporânea dos meios de comunicação traços do testemunho tal como aparece na Bíblia.

Veremos aqui o vazamento de informações como um ritual sacrificial moderno, onde se busca apaziguar a nação entregando um jovem valoroso à imolação. Isso pode ser necessário quando a relação entre Estado e sociedade se encontra comprometida pelo descompasso de expectativas mútuas, causado por mudanças nas expectativas sociais, na ação estatal ou mesmo em condições gerais que não foram seguidas por adaptações de parte a parte, entre as quais apontamos mudanças nos meios de comunicação. O vazamento não é propriamente um erro que pode ser corrigido pelas agências governamentais, nem mesmo um ato heroico individual, ainda que muito possa ser feito por funcionários públicos para diminuir sua ocorrência e que ele exija uma enorme coragem pessoal e idealismo por parte do *whistleblower*, ou alardeador.

Note a dificuldade de encontrar uma tradução boa no português para *whistleblower*, pois os termos informante ou denunciante não capturam o elemento de publicidade do termo: o *whistleblower* acima de tudo lança luz sobre práticas secretas e não crimes individuais. Alardeador, tradução mais literal para "assoprador de apito", tem a conotação um pouco negativa, ligada ao exibicionismo, como na expressão "fazer alarde". Gírias de uso corrente são ainda mais inadequadas: o "dedo-duro" ou o "X-9" são estigmatizados por delatarem crimes particulares para as autoridades, e não abusos da autoridade para o público.

De modo esquemático, o ritual consiste no seguinte: um jovem se encontra em poder de segredos de estado, provavelmente por ser funcionário público. Tais informações retratam comportamentos que vão contra as expectativas que a sociedade tem em relação ao Estado, sociedade essa onde o jovem se formou e cujos valores aceita. Muitos em torno do jovem conhecem essas informações e estão cientes da contradição que elas encerram. Há uma solidariedade interna em sua repartição, mais ou menos frouxa, e uma submissão aos regulamentos que regulam a classificação de informações que impedem que eles as alardeiem, mas não que incluam cada vez mais pessoas em seu meio (ou que deixem aumentar a contradição original) até o ponto em que a tensão da posse do segredo se torna impossível de manter.

Simmel (1906, p. 466) defende mesmo que o segredo "ocorre envolto na possibilidade e na tentação da revelação", a qual se assemelha a atração do abismo. Mas por que um jovem decide pela revelação não autorizada de um segredo de Estado, se aproximando do abismo e assumindo o risco da queda? Porque para ele ou ela a contradição entre os valores que aprendeu na sociedade e os que

encontra nos documentos classificados são intoleráveis; ele encarna, como num tipo social simmeliano, uma tensão social mais geral (Simmel, 1987). Talvez outros tenham aceito a contradição sem desconforto, ou não estejam dispostos ao sacrifício. Talvez sintam como obrigação continuar trabalhando sem pensar em sua missão maior que é iniciar o ritual de reparação entre Estado e sociedade. O jovem divulga as informações, e preferencialmente se expõe ao público, mas pode também delegar essa função a um patrono, como um jornal de prestígio ou um órgão público independente.

E aí a parte mais interessante do vazamento acontece: a reação pública e estatal. Como o jovem será retratado? Sua personalidade é exposta em praça pública, como os pedaços esquartejados de nosso herói Tiradentes. Quem é, de onde vem, quais as motivações políticas, mas especialmente, que dramas pessoais o movem? Isso é parte importante do vazamento; em sociedades arcaicas o objeto do sacrifício, humano ou animal, é cuidadosamente escolhido e examinado. Examina-se também o objeto do vazamento e suas consequências e aí a sociedade dá um veredicto: há de fato algo roto, e será necessário então um ajuste subsequente de ações e expectativas, com implicações legais? Ou trata-se de uma vingança pessoal apenas, de resultado da insatisfação profissional do denunciante? A burocracia optará por essa última interpretação, mas a estratégia tende a não ser bem sucedida, pois a sociedade não se importa com questões internas ao trabalho burocrático.

Foi traição? Esse sim é um risco grande que o *whistleblower* corre, o de ser visto como traidor. Nos casos Vanunu e Anat Kamm de vazamentos de informações militares em Israel, por exemplo, a esfera pública não viu a necessidade de remendar qualquer relação; o conteúdo das revelações não causou impacto na população, para quem o Estado agia de acordo com o esperado. Como na ordália medieval, o julgamento por provação, o *whistleblower* deve sobreviver ao debate público; o ritual o exige. É sua capacidade de sair ileso da fogueira que vai determinar em larga medida o resultado final do vazamento. Refugiar-se em outro país não conta; mesmo que pareça fazer sentido buscar um porto seguro, isso enfraquece o vazamento enquanto instrumento de comunhão entre Estado e sociedade. O *whistleblower* deve ficar e se apresentar ou ao menos buscar um patrono visível que o represente; se a situação é tão dramática que ele não vê chances de ser compreendido pela esfera pública, então não há por que esperar que o vazamento tenha algum efeito interno. O vazamento nesse caso servirá aos inimigos sem efeito no país.

Veja que diferentemente do ritual sacrificial arcaico, esse de que falamos se dá em torno de um público mediado, ou seja, um público que participa do ritual

através dos meios de comunicação à disposição, seja a imprensa escrita alimentada pelo correio, telégrafo e telefone, os meios de massa como o rádio e a televisão e também o cinema, ou mais recentemente a televisão em escala global e a internet, com seu enorme potencial de comunicação em rede. A imolação é pública e nacional, porém não presencial; são rituais mediados, muito semelhantes aos eventos mediados descritos por Elihu Katz e Daniel Dayan (Dayan e Katz, 1994), tais como competições esportivas, encontros de dignitários ou debates televisivos. Se fazemos mesmo parte de uma aldeia global, como diz McLuhan, não é tão absurdo pensar que alguns rituais se estendam até onde os meios de comunicação alcancem. Katz lembra que os indianos acompanharam o funeral de Indira Gandhi pela TV de modo solene e vestindo-se sobriamente e nas eleições de 2014 no Brasil o público dos debates televisivos exaltou, criticou, apoiou e debochou dos candidatos pelo Twitter como se todos compartilhassem do mesmo espaço e pudessem ser ouvidos uns aos outros.

Ao contrário dos mencionados eventos mediados, o ritual do vazamento não tem hora para começar nem é acordado com antecedência com os meios de comunicação de massa; além disso, não é um evento pontual; ele se espalha no tempo. Mas como estes, ele é acompanhado pelo público como participante e testemunha, também segue um rito próprio e seu desenrolar tem impacto sobre a situação anterior. Algo está em jogo quando alguém vaza uma informação. Ou seja, inquirindo e execrando o *whistleblower*, defendendo os interesses de Estado ou clamando por mudanças urgentes, somos todos parte desse ritual mediado. Somos nós, em última instância, em sociedades democráticas, que determinamos se o vazamento é um mero crime ou uma ação transformadora, independentemente do processo legal que o agente da revelação sofra. Pois é possível, ainda que improvável, que o alardeador seja preso e ainda assim transforme; ou que ele seja absolvido, mas não mude nada.

## VAZAMENTO E SEGREDO NA ERA DA INTERNET

■ Em uma estação de trabalho, no interior da base do exército, com dois computadores conectados às redes sigilosas e sem supervisão, o soldado Bradley Manning foi capaz de, sem dificuldades e muito rapidamente copiar enorme quantidade de dados sigilosos para mídias portáteis, os quais seriam, posteriormente, oferecidos a Julian Assange, fundador da organização Wikileaks, e logo tornados amplamente públicos. Condenado pela justiça como traidor da nação ele deve cumprir muitos anos de prisão. O contraste em relação ao caso dos Papéis do Pentágono

é evidente. Daniel Ellsberg, o herói inocentado, era um estrategista de prestígio trabalhando para o Pentágono, e guardava em um cofre em sua sala na RAND Corporation uma das poucas versões impressas do estudo ultrassecreto que inclusive ajudara a produzir. Uma vez decidido a vazar as informações, Ellsberg teve então de superar vários desafios, sendo o primeiro o de copiar uma por uma as sete mil páginas do documento, tendo de recorrer a uma máquina de xerox, invenção ainda recente à época.

Daniel Ellsberg teve de passar mais de um ano copiando os documentos fora de seu horário de serviço, correndo o risco de ser pego a qualquer momento. Segundo ele, não se andava com documentos ultrassecretos pelos corredores da Corporação a não ser indo ou voltando do Gabinete de Controle de Documentos Ultrassecretos. Esses arquivos não poderiam ser deixados em cima de mesas, ou mesmo trancados em cofres para arquivos secretos: só poderiam ficar fora do alcance da visão daqueles que tinham sua guarda caso trancados em cofres especiais para arquivos ultrassecretos, que poucos possuíam (ELLSBERG, 2003, p. 307).

Já o depoimento do soldado Bradley Manning, que passou apenas sete meses na Estação Operacional de Contingência Hammer, no Iraque, é muito distinto. Para Manning, o vazamento realizado por ele havia sido facilitado por uma série de fatores físicos, técnicos e culturais: "Eu entrava com um CD-RW de música (...), apagava as músicas e gravava um arquivo dividido e comprimido. Ninguém suspeitava de nada. Era meio triste" (Leigh; Harding, 2011, p. 93). Tamanha facilidade levou ao maior vazamento de informações sigilosas da história, que expôs centenas de milhares de segredos militares e diplomáticos dos Estados Unidos da América. Mas em face dessa quantidade massiva de informações, muito se disse sobre a alegada obviedade e irrelevância de suas revelações. Críticos do Wikileaks se apoiaram no argumento de que os documentos não revelavam grandes irregularidades ou aspectos condenáveis da política externa americana, não sendo, assim, de interesse público.

A ponderação sobre a relevância ou real sensibilidade das informações vazadas é de fato pertinente. Deve-se ter em vista que, seguindo um padrão mantido desde os tempos da Guerra Fria, somente entre 3 e 5% das classificações originais do sistema americano de proteção aos segredos de Estado se dá na categoria "top secret", sendo os demais 95% divididos de forma mais ou menos equilibrada entre as categorias de menor sensibilidade, e que dessas informações grande parte é classificada indevidamente. Desse modo, não surpreende que parte significativa dos telegramas vazados pelo Wikileaks seja composta por segredos burocráticos,

em última análise, mantidos porque são úteis, por permitirem a preservação da atividade diplomática, suas fontes e métodos, e não pela importância de seus conteúdos. O fato é que importantes segredos políticos também foram revelados: infrações aos direitos humanos, corrupção, espionagem. Isso, no entanto, não impediu que o impacto do vazamento fosse muito relativizado e que seu sucesso enquanto ritual seja questionável, principalmente se comparado ao caso dos Papéis do Pentágono.

O Wikileaks como uma rede transnacional de indivíduos unidos pelo ideal da transparência, voltados contra o segredo de governos e grandes corporações, que, como entendem, permite más condutas cujas consequências se refletem globalmente, seria fruto de um contexto de ascensão de esferas públicas globais, e, além disso, consistiria em uma de suas expressões mais significativas. Essas esferas públicas globais, engajadas em monitorar e influenciar o exercício do poder no cenário global, senão em exercê-lo, contribuem para a ascensão de uma demanda mais incisiva por transparência, que se não atendida, pretende ser imposta na forma de novos vazamentos. Ponderamos, porém, que a associação entre transparência e racionalização, moralização do exercício do poder só é verdadeira quando a perspectiva da revelação é capaz de instar o agente público a uma auto-regulação, a qual, quando não suficiente, seria complementada por uma regulação *a posteriori* derivada dos constrangimentos da opinião pública. No caso de banalização do vazamento, com o descrédito do público em relação às informações reveladas, esse potencial de moralização, racionalização, ou de recomposição entre Estado e Sociedade, se perde.

Apesar disso, transparência é de fato uma exigência do contexto da Era da Informação, e os vazamentos são cada vez mais a regra. E além de condicionar a ascensão dessas esferas públicas globais, a internet também afeta diretamente a demanda por transparência por sua própria essência enquanto meio. Como destacou McLuhan (2002, p. 23), nos adaptamos distraidamente aos meios, acatamos simplesmente seus pressupostos que configuram e controlam "a proporção e a forma das ações e associações humanas". No caso da nova rede mundial, a facilidade e instantaneidade da pesquisa e do acesso a informações, a ampliação exponencial da capacidade de armazenamento de dados e a rapidez e alcance de sua divulgação são pressupostos já assimilados por toda uma geração de usuários. E é justamente essa assimilação que condiciona a formação de indivíduos cada vez menos reverentes ante aquilo que lhes é ocultado.

Por isso, o grande desafio ao segredo hoje não advém propriamente de falhas em sistemas de classificação e proteção, mas sim de uma maior demanda por

informação associada a um estágio de desenvolvimento tecnológico que torna níveis cada vez maiores de transparência não só possíveis como também atrativos.

Bradley Manning certamente esteve ciente dos riscos associados aos vazamentos, mas, tomando por base seus próprios depoimentos, fica claro que para sua decisão pesou muito a ideia de que estava "envolvido em algo de que discordava completamente". Tivesse o soldado tomado conhecimento somente de verdadeiros segredos de segurança nacional, ou mesmo de segredos essencialmente burocráticos, produzidos aos montes por diplomatas e oficiais de inteligência, a motivação para revelar os segredos não seria a mesma, ou sequer existiria. Foram os segredos políticos, aqueles que uma vez conhecidos despertaram em Manning a noção de estar sendo cúmplice da conduta, segundo ele, condenável de seu governo. De fato, quatro décadas antes, os segredos políticos a respeito do envolvimento norte-americano na Indochina tiveram efeito semelhante sobre o estrategista Daniel Ellsberg, e em 2013 os segredos sobre a vigilância do governo motivaram o vazamento de Edward Snowden, mais recente, que também alcançou grande repercussão.

## CONCLUSÃO

■ O vazamento de informações secretas é sempre um risco. Ele é um risco para o alardeador. É um risco para a nação, que o alardeador pesa com muito cuidado. Claro que é um risco para as burocracias que o temem e que precisam dele para manter seu controle sobre a sociedade ou meramente seus privilégios. Mas ele também apresenta risco para a delicada relação entre Estado e sociedade em países democráticos; é ao longo do processo que se inicia com o vazamento que valores a aspirações comuns serão renegociados, dependendo da reação da sociedade quanto ao vazamento e o alardeador. A imagem do Estado também será redesenhada dependendo da reação que tiver, mais enfurecida ou magnânima, com relação ao criminoso.

Além de reforçar um pacto democrático, um vazamento pode abrir uma cunha num governo autoritário hesitante, como foi o caso da publicidade internacional quanto aos mortos e desaparecidos durante a ditadura brasileira, em meados dos anos 1970. Pode também servir de pretexto para mais repressão; é um jogo fascinante, que a sociedade acompanha avidamente e sobre a qual reflete depois em estudos científicos ou na ficção. Entretanto, com a mudança na escala dos vazamentos e nos modos como eles são feitos, como vimos na parte anterior, os vazamentos podem perder esse caráter simbólico importante. Benjamin repa-

rou que a pintura nos causa um fascínio enquanto a fotografia, tão próxima a nós, nos convida a fotografar. Os vazamentos de hoje se assemelham muito a nossa própria rotina de trabalho enquanto processadores de informações, imagens e códigos. Vemos em Manning uma versão um pouco grotesca de nossos enganos diante do computador, quando enviamos para um grupo enorme um email indiscreto; o vazamento massivo não se presta bem ao ritual simbólico.

Além disso, os vazamentos têm cada vez mais um caráter global, enquanto ainda prestamos atenção à nossas novelas muito nacionais, que são a base do debate público. Abarcando tudo, o Wikileaks acabou não causando enormes terremotos, pois ficou difícil para o público compreender o que estava em jogo. Essa é ainda mais uma razão para termos, ainda seguindo Benjamin, uma atenção dispersa e fragmentada com relação aos vazamentos, e não dramática e repleta de significados. É possível, entretanto, que com o tempo um verdadeiro palco global se construa e daí os vazamentos passem a ser mais interessantes, mais úteis no sentido simbólico, na construção de sociedades mais democráticas. Se estamos nos constituindo enquanto sociedade global (Alexander, 2006), também criaremos nossos rituais coletivos, adotaremos nossos heróis e nos constituiremos como público supranacional.

Enquanto isso não ocorre, diferentes sociedades, com diferentes culturas políticas, se encontram nos vazamentos globais. Sociedades democráticas, patrimoniais, autoritárias e mesmo tradicionais terão na mesma rede de informação os seus segredos mais guardados e mais alardeados. Talvez elas não sejam tão tocadas internamente por essa caixa de Pandora global que é a internet, mas sofrem de modos distintos pelas mesmas ações. Aprenderemos muito examinando como cada país enfrenta seus vazamentos, que punição o Estado reserva aos seus alardeadores e a cada tipo de alardeador, pois há em cada nação assuntos sagrados e profanos, os que devem permanecer ocultos ou os que merecem a luz do dia. Aprenderemos mais ainda quando, na mesma arena global, encontrarem-se as nações e posicionarem-se com relação ao que têm em comum, revelando o que têm de diferente. Vazamentos são então um lugar privilegiado de análise, tanto nacional, quanto global ou comparativa.

E voltamos aqui a Walter Benjamin, com seu fim triste nos Pirineus durante a Segunda Guerra. Para cada nação, aquele homem representava uma coisa distinta. Nos Estados Unidos, teria um emprego acadêmico, como Adorno ou Lévi-Strauss. Para os espanhóis, era um mero estorvo burocrático a quem deveriam ter dado passagem. Em não dando, seus escritos, inofensivos e inspiradores, ficaram sem leitores, engolidos pelo totalitarismo em voga. É a metáfora perfeita

para os segredos globais. Alguns querem que passem sem deixar rastro, outros os neutralizam publicando em artigos assépticos que ninguém lê. Mas outros ainda os temem e só descansam com sua eliminação, cada vez mais complexa. Cabe a nós conhecer, se não o conteúdo total do que é secreto, ao menos seus significados nessa sociedade global e mediada.

HELOISA PAIT foi bolsista da Comissão Fulbright e é professora de sociologia da comunicação da UNESP. Sua tese de doutorado, defendida na New School for Social Research, investiga os desafios individuais da comunicação mediada, tema que examina em seus estudos sobre o diálogo político nacional e global. Heloisa participa do debate público com contribuições para Panoramas, Estadão Noite, Quartz e Simon's site.

RUAN SALES DE PAULA PINHEIRO é mestre em Relações Internacionais pela UNESP. Sua pesquisa de mestrado, fomentada pela CAPES e pelo CNPq, investigou por uma perspectiva histórico-comparativa a dinâmica entre segredo e transparência no Brasil e nos Estados Unidos, com atenção especial à política externa. Ruan Sales colabora com Estadão Noite, Jornal Unesp e Revista Unesp Ciência.

## FONTES DOCUMENTAIS

BRASIL. Ministério dos Negócios Estrangeiros. Decreto de 15 de maio de 1834. 1º Regimento das Legações de Sua Majestade o Imperador do Brazil. Rio de Janeiro, RJ, 1834. Disponível em: <//books.google.com.br/books?id=Wgc6CliZ6d4C&dq=1º+Regimento+das+Legações+de+Sua+Majestade+o+Imperador+do+Brasil&hl=pt-BR&source=gbs_navlinks_s>. Acesso em: 6 jan. 2015.

BRASIL. Secretaria d'Estado dos Negócios Estrangeiros. Decreto nº 135, de 26 de fevereiro de 1842. 1º Regulamento da Secretaria de Estado. Rio de Janeiro, RJ, 1842. Disponível em: http://www2.camara.leg.br/legin/fed/decret/1824-1899/decreto-135-26-fevereiro-1842--560860-publicacaooriginal-84071-pe.html>. Acesso em: 6 jan. 2015.

BRASIL. Secretaria d'Estado dos Negócios Estrangeiros. Decreto n.º 2.358, de 19 de dezembro de 1859. Disponível em: <http://www2.camara.leg.br/legin/fed/decret/1824-1899/decreto-2358-19-fevereiro-1859-557269-publicacaooriginal-77613-pe.html>. Acesso em: 6 jan. 2015.

BRASIL. Decreto nº 4.743, de 31 de outubro de 1923. Regula a liberdade de imprensa e dá outras providencias. Rio de Janeiro, RJ, 1923. Disponível em: <http://www2.camara.leg.br/legin/fed/decret/1920-1929/decreto-4743-31-outubro-1923-567758-publicacaooriginal-91090--pl.html>. Acesso em: 6 jan. 2015.

## BIBLIOGRAFIA

ARENDT, Hannah. *Entre o passado e o futuro.* 5. ed. São Paulo: Editora Perspectiva, 1968.

ALEXANDER, J. Global Civil Society. *Theory, Culture & Society*, v. 23, n. 2-3, p. 521-524, 2006.

BENJAMIN, W. The Work of Art in the Age of Mechanical Reporduction (ed.), *Illuminations: Essays and Reflections.* English Language. New York: Schocken Books, 1968.

BLANTON, T. S. *National Security and Open Government in the United States:* Beyond the Balancing Test. In: National Security and Open Government: Striking the Right Balance. Syracuse, New York, Campbell Public Affairs Institute, 2003. p. 33-73.

BLEDSOE, C. H.; ROBEY, K. M. Arabic Literacy and Secrecy Among the Mende of Sierra Leone. *Man,* v. 21, n. p. 202-226, 1986.

BLONDHEIM, M.; LIEBES, T. Archaic Witnessing and Contemporary News MediaIn: Frosh, P.; Pinchevski, A. (eds.), *Media Witnessing: Testimony in the Age of Mass Communication.* Basingstoke, Palgrave Macmillan, 2009.

BOBBIO, Norberto. *Dicionário de Política.* Brasília, UNB, 1999.

CANETTI, Elias. *Massa e Poder.* 2. ed. São Paulo: Companhia das Letras, 2005. p. 290-296.

CEPIK, Marco. *Espionagem e Democracia.* Rio de Janeiro: Editora FGV, 2003.

DAYAN, D.; KATZ, E. *Media Events: The Live Broadcasting of History.* Harvard University Press, 1994.

ELLSBERG, Daniel. *Secrets:* a Memoir of Vietnam and the Pentagon Papers. New York: Viking, 2003.

FAORO, R. *Os donos do poder.* Porto Alegre e São Paulo: Globo e EDUSP, 1975.

LEIGH, D.; HARDING, L. *Wikileaks* – A Guerra de Julian Assange Contra os Segredos de Estado. Campinas: Verus, 2011.

MANZUR, T. M. Opinião pública e política externa do Brasil do Império a João Goulart: um balanço historiográfico. *Revista brasileira de política internacional,* v. 42, n. 1, p. 30-61, 1999.

McLUHAN, M. *Os meios de comunicação como extensões do homem.* 12. ed. São Paulo: Cultrix, 2002.

MOYNIHAN, D. *Secrecy:* the American Experience. New Haven: Yale UP, 1998.

SIMMEL, G. The Sociology of Secret and of Secret Societies. *The American Journal of Sociology*, v. 9, n. 4, p. 441-498, 1906.

_____. Social Types In: LEVINE, D. N. (ed.), *On Individuality and Social Forms.* Chicago: The University of Chicago Press, 1987.

SCHWARTZ, S. The Mysterious Death of Walter Benjamin. *The Weekly Standard,* v. 6, n. 37, p. 2001.

# Regulamentação da Web

PATRICIA PECK PINHEIRO

## REGULAMENTAÇÃO DA WEB

■ A Sociedade humana desenvolveu há muito tempo um modelo harmônico de convivência social baseado em um sistema de regras de conduta. Segundo Jean Dabin, advogado e filósofo belga, só há que se falar de uma relação legal se há uma relação social, quando existe uma sociedade organizada.

Inicialmente, estas regras eram transmitidas de forma oral, mas rapidamente o sistema evoluiu para um formato escrito e documentado. Isso porque um dos fatores principais para o sucesso de qualquer regulamentação é que a norma comportamental precisa estar clara, ser objetiva, para conseguir ser imposta a uma coletividade.

Ademais, com o passar do tempo também foi aprimorado o método de criação deste conjunto de regramentos para que fosse também socialmente aceito, legítimo, até chegarmos no cenário atual do Poder Legislativo.

A motivação para todo este desenho jurídico-social é o estabelecer um melhor relacionamento social entre os homens. A partir do momento que o indivíduo sabe previamente qual a postura recomendada, qual comportamento é esperado e desejado pela comunidade na qual está inserido, tem então o livre-arbítrio de escolher entre cumprir com a regra ou não, e no último caso sofrer com as consequências previstas, chamadas de sanção.

Sendo assim, independente do avanço tecnológico, a necessidade de se estabelecer parâmetros e limites para as atitudes humanas é uma condição para a própria vida em sociedade. A garantia das liberdades depende do cumprimento deste compromisso, deste pacto social.

Dito isso, desde a criação da Internet, uma das maiores discussões é justamente sobre a necessidade ou não de se regulamentar este ambiente que teria, em princípio, surgido, sem qualquer controle impositivo. Por certo, quanto maior o número de usuários de uma determinada ferramenta, maior a necessidade de se estabelecer um código de conduta.

Foi o que ocorreu com o automóvel, que hoje, após seu uso massificado, passou a exigir não apenas uma habilitação, ou seja, um treinamento prévio para capacitar o usuário, como também o atendimento a um conjunto de normas obrigatórias, que sujeitam a penalidades que vão de multa até a perda do direito de dirigir.

Então, seguindo esta linha de raciocínio, após aproximadamente 50 anos da invenção da Arpanet, que foi o embrião do mundo digital que vivemos hoje, vemos a necessidade de construir regras mais claras para seu uso ético, seguro, legal, saudável e sustentável. Mas com um novo desafio, que é a quebra do paradigma geográfico na aplicação da norma legal.

Portanto, todos os operadores envolvidos na viabilização do universo digital, materializado nas interfaces do "www", e de seus desdobramentos mais recentes até a chegada dos aplicativos, devem coordenar esforços para padronizar o que deve ser seguido por todos neste ambiente, de usuários às instituições, onde quer que estejam.

Logo, o primeiro e talvez maior desafio a ser enfrentado tem relação direta com a própria natureza da web, que é a ausência de limitação territorial. Contrariando o modelo estabelecido até então em que as leis se aplicam dentro de determinados limites geográficos, em respeito à soberania dos Estados.

Mas não é a primeira vez que vivenciamos isso, vide a necessidade recorrente de se estabelecer Tratados e Convenções Internacionais entre os países e seus cidadãos.

O primeiro passo neste sentido foi dado quando da definição do padrão de protocolo TCP/IP e criação de Comitês Gestores de Internet em todo o mundo, com a missão de articular a melhoria evolutiva da mesma, bem como os requisitos necessários para a sua interconectividade e integração.

A partir daí, o crescimento foi tão acelerado que andou mais rápido o estabelecimento de regras através de contratos privados, ou seja, criadas pelos fornecedores de serviços da Internet e traduzidas em Termos de Uso, que representam um modelo de auto-regulamentação como ocorre com o regimento interno de um condomínio, uma escola, ou um clube.

Ou seja, o primeiro avanço para regulamentação da web foi realizado pela iniciativa privada e não pelo poder instituído. Estes códigos de conduta digitais estão espalhados por toda a Internet, para tudo que se queira fazer. No entanto, ainda utilizam um formato precário de linguagem essencialmente jurídica, deixando de tomar proveito do potencial multimídia da rede que permite uma abordagem mais didática e educativa.

Afinal, uma regra que ninguém lê, logo, desconhece, tem pouca eficácia preventiva e acaba só tendo utilidade quando há um desfecho judicial. Isso fez com que, nos últimos anos, com o aumento vertiginoso de usuários, a Internet tenha se tornado um local selvagem, como se tivéssemos voltado ao estado de natureza, onde vale a lei do mais forte, ou ainda a lei de Talião, olho por olho, dente por dente, com as pessoas fazendo justiça com o próprio mouse.

Devido justamente a este caos, os sistemas jurídicos de todo o mundo iniciaram uma cruzada para elaborar e/ou atualizar as leis de modo que estas alcançassem melhor as situações e condutas surgidas com o advento deste ambiente de relacionamentos digitais atemporais e multiterritoriais.

Sendo assim, a maioria dos países passou a discutir e aprovar regras novas, mais condizentes com esta atual realidade. Em alguns casos, inclusive, foram criadas Diretivas para tratar uniformemente alguns temas mais essenciais tais como neutralidade, liberdade de expressão, privacidade, proteção de dados pessoais, crimes eletrônicos, consumidor online, comércio eletrônico, proteção de direitos autorais digitais, entre outros.

Cada país no seu ritmo, e o Brasil de forma mais lenta, promulgou leis com o objetivo de regulamentar melhor a web. Algumas bem intencionadas, outras desastrosas. Isso porque a premissa basilar da Internet tem a ver com o fato de que não é uma outra realidade, paralela, chamada de virtual, ou cibernética.

Vivemos um uma Sociedade única, e as condutas devem ser tratadas com certa equidade, quer tenham ocorrido de forma presencial ou à distância, pela via analógica ou pela via digital. E nesta última hipótese, não importa que tecnologia seja inventada para viabilizar relações e obrigações entre partes ausentes, do telex, ao telefone, ao celular, à internet.

Tratar a Internet como um mundo à parte é um dos maiores erros que pode ser cometido pelos estrategistas jurídicos. Por certo, a tecnologia trouxe algumas situações novas, ainda não previstas pelas leis existentes, pois afeta e altera o comportamento dos indivíduos.

Antes de inventarem o carro não havia o acidente de carro. Antes da internet não havia um dano causado por “bug” ou por “vírus” de computador. Muito

menos um golpe de engenharia social baseado no envio de um email falso com a pegadinha "clique aqui no link".

Apesar de toda a inovação, o que mudou mesmo foi o *modus operandi*, a forma de executar determinada ação, seja ela lícita ou ilícita, mas não os valores que devem ser protegidos por um sistema jurídico-social. Por isso, princípios gerais do direito como "a ninguém lesar", "dar a cada um o que é seu" e "viver honestamente" são ainda tão válidos e aplicáveis, não importa quanto tecnológica a Sociedade tenha se tornado.

Provavelmente, o maior efeito que sentimos hoje está mais relacionado com a capacidade de informação, ou seja, saber o que está ocorrendo pois há maior documentação e prova das condutas.

Os crimes mais recorrentes do mundo digital são velhos conhecidos dos ordenamentos jurídicos, como os crimes contra a honra (injúria, difamação, calúnia), ameaça, discriminação, falsa identidade, falsidade ideológica, fraude.

A diferença é que agora tem mais evidências da ocorrência dos mesmos. E isso, por si só, já contribui para gerar um grande sentimento generalizado de insegurança dentro da Internet.

Isto porque a partir do momento em que há prova de um ato ou fato, nasce o dever de agir. E se não há uma resposta da autoridade competente para combater a prática ilícita, cresce a impunidade, que por sua vez estimula mais ilícitos.

O maior estímulo ao descumprimento de regras, por melhor que ela tenha sido feita, é a certeza da impunidade. No caso da Internet, o que mais tem contribuído para este quesito é a possibilidade do anonimato.

Desse modo, um dos pontos cruciais no meio digital é justamente evitar que alguém possa cometer atos sem ser identificado, ou pior, realiza-los fingindo ser outra pessoa. A confiança na identidade declarada é requisito para o crescimento da própria Economia Digital.

Ademais, há dois fatores agravantes nas condutas exercidas através da internet: primeiro a sensação de distanciamento que ela causa, que faz com que os atos sejam mais covardes e cruéis; segundo a sua amplitude, que tem dimensão global e pode se perpetuar no tempo.

Enquanto uma ofensa presencial gera um efeito e tem uma duração limitada no tempo, a mesma ofensa através da internet tem um poder danoso muito maior, ilimitado e inesgotável.

Logo, simultaneamente a vontade de construir um arcabouço legal de regras e limites para a vida digital, o acesso facilitado às novas tecnologias, por pessoas

cada vez mais jovem, fez crescer o perigo desta nova "praça pública" que estimula maior convivência de pessoas, de forma interconectada em tempo real.

Para desespero do poder público, o crime organizado tomou proveito desta oportunidade da Internet ter surgido inicialmente como uma "terra sem lei" para ampliar sua atuação, o que fez surgir a "Deep Web", que seria a internet obscura, que atraiu nos últimos anos de quadrilhas de fraudadores de cartões de crédito a terroristas.

Podemos afirmar que vivemos atualmente um estado primitivo de direito na Internet. O que pode ser feito então para proteger o bem público digital? Como instrumentalizar as regras de conduta para que sejam mais eficazes na Internet e com isso garantir maior segurança para todos os seus cidadãos-internautas?

No Brasil, a importância da regulamentação da web vem aumentando, com a promulgação de leis mais específicas como a Lei de Crimes Eletrônicos (Lei 12.737/2012) e a Lei do Marco Civil da Internet (Lei 12.965/2014). Além do andamento de diversos projetos de lei, entre eles o de Proteção de Dados Pessoais.

Estas duas leis brasileiras recentes, uma com ênfase criminal e outra civil, são um bom exemplo da dificuldade de se legislar sobre matérias mais técnicas, como as que envolvem a Internet.

Ambas tiveram longos períodos de tramitação no Legislativo, envolveram consultas públicas, e ao final, recepcionaram uma redação muito tímida se comparada com a relevância das pautas abordadas, seus propósitos e objetivos.

A atualização da norma penal é essencial, visto que na interpretação da mesma pelo Judiciário não é possível ser aplicada analogia. Ou o crime está bem tipificado, ou então a conduta não será enquadrada como crime.

Ademais, há diversos crimes que quando ocorrem através do meio digital merecem uma penalidade maior, visto que passam a ser mais graves e têm consequências maiores.

Sendo assim, para haver uma boa regulamentação da parte criminal, há necessidade de se alcançar estes dois objetivos: dar o devido tratamento às condutas novas, bem como revisar a penalidade das condutas que possuem um novo *modus operandi* digital.

A Lei "Carolina Dieckmann", como ficou conhecida, após mais de 10 anos de discussão, acabou por trazer apenas 4 artigos novos para o contexto legal nacional. Dentre estes, o mais relevante foi a adequação do artigo 154 do Código Penal para tratar do crime de invasão digital (redação nova do artigo 154-A e 154-B).

Pela nova lei, passou a ser crime invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de meca-

nismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Destaque-se que o crime tem um requisito, que é a violação indevida de um mecanismo de segurança. Ou seja, se o dispositivo não estiver bloqueado, por exemplo, com uma senha, não será possível determinar que houve violação.

Este ponto foi muito discutido para que se evitasse criminalizar a conduta proveniente de um acesso não intencional. No entanto, gerou um ônus para a vítima, que é o de ter que manter a "porta fechada" do seu equipamento.

Apesar da gravidade de um crime de invasão, a pena ficou muito branda, sendo de detenção de três meses a um ano, e multa. Podendo ser aumentada de um sexto a um terço se da invasão resultar prejuízo econômico.

A penalidade maior ficou para o caso em que haja extração de dados em consequência da invasão, que foi uma forma de tratar do furto de informações sem ser no artigo tradicional de furto que é o 155 do Código Penal.

Logo, se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido, a pena ficou de reclusão, de seis meses a dois anos, e multa, se a conduta não constituir crime mais grave. Podendo ser ainda aumentada de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.

Além deste crime, a lei fez mais duas atualizações singelas no Código Penal, acrescentando ao artigo 266 a hipótese de interrupção de serviço telemático ou de informação de utilidade pública, que vem em resposta às ações de retirada de sites públicos do ar, como ocorreu com a atuação do grupo "Anonymous". E atualizando o artigo 298 para abranger no rol de falsificação de documento particular a falsificação de cartão de crédito ou débito.

Infelizmente, ficaram de fora ajustes importantes para dar melhor tratamento às condutas de fazer arquivos maliciosos, artefatos e/ou vírus de computador, bem como o de estelionato digital que ocorre mediante o uso não autorizado de dados financeiros e/ou bancários de alguém na internet e que tem sido tratado como furto mediante fraude pela falta de um melhor enquadramento.

Traçando um comparativo com outros países, o Estado da Califórnia, nos EUA, vem dando tratamento rigoroso às condutas digitais mais danosas, como é o crime de falsa identidade praticado na criação de um perfil falso ("fake") na

Internet, com aplicação de multa de U$ 1.000 dólares e prisão de até 1 ano (seção 528.5 do Código Penal da Califórnia).

No Brasil, a situação da falsa identidade está tratada no artigo 307 do Código Penal, mas é um crime de penalidade leve, detenção de três meses a um ano ou multa. Poucos são os casos em que este tipo de conduta é de fato penalizada. E quando isso ocorre, a pena acaba convertida apenas no pagamento de uma cesta básica.

A falsa identidade é considerada um tipo de crime acessório, ou seja, um crime utilizado normalmente como meio para execução de outro crime mais grave. No entanto, na Internet, o mero fato de alguém se fazer passar por outra pessoa, por si só, já pode ser extremamente prejudicial para a vítima, mesmo que seja uma "brincadeira de mau gosto".

Pessoas públicas, celebridades, autoridades, políticos, alto escalão executivo, todos têm sido vítima de perfis falsos, mesmo que a título de protesto, devemos ter muito cuidado com a forma de manifestar a opinião pois os fins não justificam os meios.

Se por um lado a web possibilita que alguém possa facilmente se passar por outra pessoa, ela também dificulta bastante a prova de autoria quando necessária para impor uma obrigação ou uma sanção.

Um dos temas que mais merecem debate para dar melhor tratamento por parte do Estado ao combate do crime digital é justamente o sobre a necessidade de aperfeiçoamento da capacidade de prova de autoria de um ato ocorrido em meio digital.

Muitos casos ficam sem solução justamente pela dificuldade de se atribuir de forma inequívoca um ato à uma identidade. Ou seja, uma questão jurídica essencial para regulamentação da web envolve justamente a definição de um padrão único de identidade digital, não apenas no âmbito nacional, mas sim internacional.

A identificação de pessoas através de fronteiras é um dos controles mais primordiais para se garantir segurança coletiva e capturar criminosos foragidos.

Além disso, deve-se padronizar o tempo de guarda das evidências eletrônicas visto que para um único evento pode ser necessária apresentação de provas coletadas e armazenadas por várias máquinas que podem estar inclusive em países diferentes.

E este foi um dos pontos abordados pela Lei do Marco Civil da Internet, na questão do tratamento de guarda de logs (registros) de conexão e navegação na web.

Por último, além de se atualizar a lei penal, deve-se também melhorar a Lei de Execuções Penais, para que fique mais adequada a questão do encarceramento do criminoso digital.

Em muitos países, este novo tipo de bandido recebe um tratamento diferenciado, visto que apenas a prisão física restritiva de Liberdade não é suficiente para segurá-lo.

Ademais, alguns novos institutos passaram a ser tratados no tocante a regulamentação da web, que tem relação direta com a proteção dos direitos essenciais do cidadão digital. Entre eles, o da neutralidade, recepcionado nos artigos 3º. e 9º. do Marco Civil da Internet.

A neutralidade na internet significa, em resumo, garantir que não haverá discriminação ou privilégio no tráfego de dados. Ou seja, não haverá uma manipulação unilateral para atender interesses de alguns em detrimento dos demais, fazendo com que os dados de um trafeguem mais rápido e com melhor performance do que os dados de outro similar.

Há que se destacar, por oportuno, que o Marco Civil da Internet, em seus artigos 4º. e 7º., inovou ao elevar o direito de se conectar a web à categoria de direito essencial para o exercício da cidadania. Isso significa que esta recente regulamentação brasileira destacou do que seriam valores e direitos fundamentais do indivíduo da Sociedade Digital.

Apesar de bem intencionada, esta nova lei esbarra em alguns entraves técnico-jurídicos ainda intransponíveis, como é a previsão do artigo 11, que determina a aplicação da lei brasileira em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, desde que pelo menos um dos terminais esteja localizado no Brasil.

Este artigo aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

Para exemplificar, isso significa que se alguma empresa, de qualquer lugar do mundo, disponibilizar um aplicativo gratuito na loja da Apple ou da Google, e o mesmo venha a ser baixado por um brasileiro, vai aplicar a lei Brasileira por um dos terminais estar no Brasil, ou mesmo por haver troca de dados a partir do Brasil.

O que traz o dever de atender as demais previsões do Marco Civil da Internet, no tocante ao idioma necessariamente ter que ser o português nos Termos de Uso

dos Serviços (contrato), bem como haver possibilidade de o usuário solicitar exclusão da base de dados se deixar de ser cliente do serviço.

Ademais, haverá o dever de guarda de evidências eletrônicas geradas na aplicação web pelo prazo de 6 meses e se a conexão for a partir de um número de IP registrado no território nacional deve ser guardada a evidência desta conexão por 1 ano.

Por certo, há princípios universais do direito que devem também estar garantidos na Internet, como o direito à privacidade e a própria liberdade de expressão. Mas o desafio maior é como fazer isso usando técnicas tradicionais de uma época anterior a toda a Revolução Digital?

O Marco Civil da Internet tratou destes princípios, já recepcionados e garantidos pela Constituição Federal de 1988, mas deu tratamento preferencial à liberdade de expressão em detrimento a proteção da honra e reputação do indivíduo, na medida em que passou a determinar que um conteúdo só possa ser removido da web com ordem judicial.

Ou seja, independente do avanço de autogestão dos serviços digitais, como as Mídias Sociais, em que há uma mediação de conflitos realizada pela própria ferramenta, a lei brasileira priorizou a permanência do conteúdo publicado e compartilhado, excetuando apenas o caso de exposição de nudez não autorizada, que enseja remoção imediata a pedido do envolvido, de forma extrajudicial.

Mas será que o Legislativo e o Judiciário estão preparados para acompanhar esta dinâmica social tão transformadora? O tempo normal de tramitação nestas duas esferas é muito superior ao que um usuário está disposto a aguardar para ter seu direito garantido (seja por lei ou por decisão judicial).

Portanto, em última instância, a tendência de regulamentação da web exige rever o próprio modelo de criação de leis e de execução das mesmas. Afinal, se as partes podem estar em qualquer lugar, a qualquer momento, como trazer a discussão da causa para uma corte que exija a apresentação presencial dos envolvidos?

Talvez tenhamos que desenvolver um modelo que permita que haja toda uma tramitação também digital. O processo eletrônico do judiciário já é um primeiro avanço neste sentido, mas como já foi dito, não será possível alcançar a eficácia necessária para impor regras de conduta na Internet se isso ficar adstrito e limitado a um país.

Lawrense Lessig, professor de Direito de Harvard, já dizia que a transparência é a principal moeda da sociedade atual e que a tecnologia deve ser utilizada para passar a regra do jogo no próprio jogo. Por isso foi um dos precursores ao criar o modelo de licenças de direitos autorais chamado "Creative Commons" no

qual os autores podem facilmente deixar descrito no conteúdo quais os limites de uso do mesmo, através de uma iconografia específica.

Além de regras claras, a web precisa de uma Justiça mais célere, na verdade, de um Judiciário totalmente digital também. Mas, mesmo com tudo isso ocorrendo, não seremos capazes de garantir uma internet mais segura e saudável para todos sem educação.

O próprio Judiciário poderia tomar mais proveito do uso de ferramentas tecnológicas que permitissem a análise de casos similares e todas as decisões já tomadas, como se fosse um Juiz digital que tem uma base de dados de precedentes e assim pode servir de orientação sobre como decidir um conflito.

Isso é importante porque o Juiz, como um ser humano, possui suas próprias convicções e dependendo da situação pode não estar a par dos princípios que devam reger a análise de uma situação concreta, ainda mais quando envolve os meios digitais, que são algo muito novo e ainda sem muitas referências.

Michael Sandel, professor de filosofia de Harvard, em sua obra sobre Justiça, traz justamente a provocação "o que é fazer a coisa certa"? Independente de eventual punição, será que aprendemos a tomar decisões baseadas em um conjunto único de valores que definem e distinguem a decisão certa da decisão errada?

Apenas para ilustrar, já tratamos do problema da falsa identidade na internet. Mas será que um pai poderia se fazer passar pela filha menor de idade para dialogar com um suposto amigo digital desta a fim de gerar flagrante de assédio ou de pedofilia?

Como ficaria então a aplicação do instituto da legítima defesa, previsto no artigo 25 do Código Penal Brasileiro, em uma situação na internet? Até onde podemos ir sem que uma medida de proteção se transforme também numa infração?

Entende-se por legítima defesa quem, usando moderadamente dos meios necessários, repele injusta agressão, atual ou iminente, a direito seu ou de outrem. Portanto, a legítima defesa ocorre quando seu autor pratica um fato típico, previsto em lei como crime, para repelir a injusta agressão de outrem a um bem jurídico seu ou de terceiros.

O futuro da regulamentação da Internet, como local onde exercemos nossa vida digital, depende diretamente do alinhamento de um rol de princípios uniformes que devem estar legitimados e ser de conhecimento de todos os seus participantes.

A partir desta base de princípios éticos é que se pode construir qualquer ordenamento legal, onde a regulamentação é apenas um meio de instrumentalizar a sociedade para que se faça cumprir o que tiver ficado combinado.

Estamos enfrentando já o dilema trazido pelas novas tecnologias de comunicação que permitem aumentar segurança mas que ferem as garantias de privacidade, vide as acusações entre diversos países sobre a espionagem digital justificada e legitimada com base na necessidade de se combater o terrorismo, mas que pode ser facilmente extrapolada para atender outros interesses escusos.

A Internet nos tornou uma aldeia global, agora precisamos construir um novo modelo integrado de autoridade que possa representar todas as culturas, povos e cidadãos que já convivem neste novo ambiente digital.

Por certo, um cadastro único de internauta seria muito útil. Mas imagine o poder deste banco de dados que pudesse associar quem é cada um e o que está fazendo na web? Quem poderia gerenciá-lo? Quais seriam os limites?

Como fazer uso do Big Data de forma ética e legal? O uso das informações dos indivíduos que estão esparsas de forma estruturada ou não em meios digitais e bancos de dados é justamente a pauta de leis e projetos de lei em diversos países, inclusive no Brasil.

A Internet avançou muito do ponto de vista econômico e social, em tudo aquilo que pode ser realizado por auto-regulamentação do próprio mercado, pela iniciativa privada. Mas a grande quebra de paradigma envolve justamente a faceta pública da mesma, que vai desde as discussões de arrecadação de tributos até de implementação de poder de polícia.

Por certo, se a privacidade é um conceito que está em transformação, o mesmo podemos dizer sobre soberania. Como redefinir este instituto em um momento do desenvolvimento tecnológico da sociedade humana em que há livre circulação de pessoas e bens através da Internet?

Como garantir acesso para todos? A inclusão digital delimita a separação entre os desenvolvidos e os marginalizados na Sociedade do Conhecimento. Mas além de incluir, temos que capacitar, educar, investir em sustentabilidade até para evitar o tão assustador apagão digital.

A Nova Ordem Digital exige um Estado bem mais articulado, que compreenda o seu real papel em equilibrar as forças que devem garantir o crescimento com fornecimento suficiente de recursos essenciais quais sejam: Energia, Telecomunicações e Tecnologia. E nesta agenda pública, o Brasil está atrasado.

Além da infraestrutura, cabe a este Estado Digital desenhar uma arquitetura jurídica internacional que permita a proteção de seus cidadãos e dos dados destes quando estiverem conectados, bem como também atualizar a grade de ensino para melhor prepará-los para esta realidade competitiva e globalizada.

Um Estado que saiba tomar proveito das ferramentas atuais de inteligência coletiva e de colaboração digital para aumentar a riqueza bem como a sua distribuição. Se estamos na Sociedade do Conhecimento, a produção criativa e a propriedade intelectual tendem a crescer de valor como insumos econômicos.

Concluindo, nesta jornada rumo ao próximo estágio da Internet, que passa a exigir uma dimensão política-jurídica mais global, teremos que enfrentar todas estas questões fundamentais para garantir segurança e bem estar social-digital, que vão desde a criação de um modelo único de identidade não repudiável, que pode ser da autenticação biométrica ou outra tecnologia que se invente até o que fazer com esta nova versão de criminoso muito mais tecnológico.

---

Dra. Patricia Peck Pinheiro é advogada especialista em Direito Digital, formada pela Universidade de São Paulo (Twitter:@patriciapeckadv), é sócia fundadora do escritório Patricia Peck Pinheiro Advogados (www.pppadvogados.com.br), da empresa de cursos Patricia Peck Pinheiro Treinamentos, do Instituto ISTART de Ética e Segurança Digital que conduz o Movimento Família mais Segura na Internet (www.istart.org.br) e apresenta o talk-show "É Legal" (www.youtube.com/programaelegal).

# O *soft power* das novas mídias nas Relações Internacionais

RAFAEL SANTOS DE OLIVEIRA

## INTRODUÇÃO

■ As mudanças no exercício do poder político contemporâneo e no processo de tomada de decisões se modificaram nos últimos anos. Atualmente, diversas questões de política internacional são discutidas por vários atores, incluindo-se a mídia internacional, apesar de as decisões finais ainda se encontrarem vinculadas às respostas dadas pelos Estados. No campo das comunicações, foram estabelecidas novas formas de se trocar informações, cultura e saber e isso também influencia o rumo das relações internacionais e de seus atores. Diante desse contexto, evidencia-se a importância de se pesquisar esses elementos e suas implicações, focalizando-se, todavia, na análise do *soft power* da mídia dentro desse novo cenário.

A mídia, sem dúvida, sempre soube influenciar, muito bem, por meio de seus discursos e práticas sociais, as relações políticas nacionais. Contudo, com o avanço das novas tecnologias da informação, o exercício do seu *soft power* se expande além das fronteiras nacionais e ganha escala global. As oportunidades que as mídias *online* alcançaram por meio da facilidade de difusão de informações por meio da *Internet*, "seja como complexo de conteúdos, seja como ambiente de conexão ou sistema de interações, devem ser vistas de modo associado às motivações dos próprios atores sociais e aos procedimentos da comunicação estabelecida entre eles" (Maia, 2002. p. 66).

Aqui, portanto, é que talvez se evidencie um aspecto importante da mídia. Apesar de o interesse político não surgir automaticamente e nem sempre as oportunidades que a *Internet* oferece serem aproveitadas, há um crescente benefício por parte da sociedade civil ao poder se beneficiar de uma comunicação cada vez

mais horizontal e interativa oferecida pelas novas tecnologias da informação. Isso permite conhecer mais adequadamente certos assuntos e suas questões específicas mas, principalmente, também poder participar ativamente do processo comunicativo como agente de informação identificado no caso dos *blogs* e redes sociais.

De qualquer forma, esse fluxo comunicativo potencializado pelas novas mídias somente ganhará ênfase junto aos processos de tomada de decisão política, se as instâncias decisórias e institucionais do Estado se mostrarem "porosas" a tais fluxos, "dispondo-se a realizar cooperativamente negociações pragmáticas" decorrentes da incorporação dessa nova interação *online* (Maia, 2002. p.66). Com isso, pode-se afirmar desde já, que a mídia, emerge como um protagonista na utilização do *soft power* para certas situações, ainda que essa mídia não seja mais aquela dos primeiros estudos dos teóricos da comunicação que acreditavam em seu poder supremo (Wolf, 2006). O grau de influência dos meios tradicionais já não é o mesmo, porém, ao mesmo tempo em que isso ocorre, as novas mídias passam a desempenhar um papel cada vez maior no deslinde de questões políticas que também ultrapassam as fronteiras nacionais.

## 1 A CONSTRUÇÃO CONCEITUAL DO SOFT POWER E SUAS IMPLICAÇÕES NO SISTEMA MIDIÁTICO GLOBAL

■ Joseph Nye, ao descrever o poder, o compara ao amor. Para ele, o poder "[...] é mais facilmente sentido do que definido ou medido" (Nye Jr, 2002-a. p. 70). Por essa razão, o autor o visualiza como sendo "a capacidade de atingirmos os nossos objetivos ou fins" (Nye Jr, 2002-a. p. 70). Lembra, ainda, que as fontes de poder estão em constante mudança, pelo fato de não serem estáticas. Observa que diante de economias "baseadas na informação e na interdependência transnacional, o poder está a tornar-se menos transferível, menos tangível e menos coercivo" (Nye Jr, 2002-a. p. 74). Dessa forma, o autor destaca que as transformações do poder ainda não terminaram, tendo em vista que o presente século assistirá a uma expansão no papel desempenhado pelo domínio da informação enquanto fonte de poder.

A contribuição teórica mais importante dada por Nye a esse artigo reside na aplicação de sua definição de poder. As suas obras são fundamentais para entender o atual estágio da política internacional contemporânea e, além disso, é a partir dessa sua concepção teórica, especialmente aquela ligada ao *soft power*, que se torna possível identificar as formas de exercício desse tipo de poder pela mídia, em especial junto às Relações Internacionais.

*Soft power* é uma expressão criada por Joseph Nye, com o intuito de descrever a habilidade política, não somente por parte dos Estados, em influenciar indiretamente o comportamento e o interesse dos demais atores das relações internacionais. Para Nye, o conceito básico de *soft power* relaciona-se com a habilidade de influenciar os outros a fazer aquilo que se deseja, sem necessidade de emprego da força bruta (*hard power*), tendo em vista que essa sempre foi a medida realista de poder predominante. O autor observa que na política mundial contemporânea é possível, e cada vez mais provável, que um "país obtenha os resultados que quer porque os outros desejam acompanhá-lo, admirando os seus valores, imitando-lhe o exemplo, aspirando ao seu nível de prosperidade e liberdade" (Nye Jr., 2002-b, p. 36).

O *soft power,* ou poder brando, dessa forma, coopta as pessoas ao invés de coagi-las (Nye Jr., 2002-b, p. 36). Em face disso, o conceito formulado por Nye, apesar de ser um conceito recente junto às Relações Internacionais, já se encontra presente em diversos discursos políticos contemporâneos. O autor observa, ainda, que o *soft power* "[...] está a tornar-se mais importante em relação ao poder duro do que acontecia no passado, à medida que a credibilidade se transforma num recurso crucial de poder, tanto para os governos como para as ONGs" (Nye Jr, 2002-a. p. 257). O autor afirma ainda que o *soft power* pode ser considerado como uma "segunda face do poder", e que isso se deve à proposta de se estabelecer uma agenda política mundial e atrair a posição de outros países no sistema internacional (Nye Jr., 2004-b. p. 5).

Para Joseph Nye, o *soft power* depende grandemente da reputação e credibilidade do ator na comunidade internacional, e também do fluxo de informações entre atores, sendo que esta forma de poder é geralmente associada à ascensão da globalização e à doutrina neoliberal nas Relações Internacionais. Além disso, o autor identifica na cultura popular e na mídia fontes de *soft power* muito influentes, tendo em vista que se trata de um tipo de poder que, em tese, pode ser compartilhado entre diversos atores (Nye Jr., 2004-b. p. 5).

Um aspecto interessante que o autor reforça é o de que o *soft power* deve ser visto como a habilidade de se moldar à preferência dos outros para aquilo que se deseja. Com isso, sustenta que as políticas adotadas com base nesse tipo de poder acabam sendo vistas como legítimas, com autoridade moral, inclusive. "O país que consegue legitimar seu poder aos olhos dos demais encontra menor resistência para obter o que deseja. [...] Se conseguir estabelecer regras internacionais compatíveis com a sua sociedade, é menos provável que tenha de mudar" (Nye Jr., 2002-b, p. 39).

De qualquer forma, Nye afirma que não se pode considerar o *soft power* apenas como sendo um poder de influência. Embora seja uma fonte de influência, o *soft power* também deve ser considerado como poder de atração. O autor justifica esse raciocínio observando que é possível exercer influência por meio de ameaças ou estabelecendo recompensas. Contudo, o *soft power* é mais que influência ou persuasão, ou ainda, a simples capacidade de movimentar as pessoas em face da argumentação.

O *soft power* expressa a "capacidade de seduzir e atrair. E, a atração geralmente leva à aquiescência e à imitação" (Nye Jr., 2004-b. p. 37). Nesse sentido, o *soft power* incentiva a cooperação, usando uma "moeda diversa da constrição e do dinheiro" ao se fundar sobre o senso de atração (Nye Jr., 2009. p.37).

Outro raciocínio interessante que o autor apresenta diz respeito à necessidade de "conversão do poder". Para ele, é necessário que o poder potencial seja convertido em poder real. A mídia, em geral, consegue fazer essa conversão com grande eficácia, tendo em vista que, diante da abundância de informação, são os meios de comunicação de massa que primeiro filtram os fatos relevantes e os transformam em notícias levando-os ao conhecimento público. Com isso, o seu poder de agir potencialmente, em certas circunstâncias, se transforma em poder real na medida em que com rapidez e eficiência obtém certas informações e as divulgam como um produto vendável de interesse global.

Joseph Nye sustenta que a capacidade de obtenção de informações e de ação a partir delas não é algo que todos os atores das Relações Internacionais consigam fazer em tempo hábil. Ou seja, em sua concepção, a informação se torna poder na medida em que ela ainda se encontra concentrada em quem a descobriu e, com isso, poderá decidir o momento de espalhá-la ou não. No caso da mídia tradicional e das novas mídias, todavia, esse processo é mais veloz, pois os novos meios de comunicação procuram sempre agir da forma mais rápida possível para comercializar essa nova informação atendendo a tendências do mercado.

Com isso, a partir da análise da alteração do comportamento dos outros, tem-se como identificar qual a capacidade de um ator realizar essa conversão do poder potencial em real. Joseph Nye destaca que é preciso "reconhecer tanto a habilidade de um país na conversão de poder como a sua posse de recursos de poder" (Nye JR, 2002-a. p. 71). As formas de conversão do poder e os meios para tanto sofrem uma influência muito forte dos atuais fluxos de informação global. "O poder na era da informação global está se tornando menos tangível e menos coercitivo, particularmente nos países avançados; todavia a maior parcela

do mundo não é constituída de sociedades pós-industriais, e isso limita a transformação do poder" (Nye Jr., 2002-b, p. 41).

Ao analisar a realidade da política externa norte-americana, Nye afirma que a revolução no campo da informação está alterando radicalmente o campo político e, consequentemente, criando dificuldades para uma atuação política plena e controlada tão somente pelos diplomatas.

Ao lembrar as palavras do filósofo Francis Bacon, de que informação é poder, Nye relembra que no século 21 cada vez mais a população terá acesso a esse tipo de poder (Nye Jr., 2002-b, p. 83-85). O que favorece essas alterações são os avanços tecnológicos na área da informática e das comunicações que, ao terem seus custos reduzidos, oferecem maiores possibilidades de processamento e transmissão da informação pelo mundo. Essa mudança nas tecnologias configura-se como uma "terceira revolução industrial" e permite, inclusive, modificações na natureza "dos governos e da soberania, aumentando o papel dos agentes não estatais e fazendo crescer a importância do poder brando na política externa" (Nye Jr., 2002-b, p. 86). Por tais razões, as perspectivas futuras indicam que

> [...] todos os tipos de governo perceberão que o controle lhes escapa à medida que a tecnologia da informação se espalha gradualmente na parte minoritária do mundo que ainda carece de telefones, computadores e eletricidade. [...] Atualmente, muitos governos controlam o acesso dos cidadãos à *Internet* vigiando o serviço dos provedores. Embora seja custoso, os indivíduos mais habilidosos conseguem driblar tais restrições, e o controle não precisa ser total para ser eficaz quanto aos propósitos políticos. Mas, à proporção que se desenvolvem, as sociedades enfrentam dilemas ao tentar proteger o controle soberano sobre a informação (Nye Jr., 2002-b, p. 93).

No início do ano de 2008, Joseph Nye publicou outra obra – *The Powers to Lead* – na qual analisa as qualidades necessárias para que um líder alcance o sucesso tendo como cenário a era da informação e suas incessantes revoluções. Para isso, o autor parte dos conceitos de *soft e hard power*, trabalhados anteriormente em outras obras, cunhando o conceito híbrido chamado de *smart power*, o que poderia ser traduzido como poder esperto ou inteligente. O autor observa que "a habilidade para combinar *hard power* e *soft power* numa estratégia eficaz se configura num *smart power*" (Nye Jr., 2008. p.43). Nye sustenta que, a partir de agora, uma grande habilidade passará a ser exigida dos maiores líderes mundiais: saber conciliar o *hard* e o *soft power*. Justifica que o *soft power* não é algo bom, por

si próprio, e que nem sempre ele é melhor que o *hard power,* pois isso dependerá do caso em análise. Saber identificar qual é a melhor estratégia faz surgir um verdadeiro líder, com poder de comando efetivo no cenário internacional (Nye Jr., 2008. p. 43-44).

Todas essas perspectivas decorrentes da visão de Nye se aproximam das análises feitas por outro teórico do poder global, Alvim Toffler. Para ele, grande parte das teorias e hipóteses sobre o poder dá a entender que "poder é uma questão de quantidade", enquanto que, no seu entendimento, o fator mais importante é a "qualidade do poder" (Toffler, 2003. p. 39). Por isso, entende que "a principal fraqueza da força bruta ou da violência, no entanto, é a sua total inflexibilidade", o que demonstra ser um poder de "baixa qualidade" (Toffler, 2003. p. 39).

Seguindo com esse raciocínio, o autor explica que a riqueza é um exemplo de poder de qualidade média, já que pode ser usada de modo positivo ou negativo, sendo, portanto, muito mais flexível do que a força bruta. O poder considerado como sendo de "mais alta qualidade", é aquele proveniente da "aplicação do conhecimento" (Toffler, 2003. p. 40).

Essa reflexão feita por Toffler se aproxima de certos pontos abordados por Nye, e demonstra que a conjugação dessas duas concepções pode ser encontrada na atuação das diversas manifestações midiáticas, nas quais a filtragem de informações relevantes e sua transformação em notícia evidencia-se um forte exemplo de poder com qualidade, cujo domínio muitos dos demais atores das relações internacionais almejam.

O grande desafio ao se admitir tal poder é também reconhecer que se vive uma grande batalha em andamento pelo controle da mídia. Segundo Ignácio Ramonet, as grandes multinacionais da informação já compreenderam que a informação não é apenas um instrumento de propaganda e que o seu controle pode trazer muitos lucros. Por essa razão, o autor sustenta que "estamos caminhando para uma situação em que um único grupo econômico controlará o conjunto da informação e decidirá sobre o que os 6 bilhões de indivíduos do nosso planeta deverão ver, e de que maneira" (Ramonet, 1999. p. 55). É em face dessa constatação que Ramonet afirma que o poder passou da esfera política concentrada, especialmente nos Estados nacionais, para um controle de mercado financeiro, grupos planetários de mídia, as infovias da comunicação, as indústrias de informática e as tecnologias genéticas.

Apesar de as informações encontrarem-se globalmente difundidas com maior facilidade, a sua produção e difusão, ainda, são utilizadas de uma forma manipulada, que ao invés de esclarecer apenas confunde.

Nesse contexto, insere-se a comunicação como mercadoria, no sentido de que se passa a perceber os grandes lucros que esta indústria pode conferir a seus proprietários. Tal valorização dá início à busca por maiores mercados por parte das empresas do ramo, levando a uma monopolização. Com isso, "a indústria da mídia não apenas se submeteu de forma cada vez mais intensa aos interesses do mercado mundial, no sentido estritamente econômico, como também aos jogos de poder que regulamentam esse próprio mercado" (Arbex Junior, 2001. p. 99).

Por isso, é importante notar, que "a forma como se dá a apropriação dos meios e tecnologias de informação pelas grandes empresas e megaconglomerados conduz a um caminho de reiteração da vida capitalista, de forma a que se mantenha o universo simbólico" (Budó, 2003). Portanto, conforme refere Margareth Steinberger, tendo em vista que a mídia "floresceu no capitalismo" fica difícil exigir a sua desvinculação a esses interesses, principalmente quando seu poder se potencializa em face dos impulsos que as novas tecnologias conferiram à informação (Steinberger, 2005. p.28).

Assim, "o estatuto mercadológico da notícia não é um fator desprezível no dimensionamento de seu papel na formação de um imaginário geopolítico social" (Steinberger, 2005. p.28). Isso porque, é dentro desse contexto capitalista que a informação jornalística ganha ainda mais valor diante da credibilidade de suas fontes e, portanto, a inserção da notícia no cenário internacional faz com que o jornalismo atinja uma "dimensão pragmática de ferramenta geopolítica" (Steinberger, 2005. p.28).

Dessa forma, o poder de "formação da opinião pública internacional e de um imaginário geopolítico social passa a fazer parte de uma barganha da mídia com os Estados, organismos multilaterais, e com uma emergente sociedade civil internacional" (Steinberger, 2005. p.28).

Diante dessas considerações, portanto, percebe-se que a teoria de Nye reconhece que o poder bruto tem resultados relativamente rápidos, em relação ao poder brando, que tem resultado e efeito em longo prazo. Contudo, isso não deve servir como impedimento para que essa espécie de poder seja cada vez mais empregada (NYE Jr., 2004-b, p. 99). Ou seja, a mídia exerce um poder junto à vida social e política internacional, mas seus efeitos somente podem ser medidos cientificamente quando são analisados os seus efeitos em longo prazo. Por essa razão, também não se deve subestimar o poder potencial que as novas mídias poderão exercer no tratamento de questões internacionais complexas, nem mesmo ignorar os movimentos de contestação ao atual padrão da mídia tradicional e seus vínculos com interesses pessoais em detrimento da informação verdadeira.

## 2 *SOFT POWER* E NOVAS MÍDIAS: COMO LIDAR COM OS FLUXOS DA INFORMAÇÃO EM FACE DO PARADOXO DA ABUNDÂNCIA?

■ Novas tecnologias como a *Internet* permitem que a comunicação e as informações fluam com muito mais facilidade. Para Joseph Nye, a *Internet* cria um sistema em que o poder da informação se distribui muito mais largamente. As informações presentes na rede podem ser acessadas em qualquer momento ou lugar e por praticamente qualquer pessoa.[1] Esse fenômeno causa, todavia, aceleração no ritmo em que as informações são disponibilizadas e buscadas junto ao ciberespaço.

Para o jornalismo, em especial, isso causou um barateamento nos custos de produção das notícias que, por outro lado, disponibilizou um estoque excessivo de informação com possibilidade (e necessidade) de atualização contínua. Segundo Margareth Born Steinberger, isso se configura como uma vantagem relativa, tendo em vista que a "informação jornalística é um produto altamente perecível em razão do seu comprometimento com o novo" (Steinberger, 2005. p. 204). Cada vez mais, há uma necessidade de se manter informado e, para acompanhar todas as transformações da vida contemporânea, é a *Internet*, com seus inúmeros sites, *blogs*, *microblogs*, etc., que age como uma fonte inesgotável de informações nos mais variados sentidos.

Essa revolução, na forma como se estabelecem as conexões planetárias, cria comunidades e redes virtuais que transpõem as fronteiras nacionais, fazendo com que "conglomerados transnacionais e os agentes não governamentais (inclusive terroristas)" tenham um papel e um alcance bem mais importante do que possuíam há alguns anos. Para Joseph Nye, isso traz uma implicação signi-

1 Nesse ponto é preciso fazer uma ressalva quanto ao acesso às informações na internet. Apesar da crescente facilidade em obter informação junto a esse meio, ainda existe um déficit no acesso à tecnologia em muitos países que afastam uma parcela significativa da população mundial desse tipo de mecanismo. Felizmente, a situação tende a mudar e há um grande esforço mundial em universalizar o acesso à internet mediante barateamento nos equipamentos e em toda a tecnologia necessária para o ingresso na internet. Todavia, o maior problema do acesso à informação reside em locais onde paira uma censura sobre o conteúdo disponibilizado na rede. Um caso recente de censura na China envolveu a empresa Google que desde a sua instalação no país em 2006 censurava certos sites a pedido do governo chinês. Contudo, em março de 2010, a empresa deixou de censurar certos sites ao transferir seus servidores de dados para Hong Kong. Com isso, a partir de agora, as buscas realizadas no Google da China (www.google.cn) passarão a ser redirecionadas para o serviço de busca hospedado em Hong Kong (www.google.hk). Dessa forma, abre-se a possibilidade de os chineses acessar a páginas, até então proibidas, como *Facebook*, *Twitter*, *Youtube*, *Google Docs* e *Blogger*. (GOOGLE, 2010)

ficativa para a política externa, pois a mesma deixa de ser campo exclusivo dos governos e abre espaço à participação dos indivíduos e das organizações particulares que, graças a *Internet*, "terão a possibilidade de participar diretamente da política mundial" (Nye Jr., 2002-b. p. 101). Além disso, o autor entende que "a disseminação da informação levará a uma distribuição mais ampla do poder, e as redes informais, [...] destruirão o monopólio da burocracia tradicional" (Nye Jr., 2002-b. p. 101).

Outro fator a ser considerado quando se analisa esse contexto, é a velocidade com que as informações circulam na *Internet*, pois isso pode significar que todos os governos no mundo "[...] terão menos controle sobre suas agendas. Os líderes políticos desfrutarão de menor grau de liberdade ao reagir aos fatos e terão que dividir o palco com outros atores" (Nye Jr., 2002-b. p. 101). Em face disso, também será necessária a adoção de um sistema de planejamento midiático, algo que não é novo na prática política internacional. Todavia, anteriormente essa era uma preocupação chamada tão somente de propaganda política, tendo em vista que o "alvo dos governos era a população interna, sobretudo o eleitorado" (Steinberger, 2005. p. 172).

A situação atual mudou essa relação e em face da globalização da informação as principais potências precisaram alargar o seu alvo de ação, visando a atingir a comunidade internacional e, com isso, "atingir a opinião pública de outros países, até mesmo como forma de influenciar seus governantes" (Steinberger, 2005. p. 172).

A *Internet* apresenta-se, portanto, cada vez mais, não como uma simples ferramenta, mas como uma extensão dos sentidos humanos e uma significativa fonte de *soft power*. Da apuração da informação até sua transformação em notícia, houve uma redução considerável no tempo necessário para a concretização desse processo, que se completa quando atinge o seu público consumidor. Por outro lado, produz-se cada vez mais informação e ao mesmo tempo isso gera mais desatenção. O volume excessivo de dados, fatos, e todo o tipo de informação que são disponibilizados para quem o deseja, causa uma espécie de bloqueio, tendo em vista que praticamente ninguém, por mais atualizado que seja, consegue manter-se atualizado em tudo o que de relevante acontece no mundo.

Diante desse excesso de informação é que talvez se justifique o rápido sucesso de novas mídias como o *Twitter, pois*, ao limitar a mensagem a 140 caracteres, acaba por exigir uma síntese nem sempre encontrada em outros meios. Porém, até mesmo essa nova mídia sofre do excesso de informação, que perde, com isso, a sua eficácia, pois não chega com a mesma força até o seu receptor.

Segundo Paulo Vaz, o excesso de informação é

> [...] particularmente transparente na internet. Duas metáforas freqüentemente usadas para descrevê-lo sinalizam que o indivíduo é a medida de toda a informação, que o excesso é relativo a cada um de nós em uma dada configuração de nossos interesses. Fala-se de dilúvio ou inundação; se navegar é o termo usado para descrever a passagem de um documento a outro, o excesso nos ameaça de naufrágio no mundo virtual. Fala-se também de sobrecarga (*overload*) de informações. A dúvida sobre a possibilidade de o imaterial pesar é rapidamente transposta pela lembrança de que a informação pressiona por agir sobre o pensamento e que o corpo deve estar presente na interface para estimular nosso senso de realidade no mundo virtual. Ironia maior: o excesso é fomentado por seu questionamento. Em 1998, havia mais de 20.000 sites na internet dedicados ao excesso de informação (Vaz, 2004. p. 190).

Joseph Nye refere que o "paradoxo da abundância" é um dos aspectos mais interessantes do poder, em face desse constante e crescente fluxo de informação que, ao mesmo tempo, gera uma escassez de atenção. "Quando confrontados com um volume excessivo de informação, é difícil saber no que devemos nos concentrar. A atenção, não a informação, passa a ser o recurso escasso, e quem adquire poder são os mais capazes de distinguir os sinais valiosos em meio à celeuma" (Nye Jr., 2002-b. p. 121).

É por essa razão que Nye justifica o aumento na procura por pessoas que consigam filtrar essa informação. Para ele, a busca por editores capazes de filtrar as informações é uma "fonte de poder para os que têm condições de nos dizer em que concentrar a atenção" (Nye Jr., 2002-b. p. 121). O autor observa que o poder "não converge necessariamente para aqueles que podem produzir ou reter a informação (Nye Jr., 2002-b. p. 121). Ao contrário da interdependência assimétrica no comércio, no qual o poder é dos que conseguem obstar ou romper os vínculos comerciais, no fluxo da informação, o poder é de quem tem capacidade de editar e validar com autoridade a informação, selecionando tanto o que é correto como o que é importante" (Nye Jr., 2002-b. p. 121).

A alternativa, portanto, para se lidar num mundo carregado excessivamente de mensagens, é acreditar em quem consegue filtrar essas informações e mostrar tão somente aquilo que merece a devida atenção do público. O problema, todavia, é em quem confiar e como confiar. Isso porque o poder depositado nesse selecionador das informações confirmará a evidência de que o *soft power* da

informação será exercido por meio do controle da agenda dos debates públicos, tendo em vista que os responsáveis por essa filtragem são os que irão decidir quais "questões terão acesso à arena internacional de debates" (Steinberger, 2005. p. 175).

A aplicação da teoria do *gatekeeper2,* sob esse contexto do *soft power* proposto por Nye, mostra-se fundamental na análise quanto à credibilidade conferida a esses selecionadores. Isso porque a função exercida por eles acabará, cada vez mais, sendo uma fonte de poder e um requisito essencial para se destacar nesse novo cenário. Conseguir se inserir no rol de selecionadores credíveis será um exercício interessante e necessário, porém, não é algo realizável para todos que o desejarem, ao menos não pelos meios tradicionais.

A mídia, contudo, é um dos atores que possui uma tendência natural a gozar da credibilidade social. Há, portanto, uma tendência de se conferir credibilidade aos tradicionais meios de comunicação que sempre tiveram destaque em suas práticas jornalísticas. A *Internet*, por outro lado, obriga que se pense como essa credibilidade poderá vir a se transferir para esse novo meio. "Nos meios de comunicação de massa tradicionais a credibilidade antecede ou acompanha o evento informativo ou de entretenimento com o qual o usuário contata. Quando alguém pensa na RTP, na TVI, na CNN, na BBC ou RAI confere-lhes um determinado grau de credibilidade. No caso da *Internet* o processo tende a ser diferente" (Cardoso, 2007. p. 302).

Gustavo Cardoso sustenta que a credibilidade na rede e o aceitar dessa nova fonte de informação precisam ser "construídos pelo usuário à medida em que interage com a informação" (Cardoso, 2007. p. 302). A análise do *soft power* potencial da *Internet* mostra-se, portanto, como algo de fundamental importância de ser compreendido, pois na *Internet* emergem, cada vez mais, outros possíveis focos de poder decorrentes de uma credibilidade que pode vir a ser construída pelas novas mídias. Essa é uma mudança que se mostra necessária, pois, apesar de existirem diversas razões que a justifiquem, a mais importante é que

2 O conceito de *gatekeeper* (porteiro) "refere-se à pessoa que toma uma decisão após uma seqüência de decisões" (Traquina, 2001. p. 68) Esse conceito foi elaborado a partir de um estudo desenvolvido pelo psicólogo Kurt Lewin em 1947, quando o mesmo analisou o processo de tomada de decisão referente à aquisição de alimentos para casa. Nessa pesquisa, Lewin apresentou a proposta de que o fluxo de informações existentes em um dado sistema passa por diversos *gates* (portões), que funcionam como filtros que permitem ou impedem a circulação de determinadas informações (Wolf, 2006. p. 180)

> [...] a televisão e os demais veículos clássicos de comunicação estão sendo desafiados pela *Internet* e por outras tecnologias que oferecem opções mais amplas de serviços de informação e entretenimento. A fragmentação da sólida audiência da televisão é apenas um exemplo dessa tendência. Outras mídias também estão sendo afetadas. Por exemplo, nos últimos anos da década de 90, a leitura de jornais diários por adultos diminuiu de cerca de 78% (índice do final da década de 40) para menos de 60% (Dizard Jr., 2000. p. 19-20).

A busca por credibilidade é uma preocupação que atinge diversos setores, desde os políticos até a mídia. Grandes redes de comunicação de massa, como a CNN, por exemplo, sentem-se ameaçadas pela mudança de foco de seus telespectadores e, com isso, com uma possível queda em sua credibilidade junto ao público e tal circunstância, segundo a teoria de Nye, seria uma perda de *soft power* indesejada.

Para responder às novas exigências da sociedade em rede, a CNN foi a emissora de televisão pioneira em agregar junto a sua prática jornalística os valores comuns na *Internet* de conciliar a informação por meio da multimídia em voz, vídeo e texto. Além disso, a CNN passou a agir fortemente junto à *Internet* para resgatar sua audiência e firmar-se com um meio credível também junto à rede (Dizard Jr., 2000. p. 72). Essas modificações, associadas a uma prática mais interativa, são consideradas como "[...] a grande esperança dos setores de mídia e de telecomunicações na sua própria reestruturação para competir no novo contexto das comunicações de massa" (Dizard Jr., 2000. p. 37). Por outro lado, também é "[...] um conceito vago, envolvendo mais promessa que desempenho" e, dessa forma, até o momento o "objetivo final da mídia interativa – aceitação em grande escala pelos consumidores – ainda está para ser concretizado" (Dizard Jr., 2000. p. 37).

Joseph Nye, ao analisar a questão da credibilidade dos selecionadores da informação (*gatekeepers*), refere que ela é uma fonte importante de *soft power*. O autor sustenta, ainda, que a credibilidade somente se alcança quando se possui uma boa reputação no cenário midiático. O maior problema é que se vive uma fase de transição, em que os grandes meios de comunicação já não possuem a mesma credibilidade que possuíam. Juan Varela, ao analisar o fenômeno das novas mídias, entende que são esses novos meios que "ensinam à comunicação de massa" que ela necessita de uma maior transparência, bem como, ser mais aberta, de forma a "exalar confiança por meio de uma conduta visível, onde tudo seja comprovado por todos" (Varela, 2007. p. 89). O autor ressalta que deve haver um

predomínio do poder suave do fato verdadeiro em detrimento à "sacralização do acesso ao secreto, ao reservado a alguns poucos" (Varela, 2007. p. 89).

Em outras palavras, enquanto as novas mídias se fundam em bases mais participativas com a sociedade, pois não dependem de manter relações políticas ou econômicas para difundir suas informações, a grande mídia tradicional, estabelecida com o intuito de obtenção de lucro, por vezes, peca ao se omitir em sua vocação intrínseca de informação verdadeira.

O problema, todavia, não se encontra resolvido, pois na *Internet* a confiabilidade também não emergiu com total segurança, e, portanto, ainda é um obstáculo para se afirmar que as novas mídias gozam de uma credibilidade mais efetiva em comparação à mídia tradicional. Diante da facilidade de se introduzir novas informações na *Internet* não se pode identificar em muitos casos se o que está na rede é verdadeiro ou não.

Nilson Lage destaca que, *a priori*, não é possível identificar se uma informação impactante, por exemplo, "resulta de um trabalho sério" ou se é uma "mera especulação ou fantasia" (Lage, 2001. p. 157). Por tal razão, o autor enfatiza a importância de se identificar a que tipo de categoria o *site* com a informação encontrada na *Internet* pertence (Lage, 2001. p. 157). Identificando-se a qual categoria pertence, ainda assim, antes de realizar qualquer juízo de valor ou tomar alguma decisão de transformar uma informação em notícia, o autor sugere que se localize a instituição provedora para que se informe sua credibilidade.

Dentro desse contexto, a informação noticiada também sofre outro efeito dos tempos modernos, ou seja, o excessivo fluxo de informação pode causar a sua efemeridade acentuada. As notícias e os acontecimentos relevantes somente permanecem com esse *status* enquanto conseguirem atrair a atenção de um público considerável. Na medida em que outras "novas" informações são publicizadas há um deslocamento na atenção para outro foco e o problema até então noticiado "deixa de existir" e é como se tivesse "desaparecido".

Aqui se pode visualizar bem um exemplo do paradoxo da abundância, pois a própria *Internet* que gera esse ciclo avançado de "renovação" das notícias e de acontecimentos, também auxilia na preservação dessa informação para aqueles que tenham interesse em consultá-la futuramente junto à rede. Assim, apesar de certos fatos terem saído das manchetes dos jornais, poderão ser consultados sempre que necessário, ao contrário das notícias presentes em jornais tradicionais que após alguns dias já são descartadas totalmente da vida de seus leitores.

Esses aspectos da velocidade na produção e renovação das notícias tem sido uma constante em diversos episódios políticos, econômicos, internacionais e na-

cionais dos últimos tempos, afetando sensivelmente a forma como todo o processo produtivo das notícias é realizado. A figura isolada do selecionador de informações acaba sendo desafiada constantemente, pois se dificulta cada vez mais o processo de decisão entre o que será ou não notícia e de que forma ela será apresentada.

A mídia nesse cenário em que a informação é poder exerce um papel importante apesar de alguns de seus setores, como o jornalismo, encontrarem dificuldades para lidar em meio a tantas informações. É nesse ponto que a figura do *gatekeeper* precisa ser retomada, pois ainda é uma figura importante, tendo em vista que para a mídia tradicional o excesso de informação gera uma necessidade de seleção obrigatória e não há espaço para tudo aquilo que aconteceu, somente o que for relevante e que, seguindo os valores-notícia, em tese, interessarão ao público que comprará essa informação com um produto-notícia.

Gustavo Cardoso confirma essa importância atribuída ao *gatekeeper,* referindo que "aquilo que os jornais, rádio e televisão oferecem é credibilidade ou, se preferirmos, a verdade" (Cardoso, 2007.p. 198). Porém, destaca o autor, para que essa credibilidade exista é necessário que alguém a assegure e verifique se a informação noticiada é correta. O autor entende que na "maioria dos casos o usuário não possui habilidade para isso na World Wide Web, necessita de alguém que valide a informação" (Cardoso, 2007.p. 198). O papel da *Internet*, ainda para o autor, talvez torne mais difícil a identificação das informações verdadeiramente úteis e sobre as quais se deve, necessariamente, atribuir confiança e dedicar a atenção. Para Gustavo Cardoso, a *Internet* conduz a uma perda do

> [...] filtro das instituições ou, pelo menos, obriga-nos a repensar a necessidade de construir novos filtros e também a desenvolver filtros individuais. Daí que a argumentação sobre o acesso à informação tem de levar em conta que, de fato, podem existir notícias demais e que a única forma de assegurar o acesso à informação útil é dizimá-las (isto é, aplicar critérios de filtragem positiva e negativa escolhendo uma opção entre cada 10). Só que essa filtragem implica igualmente o conhecimento dos mecanismos que produziram a informação, o que nos leva à discussão sobre as habilidades necessárias. [...] A existência de abundância de informação não constitui uma garantia de sua utilidade social, pois deve-se possuir os conhecimentos necessários para agir como filtro de informação, saber distinguir e selecionar, ou o acesso a toda essa informação será inútil (Cardoso, 2007.p. 120-121).

Esse raciocínio de Gustavo Cardoso conduz a uma análise sobre a forma como a informação é buscada e filtrada na *Internet*. Uma tendência existente junto à rede é partir em busca de informações a partir de algum *site* que faça essa busca. Os *sites* com mecanismos de busca, portanto, afiguram-se como os grandes portões da informação na *Internet* pois atuam como o primeiro elemento filtrante de tudo aquilo que consta na *Internet*. Esse é o caso do *site* Google, que se firmou como um maior *site* de buscas no mundo. Mas, como esse processo pode influenciar nos fluxos de informação e no estabelecimento de fluxos de poder junto ao cenário internacional? O *Google* mediante um complexo sistema de avaliação dos inúmeros *sites* existentes na *Internet* apresenta uma listagem que se baseia, principalmente, no reconhecimento que os *sites* possuem pelos próprios usuários e na credibilidade da fonte.[3]

Com isso, evidencia-se um fenômeno interessante, pois os primeiros resultados das buscas são, geralmente, os resultados que os usuários da rede se satisfazem. Ou seja, normalmente, quem procura algo no Google se atém tão somente aos 25 primeiros resultados e ignora os demais (Cardoso, 2007, p. 297-298). Isso gera um fortalecimento naquelas fontes listadas em primeiro lugar e um afastamento daquelas que estão mais abaixo no grau de relevância, ou como refere Cardoso, a utilização de classificações de "*ranking* de popularidade para escolha de resultados, para apresentar em buscas, tende a tornar as páginas já populares mais populares e as menos populares cada vez menos visíveis" (Cardoso, 2007, p. 299).

Emerge, assim, a figura do *Internet gatekeeper* ou *gatekeeper digital*. Dessa forma, os mecanismos que efetuam as buscas na *Internet* acabam por desempenhar "a função de decidir a informação relevante para a entrada digitada pelo usuário" (Cardoso, 2007, p. 296). O autor destaca, portanto, que estar disponível na *Internet* não pode ser considerado sinônimo de estar acessível ao usuário pois "mesmo que o leitor saiba o que pretende encontrar, fica dependente das escolhas dos produtores de informação, dos criadores dos mecanismos de busca e das equipes de marketing, dos próprios mecanismos, que especificam critérios de apresentação dos resultados" (Cardoso, 2007, p. 300).

Apesar de essa postura mostrar-se coerente com a realidade, também se deve ponderar se não existe certo exagero em minimizar a capacidade interpretativa dos

3 "Existe uma clara noção dos diferentes tipos de critérios objetivos que caracterizam o funcionamento dos mecanismos de busca. Normalmente o critério pode ser de três tipos: popularidade do link (presente, entre outros, no Google), características da página e análise de conteúdo. [...] Cada método tem a sua razão de ser e há mecanismos de busca que usam apenas um ou que combinam vários" (Cardoso, 2007, p. 297-298).

usuários da rede. Pierre Lévy sustenta que "nenhuma autoridade *central* garante o valor das informações disponíveis no *conjunto* da rede" (Lévy, 1999. p. 243). O autor entende que a confiabilidade do material na rede pode em primeiro momento ser atribuído pela identificação dos seus responsáveis, pessoas ou instituições que "assinam suas contribuições e defendem sua validade frente à comunidade dos internautas. [...] As comunidades virtuais, fóruns eletrônicos ou newsgroups são freqüentemente *moderados* por responsáveis que filtram as contribuições de acordo com sua qualidade ou pertinência" (Lévy, 1999. p. 243). Porém, o fator que deve ser levado em consideração é que existe em funcionamento na *Internet* "uma espécie de *opinião pública"* (Lévy, 1999, p. 243). Ou seja, para o autor o controle sobre a qualidade da informação pode ser feita pelos próprios usuários e não tão somente pelos mecanismos de busca tal como sustentado por Cardoso. É claro que Pierre Lévy se questiona se o "caráter diluviano da informação e da comunicação no ciberespaço" não gera "um caos e colocam em desvantagem aquelas pessoas desprovidas de "fortes referências pessoais ou sociais" (Lévy, 1999, p. 244). O autor, por sua vez, mantém um forte otimismo de que, apesar do excessivo fluxo informacional desorganizado, isso não impede que as pessoas se orientem e se organizem por conta própria.

Em face dessa divergência de concepções, que não são restritas aos dois autores em discussão, mostra-se necessário, portanto, questioná-las mediante análise conjunta de outra figura emergente no controle das informações presentes na rede: o *gatewatcher*. A inclusão desse novo intermediário do processo de divulgação das informações na rede, permite que se chegue a um meio termo entre a proposta de autonomia plena dos usuários da rede e o controle total do processo de seleção nas mãos dos *gatekeepers*.

Atualmente existe uma tendência cada vez mais forte de que o próprio usuário da *Internet* também figure como um selecionador de informação, a exemplo do que ocorre com os *blogs*. Essa atuação não ocorre somente no sentido do que entra ou não no "portão" (lembrando aqui que os *gatekeepers* são considerados os guardiães do portão da informação), mas sim no sentido de organizar essa informação para os demais usuários da rede. Por essa razão, a figura do *gatewatcher* é tida como a de um bibliotecário que auxilia nesse processo, sem, contudo, definir qual a leitura que o usuário que o procura deverá realizar. O papel que cada *blog* exerce na *Internet* faz com que se possa afirmar que cada *blogueiro* possui um *soft power* potencial muito grande.

De qualquer forma, é necessário também reconhecer que certos fatores farão com que essa influência seja exercida com maior ou menor intensidade, sendo

que um dos mais relevantes é o da credibilidade do agente. Por outro lado, o simples exercício descentralizado desse papel de *gatewatcher* já permite que se concorde com o otimismo de Lévy ao perceber que existe, ainda que em gestação, um aumento na preocupação junto à rede relativos a certos problemas sociais e que a *Internet* potencializa essa consciência. Porém, deve-se frisar novamente, que se está diante de uma nova roupagem para o *gatekeeper*, que não deixa de existir, tão somente passa a compartilhar com outros usuários da rede essa tarefa de filtragem. Além disso, há outro aspecto muito bem reconhecido por Lévy de que apesar de existirem oportunidades de interação e reflexão individual sobre a informação presente da rede nem sempre ela é aproveitada adequadamente. De qualquer forma, as redes virtuais poderão mudar muitas das bases sob as quais estão estabelecidas as atuais relações de poder político. Basta relembrar a forma como as interações políticas durante certos acontecimentos excepcionais ou em situações como eleições se desenrolam por meio das mídias sociais e de fenômenos como *Twitter* e *Facebook*.

Independentemente de quem venha a exercer esse papel de guardião da informação (*gatekeeper*) ou organizador da "biblioteca" (*gatewatcher*), um problema que o excesso de informação também traz é o da necessidade de constante atualização, principalmente das notícias, para que o *soft power* dos responsáveis por esse processo não venha a ser reduzido. Os padrões das notícias internacionais, em especial, exigem uma síntese adequada dos fatos e uma estética visual construtiva da informação que prendam a atenção do usuário. A busca pelo novo e o fetiche pela velocidade, faz com que, reconhecidamente certas questões políticas internacionais, por exemplo, nem sempre encontrem um grande espaço na atenção do público se não vier acompanhada desses atributos.[4]

Joseph Nye reforça a tese de que o *soft Power* exercido pela mídia, ao captar a atenção das pessoas em prol de um determinado ideal, mostra-se essencial para enfrentar certos problemas de alcance global. Segundo o autor, para se lidar com "[...] as alterações climáticas globais, o poder militar é simplesmente incapaz de gerar sucesso e, às vezes, o seu emprego pode ser contraproducente" (Nye Jr.,

4 Por outro lado, convém destacar que, no momento em que esses elementos são atendidos e o público se vê atraído pela informação política veiculada na mídia o seu papel de ator internacional se agiganta. Conforme refere Margareth Steinberger, "a mídia configura-se, assim, como um campo preferencial na batalha das ideologias geopolíticas. Seu papel na formação de uma opinião pública internacional revela-se cada vez mais importante, como bem mostra a atual mobilização contra a guerra do Iraque através de passeatas e demonstrações populares em todo o mundo. Sem a mídia, tais movimentos não encontrariam tão rápida e eficazmente seu espaço de disseminação." (Steinberger, 2005. p. 27).

2002-b. p. 19). Justamente por isso, é que as fontes de *soft power* precisam se potencializar e agir para focalizar a atenção da opinião pública para problemas complexos. Existem, porém, dúvidas sobre como atuar frente a essa situação. Nye se questiona justamente sobre como se deve agir "nesta época de poder e perigo sem paralelos" (Nye Jr., 2002-b. p. 21). O autor questiona como "conseguiremos aprender a usar os poderes duro e brando numa combinação produtiva [...] para enfrentar outros problemas da era da informação global?" (Nye Jr., 2002-b, p. 21).

As respostas a essas indagações requerem uma consciência de que o problema precisa ser discutido globalmente, tendo em vista que em face do "[...] crescimento das redes mundiais de interdependência – não cessa de acrescentar novos itens à nossa agenda nacional e internacional" (Nye Jr., 2002-b. p. 17). Ou seja, é preciso saber utilizar as novas oportunidades que as tecnologias da informação associadas às atuais interações propiciadas pela mídia global oferecem.

Conforme refere Armand Mattelart, a "interdependência obriga a pensar o mundo como uma unidade interconectada. A força pura torna-se obsoleta diante dos problemas complexos das sociedades contemporâneas. A 'diplomacia das redes' substitui a 'diplomacia dos canhões'. Do diagnóstico sobre o estado das relações internacionais à prova da mudança técnica, o geopolítico infere a necessidade um global *political planning*" (Mattelart, 2002. p. 102).

## CONCLUSÃO

■ Os atuais ensaios sobre o papel da mídia na vida política nacional e internacional apontam para a constatação de que a comunicação apresenta-se como outra face do poder – *soft power* –, sendo identificada por meio da persuasão de ideias, culturas, valores, contrapostos ao poder das armas e dos meios de coerção física. Partindo desse pressuposto, as considerações teóricas presentes no presente artigo permitem afirmar que a mídia afigura-se como importante ator do cenário internacional. Percebe-se que, por meio do exercício de um *soft power* – poder brando –, a mídia vem ampliando a sua capacidade de influenciar os demais atores no enfrentamento de certos temas internacionais. As noções de *soft power* aplicadas à mídia permite concluir que as novas tecnologias da informação e comunicação ganham cada vez mais expressão, ao mesmo tempo em que também precisam enfrentar novos desafios. Dentre eles, está o de se lidar com o aumento no fluxo da informação e o surgimento do paradoxo da abundância. Porém, é justamente nesse momento que se confirma o *soft power*

da(s) mídia(s) ao se estabelecer como um ator capaz de filtrar o excessivo fluxo de informações contemporâneas e apontar em qual informação se deve concentrar a atenção. Como lembra Joseph Nye, o poder na era da informação global é de quem consegue exercer com habilidade a tarefa de filtrar o que é relevante e validar essa informação segundo seu entendimento e, dessa forma, expor essa sua visão aos demais, convencendo-os de segui-la também. Essa é a essência do *soft power* que ficou demonstrada que é muito bem exercida pela mídia em sua concepção tradicional e com uma crescente vocação em sua concepção virtual. Uma dessas explicações para tal afirmação se deve ao fato de a mídia, apesar de alguns percalços, ainda goza de uma credibilidade significativa junto à sociedade, sendo responsável pela formação da própria opinião pública nacional e, por vezes, até internacional. A *Internet* começa a se abrir também como uma nova arena para novos atores também adquirirem credibilidade e passarem influenciar a tomada de decisões políticas, apesar de se constatar que esse processo ainda não se encontra plenamente consolidado.

Em síntese, percebe-se que a *Internet*, em especial, propicia uma interligação entre as mais diversas mídias e isso favorece e amplia o espaço de discussão social de certos problemas. Por outro lado, o atual contexto midiático aponta para uma perda da credibilidade das mídias tradicionais e um deslocamento gradual, mas constante, do foco das atenções para as mídias *online*. Apesar de jornalismo *online*, os *blogs* e as redes sociais na *Internet* ainda se constituírem num campo de constante modificação e expansão, seu estudo mostra-se necessário ainda que sujeito a falhas, imperfeições ou compreensão incompleta do fenômeno. A tendência que se tem identificado até o momento é a de interpenetração dos universos compostos da mídia tradicional e da mídia *online* apesar da existência de um diálogo tenso e de mútua influência entre ambas.

Em face dessas constatações, também se pode afirmar que o exercício da cidadania em rede depende, por outro lado, da existência de um domínio individual para interagir com essas ferramentas de mediação que permitem, cada vez mais, o acesso a informação e também à organização e participação em acontecimentos. Por essa razão se sustenta que diante dessa necessidade de se dominar e adquirir as habilidades necessárias para a vivência no ciberespaço é que emerge o verdadeiro poder da mídia, poder este, conferido "por *ouvir, falar e ser ouvido"* (Cardoso, 2007, p. 32). Ou seja, trata-se de um poder que permite aos "cidadãos, nos seus diversos papéis, acessar o espaço simbólico produzido pelas tecnologias da mediação e, consequentemente, poder usá-las na construção da sua autonomia individual e coletiva: o poder da *mediação*" (Cardoso, 2007, p. 32).

Por outro lado, deve-se reconhecer que esse é um poder limitado tendo em vista que depende do contexto em que o mesmo é exercido. Assim, "embora a mídia possua o poder de influenciar (e mudar) processos políticos, econômicos e sociais e de mudar a balança do poder, esse poder lhe é igualmente negado pelo Estado, pelo mercado, pelas audiências resistentes ou proativas, pelos cidadãos e pelos consumidores" (Cardoso, 2007. p. 32). Essa negação, todavia, não lhe impede que continue a exercer o poder de influenciar, muito pelo contrário, o que se identifica é que as novas tecnologias da informação e comunicação permitirão novos caminhos para o exercício desse poder.

Rafael Santos de Oliveira · Professor no Programa de Pós-graduação em Direito da Universidade Federal de Santa Maria (PPGD/UFSM-RS). Doutor em Direito pela UFSC. email para contato: rafael.oliveira@ufsm.br

## REFERÊNCIAS

ARBEX JUNIOR, José. *Showrnalismo:* a notícia como espetáculo. São Paulo: Casa Amarela, 2001.

BUDÓ, Marília Denardin Budó. As novas tecnologias de informação frente à ditadura do pensamento único: o mercado. In: *Anais do IV FoMerco*, 2003, Maringá - PR, 2003.

CARDOSO, Gustavo. *A mídia na sociedade em rede:* filtros, vitrines, notícias. Rio de Janeiro: FGV, 2007.

CASTELLS, Manuel. *O poder da identidade.* Tradução de Klauss Brandini Gerhardt. 5. ed. São Paulo: Paz e Terra, 2006.

CASTRO, Paulo Jorge Canelas de. Mutações e constâncias do Direito Internacional do Ambiente. *Revista Jurídica do Urbanismo e do Ambiente,* Lisboa: Instituto de Direito do Urbanismo e do Ambiente, n.2, dez, 1994.

CHAPARRO, Manuel. *Pragmática do jornalismo: b*uscas práticas para uma teoria da ação jornalística: São Paulo: Summus, 1994.

CONVENÇÃO sobre a Poluição Atmosférica Transfronteiriça a Longa Distância. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= CELEX:31981D0462:PT: HTML> Acesso em: 2 abr.2010

DIZARD JR., Wilson. *A nova mídia:* a comunicação de massa na era da informação. Tradução de Edmond Jorge. 2. ed. Rio de Janeiro: Zahar, 2000.

GOOGLE acaba com a censura na China. Disponível em: <http://pt.euronews.net/2010/03/22/google-acaba-com-a-censura-na-china> Acesso em: 22 mar.2010.

LAGE, Nilson. *A reportagem:* teoria e técnica de entrevista e pesquisa jornalística. Rio de Janeiro: Record, 2001.

LÉVY, Pierre. *Cibercultura.* Tradução de Carlos Irineu da Costa. São Paulo: Ed. 34, 1999.

LÉVY, Pierre. Ciberdemocracia. Tradução de Alexandre Emílio. Lisboa: Piaget, 2002.

MAIA, Rousiley C. M. Redes cívicas e internet: do ambiente informativo denso às condições de deliberação pública. In: EISENBERG, José; CEPIK, Marco (Orgs.). *Internet e política:* teoria e prática da democracia eletrônica. Belo Horizonte: UFMG, 2002.

MARCONDES FILHO, Ciro. *O capital da notícia: jo*rnalismo como produção social da segunda natureza. São Paulo: Ática, 1986.

MATTELART, Armand. *História da sociedade da informação.* Tradução de Nicolás Nyimi Campanário. São Paulo: Loyola, 2002.

McCORMICK, John. *Rumo ao Paraíso:* a história do movimento ambientalista. Tradução de Marco Antonio Esteves da Rocha e Renato Aguiar. Rio de Janeiro: Relumé-Dumerá, 1992.

McLUHAN, Marshall. *Os meios de comunicação como extensões do homem.* São Paulo: Cultrix, 1999.

MORETZSOHN, Silvia. *Jornalismo em tempo real:* o fetiche da velocidade. Rio de Janeiro: Revan, 2002.

NYE JR, Joseph S. *Compreender os conflitos internacionais:* uma introdução à Teoria e à História. Tradução de Tiago Araújo. Lisboa, Portugal: Gradiva, 2002-a.

NYE Jr., Joseph S. *Leadership e potere:* Hard, soft, smart power. Roma: Laterza, 2009.

NYE Jr., Joseph S. *O paradoxo do poder americano:* por que a única superpotência do mundo não pode prosseguir isolada. Tradução de Luiz Antônio Oliveira de Araújo. São Paulo: UNESP, 2002-b.

NYE Jr., Joseph S. *Power in the global information age:* from realism to globalization. New York: Routledge, 2004-a

NYE Jr., Joseph S. *The Powers to lead.* New York: Oxford, 2008.

NYE Jr., Joseph. *Soft Power:* The Means to Success in World Politics: New York: Pubblic Affairs, 2004-b.

OLIVEIRA, Rafael Santos de. *Direito Ambiental Internacional:* o papel da *soft law* em sua efetivação. Ijuí: UNIJUÍ, 2007.

PENA, Felipe. *Teoria do Jornalismo.* São Paulo: Contexto, 2005.

PRUDENCIO, Kelly Cristina de Souza. *Mídia ativista:* a comunicação dos movimentos por justiça global na internet. Florianópolis: UFSC, 2006. 207 p. Tese (Doutorado) - Programa de Pós-graduação em Sociologia Política, Centro de Filosofia e Ciências Humanas, Universidade Federal de Santa Catarina, Florianópolis, 2006.

RAMONET, Ignácio. *A tirania da comunicação.* Petrópolis: Vozes, 1999.

RAMONET, Ignácio. *Guerras do Século XXI:* Novos Temores e Novas Ameaças. Petrópolis: Vozes, 2003.

ROLLEMBERG, Marcello. Ética de papel. *Revista USP,* São Paulo, n. 59, setembro/novembro, 2003.

SANTOS, Milton. *Por uma outra globalização:* do pensamento único à consciência universal. 13. ed. Rio de Janeiro: Record, 2006.

SOARES, Guido Fernando Silva. *A proteção internacional do meio ambiente.* Barueri: Manole, 2003.

STEINBERGER, Margareth Born. *Discursos geopolíticos da mídia:* jornalismo e imaginário internacional. São Paulo: Cortez, 2005.

TOFFLER, Alvin. *Powershift:* as mudanças do poder. Tradução de Luiz Carlos do Nascimento Silva. 6 ed. Rio de Janeiro: Record, 2003.

TRAQUINA, Nelson. *O estudo do jornalismo no século XX.* São Leopoldo: Unisinos, 2001.

VARELA, Juan. Jornalismo participativo: o Jornalismo 3.0 In: ORDUÑA, Octavio I. Rojas; ALONSO, Alonso; ANTÚNEZ, José Luis; ORIHUELA, José Luis; VARELA, Juan.

*Blogs:* revolucionando os meios de comunicação. Tradução de Vertice Translate. São Paulo: Thomson Learning, 2007.

VAZ, Paulo. Esperança e excesso. In: PARENTE, André (Org). *Tramas da rede:* novas dimensões filosóficas, estéticas e políticas da comunicação. Porto Alegre: Sulina, 2004.

VIRILIO, Paul. *Velocidade e política.* São Paulo: Estação Liberdade, 1996.

WOLF, Mauro. *Teorie delle comunicazioni di massa.* 22. ed. Milão: Bompiani, 2006.

# Securitização da Cibersegurança no Brasil[1]

ROBERT MUGGAH
MISHA GLENN
GUSTAVO DINIZ

RESUMO

■ O Brasil vem incrementando sua arquitetura de cibersegurança e ao mesmo tempo consolidando sua posição de potência emergente. Embora o crime organizado seja uma das principais ameaças ao ciberespaço brasileiro, são dirigidos recursos às soluções militares que melhor serviriam à excepcional hipótese de guerra. Há menos ênfase na ampliação da capacidade de segurança pública, de modo a identificar e reagir ao crime cibernético bem como aos delitos digitais correlatos. Em razão da ausência de uma posição uniforme do governo sobre a questão, ou de dados confiáveis, o Brasil possui uma abordagem pouco coerente sobre a cibersegurança. Caso o Brasil volte a organizar sua abordagem, o governo deverá incentivar um amplo debate com uma estratégia clara de comunicações sobre as exigências da cibersegurança e quais as suas formas. Há necessidade de maior pensamento crítico sobre forma e conteúdo das estratégias ponderadas e eficientes para fazer face às ameaças cibernéticas. Torna-se essencial aperfeiçoar a coordenação entre as polícias estaduais de modo a melhor se antecipar e lidar com os crimes cibernéticos.

1 O presente estudo possui como base a Nota Estratégica elaborada pelo Instituto Igarapé, que se encontra no portal http://igarape.org.br/desconstruindo-a-seguranca-cibernetica-no-brasil-ameacas-e-respostas/.

## APRESENTAÇÃO

■ O Brasil sofre ameaças de uma ampla variedade das chamadas *ameaças cibernéticas*, inclusive as fraudes virtuais, os crimes cibernéticos e a vigilância digital. Nem todas estas ameaças são por natureza iguais. Indiscutivelmente, o risco mais sério e difundido é o crime virtual de motivação econômica – aquele que visa os bancos privados, firmas e pessoas físicas em busca de proveito. Outro importante conjunto de ameaças cibernéticas emana de grupos de hackers nacionais e estrangeiros, os quais procuram sabotar serviços governamentais, portais e alvos empresariais. Por exemplo, os maciços protestos populares de junho a agosto de 2013 coincidiram com uma alta no ativismo dos hackers. Por final, as divulgações por Edward Snowden de que as redes oficiais de comunicações do Brasil se sujeitavam à espionagem rotineira pela Agência de Segurança Nacional (NSA) norte-americana, criou o espectro de uma nova ameaça cibernética no país: A ciberespionagem e segundo alguns a ciberguerra.

E ao passo que aumenta em todo o Brasil e América Latina a inquietude com as ameaças cibernéticas, conhece-se de fato relativamente pouco sobre as mesmas. Quase não há debates sobre os protagonistas dos quais emanam estas ameaças, seus interesses e motivações, seu *modus operandi* ou quais suas relações com as mais tradicionais organizações criminosas ou políticas. Há poucos especialistas se ocupando de uma avaliação pormenorizada destas variadas – e até bastante diferenciadas – ameaças cibernéticas, e muito menos ponderando as reações públicas e privadas. Em que pese a profunda falta de conhecimento, mesmo assim o governo brasileiro organizou com rapidez uma abrangente infraestrutura de cibersegurança e defesa. Curiosamente, a resposta possui foco limitado em apenas algumas dimensões destas ameaças – em especial as estrangeiras. Entre as muitas instituições deste meio, o *Centro de Defesa Cibernética* do Exército Brasileiro (o CDCiber) é peça chave na postura de defesa do país.

Até determinado ponto, a aparelhagem de cibersegurança em célere avanço no Brasil, mostra-se *em desalinho com as ameaças reais emergentes no ciberespaço. No lugar de mirar com mais precisão o cibercrime internacional e interno, o estado procura uma resposta no aperfeiçoamento da luta contra a ciberguerra e de sua capacidade antiterrorismo. Não significa afirmar que não há perigos nítidos e presentes relativos ao ciberterrorismo e à ciberguerra. Pelo contrário, o presente Estudo Estratégico opina que o governo brasileiro procura uma abordagem de securitização contra* as ameaças cibernéticas, no lugar de se contrapor aos desafios mais urgentes em face aos cidadãos, em especial o cibercrime. De forma sucinta, o estado (o agente)

securitiza o ciberespaço (o referente) em nome do povo (a plateia). Securitizado o objeto, é possível legitimar os meios extraordinários de solução do problema percebido, inclusive com legislação de emergência, ao mobilizar as forças armadas ou outros.[2] Não há consequências apenas na política pública e nos gastos; a resposta militar exagerada poderá arriscar colocar em jogo os direitos básicos dos cidadãos devido à vigilância e censura onipresente, entre outros. Por exemplo, o CDCiber em conjunto com a ABIN criaram plataformas para monitorar as mídias sociais após os protestos de 2013.

A abordagem securitizada de tratar a insegurança cibernética no Brasil acha-se de acordo com o esforço mais amplo de redefinir o papel das forças armadas do país para o século vinte e um. Na medida da consolidação da democracia, estabilidade e economia do Brasil, as forças armadas redefinem seu papel e postura relativos às ameaças não tradicionais. Por um lado, as mesmas visam mais o controle de fronteiras e as atividades antidrogas.[3] E pelo outro lado, as forças armadas procuram ampliar seu alcance e influência no domínio dinâmico e em constante evolução do ciberespaço. Ao mesmo tempo as demais importantes instituições públicas que lidam com ameaças cibernéticas, a exemplo da Polícia Federal, dispõem de menos recursos e organização. Logo, o desenvolvimento de capacidade militarizada para a resposta cibernética possui inspiração em parte no esforço e desejo do Brasil de ampliar seu alcance e relevância geopolíticas. Na condição de potência em ascensão, o governo brasileiro se vale não apenas da incipiente arquitetura de cibersegurança do país, mas também com maior amplitude de seus conhecimentos em governança cibernética, de modo a projetar o soft power nas relações bilaterais e nos fóruns multilaterais.

O presente *Estudo Estratégico* considera a evolução e as implicações desta visão securitizada na administração dos bens da cibernética do Brasil A primeira seção apresenta um panorama da paisagem cibernética do Brasil. A segunda seção avalia as ameaças reais e implícitas ao ciberespaço brasileiro, com ênfase nas prioridades nacionais bem como as deficiências na resposta do estado. A terceira seção se concentra nas respostas jurídicas e programáticas a tais ameaças, com especial atenção ao papel das instituições de segurança. A seção quatro discorre sobre os dilemas surgidos da abordagem por demais militarizada à cibersegurança. Aqui há também pormenores de como os esforços do país de afirmação internacional acabam moldando o processo interno de tomada de decisões com relação a ciber-

2 Veja a obra de Waever (1995) sobre a securitização.
3 Veja Diniz e Muggah (2012).

segurança e defesa. A conclusão oferece um resumo de conclusões assim como um conjunto de recomendações para fazer face aos desafios no Brasil de governança cibernética e segurança.

## DEFINIÇÃO DO CIBERESPAÇO BRASILEIRO

■ O Brasil acha-se sob uma revolução digital com poucos paralelos no mundo em desenvolvimento. O índice de penetração digital e adoção das mídias sociais elevou-se de forma exponencial na última década. Durante este prazo o Brasil assistiu a um aumento de dez vezes em acessos à Internet e assinaturas de telefones celulares, constando no presente mais da metade de sua população de 200 milhões conectadas.[4] A quantidade de fatores relativos às melhoras no Brasil do desenvolvimento social e econômico impulsionam estas tendências. O clima macroeconômico bastante estável bem como as políticas sociais de redistribuição levaram à ampliação da classe média no país. Ao mesmo tempo, a marcha dos novos consumidores motivou a procura por tecnologias de informação e de comunicações (TICs), transformando a escala de suprimento a níveis em conformidade com o vasto mercado interno do Brasil.

A aparição de uma classe média ampliada e conectada dá forma ao ambiente cibernético no Brasil. O acesso mais ágil às novas tecnologias de informações deu causa a uma ampla gama de formas de capacitação social, política e econômica no país. Sem surpresa alguma, a capacitação digital vem acompanhada de maiores desafios a exemplo dos protestos em massa e do crime organizado. Como país de renda mediana, o Brasil se vê obrigado a tratar de suas arraigadas desigualdades dentro e fora dos meios digitais. As contradições aparecem à medida em que seus legisladores procuram integrar mais plenamente os cidadãos recém capacitados na democracia e economia formal do país. Como potência emergente, o país se encontra também frente a dilemas com seu maior comprometimento com políticas globais. Logo, fatores internos e internacionais possuem um papel crítico no rumo da governança cibernética do Brasil.

Poucos países foram tão drasticamente afetados pela capacitação digital como o Brasil. A escala e dinamismo do ciberespaço brasileiro atingiu novas alturas nos últimos anos. A começar com as manifestações em massa de inspiração digital, atingindo as ruas do país entre junho e agosto de 2013, até a presença rotineira

4 Veja o portal Internet World Stats (http://www.Internetworldstats.com), em dezembro de 2013.

do mesmo no topo de *rankings* relativos ao cibercrime.[5] O Brasil é conhecido de modo geral como autor e vítima da criminalidade digital. Ademais, o Brasil ainda se ressente das divulgações de espionagem realizadas por alguns países, em especial os Estados Unidos, Canadá e Reino Unido, tendo iniciado processos de reforma na ONU e internamente. A natureza complexa da "ameaça cibernética" – bem como sua interpretação no Brasil [6] – exerceu um expressivo papel na moldagem da governança cibernética e arquitetura de cibersegurança do país.[7]

Há necessidade de uma avaliação equilibrada ao se considerar as respostas contra as ameaças cibernéticas e a cibersegurança. Torna-se importante levar em conta os poderosos interesses bem como as lutas simbólicas que dão forma à definição do que constitui ameaça digital em determinada sociedade. Uma cuidadosa análise da narrativa e dos fatores por trás da mesma, seria capaz de revelar como se determinam as prioridades e recursos selecionados. É possível partir para além do curto prazo em direção à visão de prazo mais amplo que formula as decisões dos grandes protagonistas. Apenas com a adoção da visão bruta será possível compreender por completo o conceito, construção e aplicação da cibersegurança. Tais escolhas possuem peso, pois exercem influência fundamental em questões de segurança pública e de direitos pessoais à privacidade, dentro e fora dos meios digitais.

---

5 A International Telecommunications Union (ITU) define o cibercrime como atividade que emprega computadores ou redes como ferramentas, alvos ou locais para fins criminais. Foram definidas cinco categorias: 1) infrações contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computação; 2) infrações relativas a conteúdo; 3) infrações relativas a computadores; 4) infrações relativas a direitos autorais e marcas registradas; e 5) infrações complexas e combinadas (a exemplo de lavagem de dinheiro, ciberterrorismo e guerra, espionagem e ação de hackers, em determinado medida). Veja ITU (2009).

6 Nossa escolha do termo "ameaça cibernética" no lugar do "cibercrime" revela a visão mais expansiva das reais dimensões das atividades digitais nocivas. Muitos países do mundo em desenvolvimento, inclusive na América Latina, acham-se expostas a determinadas "ameaças cibernéticas" que não se enquadram por completo na rigorosa definição da ITU. Ademais, a expressão "ameaça cibernética" abarca percepções que não necessariamente implicam em risco real objetivo. É importante avaliar o que a sociedade percebe como ameaças digitais primárias e como as mesmas são conduzidas através do tempo.

7 De acordo com especialistas brasileiros, a segurança cibernética inclui ações preventivas e repressivas, que normalmente embutem um estado de alerta persistente assim como o preparo dos sistemas e das pessoas engajadas. Utiliza-se também a mesma no trato de práticas privadas de proteção do ciberespaço, por pessoas e empresas." Por outro lado, a defesa cibernética inclui "atividades operacionais instaladas para combates ofensivos ou contraofensivos no ciberespaço, de forma normal ligadas aos serviços militares e de inteligência dos países." Veja Canongia e Mandarino (2009). Também nos referimos à governança cibernética em vista de suas ligações com a segurança cibernética.

## ADVENTO DAS NOVAS TECNOLOGIAS

A demografia da Internet no Brasil se assemelha a diversos outros países grandes de renda mediana, embora com expressivas diferenças em virtude da grande extensão territorial do mesmo. De modo especifico, o Brasil está bem posicionado em comparação a outras pujantes economias emergentes, em especial no meio do grupo Brasil, Rússia, Índia, China e África do Sul (os BRICS). O Brasil situa-se entre Rússia e China no tocante ao percentual de usuários da Internet (entre a população total do país).[8] Em comparação com seus vizinhos e demais potências emergentes, o Brasil lidera o grupo. O Brasil está bem na frente de seus pares da América Latina e do Caribe (ALC) no que tange ao emprego de TICs. Aqui se encontra a maior população latino-americana dentro e fora dos meios digitais: há cerca de 110 milhões de usuários da Internet no país, ou algo como 54,2 por cento da população.[9] O mesmo representa quase o dobro do total de usuários do segundo país da América Latina mais conectado digitalmente, o México.[10]

Diversas facetas relativas ao emprego da Internet no Brasil merecem especial atenção. Primeiro, os brasileiros em especial são produtores ávidos e usuários da mídia social. A ALC é a maior região mundial consumidora de mídia social,[11] o que se deve em grande parte à imensa predileção no Brasil pelas redes digitais. Os brasileiros passam em média 2,2 horas por semana em plataformas de mídia social, a exemplo do Facebook.[12] Quase 60 por cento dos usuários da Internet no Brasil possuem conta no Facebook, atrás apenas dos Estados Unidos na quantidade de perfis.[13] O mesmo se confirma em se tratando do Twitter: Os brasileiros possuem 33 milhões de contas e os registros continuam em ascensão.[14] Os brasileiros lideram assim como seguem tendências; 20,5 por cento dos usuários

8 Rússia possui 87 milhões de usuários de Internet (61,4%), Índia 195 milhões (15,2%), China 621 milhões (45,8%) e África do Sul 24 milhões (49%). Veja o portal Internet World Stats (2013).

9 Veja o portal Internet World Stats em dezembro de 2013.

10 México possui 52 milhões de usuários da Internet, ou 43,5% de penetração. Veja o portal Internet World Stats (2013).

11 Os latino-americanos ocupam 56% mais tempo em plataformas de redes sociais do que a média global. Veja http://thenextweb.com/twitter/2013/01/16 twitter-to-open-office-in-brazil-its- second-biggest- market-after-the-us-in-accounts/.

12 Veja http://online.wsj.com/news/articles/SB10001424127887323301104578257950857891898.

13 Veja o portal Internet World Stats (resultados para dezembro de 2013).

14 Veja http://semiocast.com/en/publications/2012_01_31_Brazil_becomes_2nd_country_on_Twitter_ superseds_Japan.

de Internet no país visitam a plataforma constantemente. Em termos globais, o Brasil é o quinto lugar no uso do Twitter.[15]

Segundo, nos últimos anos o Brasil experimentou um maciço incremento digital de atividades eletrônicas, econômicas e financeiras. O Brasil ostenta elevados níveis de comprometimento com serviços financeiros, que se assemelham aos meios de alta renda da América do Norte e Europa Ocidental. A economia digital tem evoluído *pari passu* com a economia nacional como um todo. No tocante ao *e-commerce*, o valor total das operações em 2012 atingiu US$ 11,3 bilhões, ou seja, aumento anual de 25 por cento em comparação com 2011.[16] Porém, está no setor de *e-banking* a verdadeiro vigor da economia digital no Brasil. Quase todas as contas bancárias hoje no Brasil possuem acesso via Internet. No total, a base de correntistas dos bancos aumentou em oito por cento em 2012 e abrigam 54 milhões de pessoas, o que representa 42 milhões de contas correntes na Internet além de 3,4 milhões de contas através dos celulares, incremento de 11 por cento e de 49 por cento respectivamente comparado a 2011.[17] Tais estatísticas são de dimensões fora do comum e ilustram a natureza inusitada do ciberespaço brasileiro. Sem dúvidas, o cibercrime no Brasil não deixou de organizar seus alvos e práticas em torno dos sistemas e usuários do *e-banking*.

Uma terceira característica da utilização da Internet no Brasil tem a ver com o acesso e emprego com celular, cujo crescimento foi vertiginoso nos últimos três anos. Há nos dias de hoje uma média de mais de duas assinaturas por pessoa.[18] A vasta maioria dos telefones celulares servem ainda para chamadas pessoais ou o envio de mensagens de texto. No entanto, há em curso um movimento vigoroso em direção aos *smartphones* e *tablets*. A quantidade de *smartphones* dobrou durante a primeira metade de 2012 e atingiu 60,1 milhões de aparelhos.[19] Os celulares com conexão Internet em banda larga já perfazem cerca de 36 por cento do mercado de telefonia móvel no Brasil.[20] A predileção pelos *smartphones* indica uma aceleração para o futuro próximo. As autoridades do país investem de modo maciço na difusão nas conexões em banda larga bem como a transição das redes

15 Veja http://www.billhartzer.com/pages/comscore-twitter-latin-america-usage/.
16 Veja http://wyse.com.br/portugues/2012/03/o-comercio-eletronico-no-brasil/.
17 Veja http://www1.folha.uol.com.br/fsp/mercado/69329-bancos-perdem-r-15-bi-com-fraudes.shtml.
18 Veja Dados e Estatísticas dos TICs ITU em http://www.itu.int/ITU-D/ict/statistics/explorer/index.html.
19 Veja http://tecnologia.ig.com.br/2013-01-18/entre-os-celulares-usados-no-brasil-36-sao-smartphones-diz-nielsen.html.
20 Ibid.

de 3G para as de 4G. Tais movimentos encontram explicação em parte nos mega-eventos esportivos recentes e futuros, inclusive a Copa do Mundo da FIFA (2014) e as Olimpíadas (2016), que insuflam a procura por conectividade mais rápida e confiável. O governo resolveu isentar de impostos os fabricantes locais dos *smartphones*, em garantia da redução dos preços no varejo.[21] A ampliação de acesso aos *smartphones* (assim como os preços mais baixos) recebeu assistência também da tomada do mercado brasileiro pelos produtos chineses de preços mais em conta.[22]

Em quarto lugar, houve uma sensível mudança de quem e como se adquire acesso à Internet. Mais de 66 por cento dos usuários da Internet no Brasil ingressam na rede todos os dias, enquanto 25 por cento o fazem no mínimo uma vez por semana. Embora os mais jovens (entre 16 e 34 anos de idade) formam a maioria dos usuários, não há expressiva diferença no tempo de uso entre as faixas etárias. Como também não há diferenças marcantes entre os gêneros, ao menos no tocante à utilização: há igual quantidade entre os dois gêneros nas redes sociais, pessoas que permanecem ligadas por prazos mais ou menos iguais.[23] As políticas públicas de promoção da inclusão digital, as maiores rendas e produtos mais acessíveis também mudaram a forma de acesso à rede pelos brasileiros. Em 2011, a Internet era acessada 59 por cento das vezes em casa, 14 por cento a partir das LAN houses (Local Area Networks), 12 por cento no trabalho, 8 por cento da casa dos outros, 3 por cento na escola, 2 por cento a partir de aparelhos móveis e 1 por cento a partir de espaços públicos com wi-fi grátis.[24] Estudos recentes realizados pelo CTS-FGV indicam uma queda acentuada na quantidade das LAN houses nos anos recentes, à medida que o custo dos laptops, tablets e aparelhos celulares vem declinando, inclusive em áreas mais pobres e densamente habitadas, a exemplo das favelas.[25] Até as residências nos mais modestos dos setores sociais são capazes atualmente de adquirir novas tecnologias para uso pessoal, do sorte que o acesso a partir de casa através de aparelhos móveis está se tornando a regra com celeridade.

---

21 Vejahttp://www.redebrasilatual.com.br/tecnologia/2013/04/programa-de-inclusao-digital-deve-reduzir-preco-de-smartphones-nacionais.

22 Veja a apresentação do CTS-FGV durante o evento Open Development (IDRC – Montevidéu, Uruguai, abril de 2013).

23 Veja http://www.cetic.br/usuarios/tic/2011-total-brasil/rel-int-03.htm Percentage using internet on a daily basis regarding age: 10-15 (57%); 16-24 (66%); 25-34 (70%); 35-44 (68%); 45-59 (68%); e maior de 60 (68%).

24 Veja http://www.cetic.br/usuarios/tic/2011-total-brasil/rel-int-04a.htm.

25 Veja CTS-FGV (2012) em http://direitorio.fgv.br/node/2507.

Finalmente, mesmo assim a escala de atividades brasileiras no ciberespaço reflete ainda as desigualdades estruturais do país. As diferenças de renda, educação e região geográfica influenciam como e se as pessoas acessam a internet. Por exemplo, 50 por cento das residências nos estados de São Paulo, Rio de Janeiro, Minas Gerais e do Espírito Santo possuem acesso à Internet, porém este percentual decai para 22 por cento na região Norte.[26] Ademais, as classes mais abastadas permanecem muito mais tempo conectados na Internet do que os pobres. A proporção dos que acessam o serviço pelo menos uma vez por semana é de cerca de 80 por cento dos usuários de categoria mais elevada, de 65 por cento nas classes médias e inferior a 50 por cento nas classes de baixa renda. A diferença fica nítida também entre os níveis de escolaridade. Embora 55 por cento da população analfabeta do país acesse a Internet em bases semanais, o tempo de permanência aumenta do forma expressiva em se tratando de pessoas de ensino superior, com diploma universitário. A frequência de acessos semanais é de 87 por cento.[27]

A conectividade em alta bem como a capacitação digital no Brasil está intimamente ligada às desigualdades estruturais do país.[28] Este fato se torna mais nítido ao analisarmos o espectro completo de usuários e as atividades correlatas no Brasil. Grupos organizados e desorganizados começam a se aproveitar do ciberespaço, seja para forçar a mudança política e social, seja para realizar seus próprios interesses econômicos particulares, inclusive os criminosos. Há exemplos edificantes de movimentos sociais que se atrelaram ao poder das novas redes e infraestrutura de comunicações, de modo a promover a transformação política positiva e progressiva. Aumenta a tendência de exploração da Internet para fins de ganhos pessoais e criminais, em grande parte devido aos formidáveis desafios estruturais do Brasil.

## AVALIAÇÃO DAS AMEAÇAS CIBERNÉTICAS

■ O tratamento das ameaças cibernéticas de amplo espectro é crítico para superar equívocos e lidar com políticas mal formuladas. Em razão da novidade e

26 Veja www.cetic.br/usuarios/tic/2011-total-brasil/index.htm.

27 54% das pessoas com escolaridade fundamental acessam a Internet pelo menos uma vez por semana; esta taxa sobe para 63% das pessoas com escolaridade de nível médio. Veja http://www.cetic.br/usuarios/tic/2011-total-brasil/rel-int-03.htm.

28 Os indicadores da inclusão digital no Brasil refletem também disparidades quando confrontados em termos nacionais e internacionais. Veja FGV-CPS (2012a e 2012b) e http://tecnologia.terra.com.br/internet/inclusao-digital-no-brasil-esta-acima-da-media-mundial,c91cfe32cdbda310VgnCLD200000bbcceb0aRCRD.html.

da natureza técnica da questão, governos e cidadãos possuem parcas informações sobre a forma de reagir. Os cidadãos, os negócios e as instituições com frequência sentem que a compreensão das questões acha-se além da sua capacidade, ou que ameaças não lhes sejam relevantes. Com frequência a ignorância ou a falsa percepção acaba em ausência de ação no tratamento direto das ameaças de cibersegurança. As estratégias, quando implementadas, tendem a unir retalhos pinçados mediante premissas espúrias e sem comprovação. Raramente há dados robustos para fundamentar a tomada de decisões. Urge uma abordagem com maior peso na evidência, de forma a avaliar as ameaças cibernéticas – com apoio na ciência dos inúmeros riscos digitais interligados. Infelizmente, tempo e recursos já escassos são com frequência dirigidos às áreas de menor importância no lugar das verdadeiras ameaças principais. A seção a seguir leva em conta o cibercrime convencional, as ciberinfrações complexas assim como as ameaças emergentes, no esforço para a formação de uma agenda mais sofisticada no Brasil.

QUADRO 1. Os três principais conjuntos de ameaças cibernética no Brasil

| Categoria | Definição | Exemplos | Reações normais do governo | Realidade brasileira |
|---|---|---|---|---|
| Cibercrime convencional | Trata-se das formas mais difundidas no mundo de infrações cibernéticas, cuja tipologia é a proposta pela ITU (2009) [veja nota de rodapé 4]. | Acesso ilícito (cracking), interceptação de dados, pornografia infantil, spam, discurso de ódio, fraude bancária, furto de identidade, infração contra direitos autorais. | Exclusivamente a segurança pública, visto que normalmente compreende crimes tradicionais, já categorizados nos códigos criminais. | Há dois grandes subconjuntos de crimes cibernéticos convencionais: 1) os de motivação econômica (em especial a fraude bancária) e 2) relativos ao conteúdo (por ex: racismo e pornografia infantil nas redes de mídia social). |
| Cibercrime complexo | Leva em conta e amplia a definição da ITU de infrações cibernéticas complexas ou combinadas, as que se enquadram em mais de uma categoria do cibercrime convencional. | Ciberterrorismo, ciberguerra, ataques contra a infraestrutura crítica, ciberespionagem e ação dos hackers. | Combinação de inteligência, ação militar e segurança pública, visto que há distintas fontes múltiplas e potenciais de ataques (sejam internas ou externas) assim como alvos. | Espionagem comercial e ação dos hackers são duas porém distintas ameaças. Há escassa comprovação de que o Brasil sofra de outros tipos de ameaças nesta categoria. |
| Ameaças emergentes | Ameaças relativas à expansão do ciberespaço que não se enquadram bem nas categorias da ITU, ou por serem emergentes ou por sua relação com o mundo em desenvolvimento. | TICs empregados pelos mais tradicionais grupos criminais, quadrilhas do crime organizado (drogas e tráfico de armas, extorsão digital, difusão da cultura de violência), ciberlavagem de dinheiro e sonegação fiscal, etc. | Deveria estar mais ligado à segurança pública, porém este campo acaba de emergir e há falta de reação do estado. | O Brasil sofre com os altos níveis de violência interpessoal e organizada, em especial com relação às quadrilhas e o crime organizado que lucra com o tráfico de drogas. Estes já assimilaram o poder das TICs para expandir e fortalecer seus negócios. |

## Cibercrime convencional

A exemplo das demais atividades ilícitas do mundo real, o cibercrime é extremamente difícil de mensurar com precisão. O ciberespaço é simplesmente enorme e descentralizado demais para aquilatar, acompanhar e relatar com certeza toda a sua atividade dolosa. Com efeito, torna-se bastante difícil até estimar uma ordem de grandeza da cibercriminalidade. Deve-se isto à relutância dos governos e empresas em divulgar este tipo de informação por temor de danos a suas reputações e perda de confiança e investimento. No entanto, algumas agências de estado assim como firmas privadas de cibersegurança emitem relatórios regulares sobre as dimensões estimadas dos mercados da cibercriminalidade. Valores e dados que na melhor hipótese são aproximações brutas, levando a amplas discrepâncias no impacto projetado destes mercados. Não obstante, os mesmos proporcionam alguma visão das grandes tendências capazes de deflagrar a determinação de prioridades assim como as questões sobre a alocação de recursos.

Os relatórios disponíveis apontam para expressivo aumento da cibercriminalidade no Brasil no decorrer da década. Tal expansão coincide com o acesso ampliado aos TICs em todo o país a partir do ano 2000. A quantidade total de incidentes cibernéticos recebidos pelo CERT.br (a central do Grupo de Resposta a Incidentes de Segurança em Computadores, ou CSIRT, no Brasil), saltou de 6000 em 2000 para mais de 466.000 em 2012.[29] Pelo menos 75 por cento dos usuários da Internet no Brasil dizem ter sido vítimas de uma ou outra forma de cibercrime. A média global é de 67 por cento, com as maiores taxas localizadas na Rússia (92 por cento), China (84 por cento) e África do Sul (80 por cento). No tocante aos hackers dos perfis das redes sociais, o Brasil encabeça a classe em conjunto com a China, com 23 por cento dos usuários que acusaram a tomada de suas contas por outros usuários. No mínimo 12 por cento dos brasileiros relatam que seus PCs foram infectados por *malware* através de manobras de *phishing* por falsos portais transmitidos pela mídia social.[30]

As empresas de cibersegurança também oferecem indicações sobre as dimensões das atividades digitais dolosas no Brasil. De fato, o Brasil consta em primeiro

29 Incidentes Totais em Computadores Relatados ao CERT.BR todo ano (1999-2012). Veja http://www.cert.br/stats/incidentes/ (CERT.br possui estatísticas sobre avisos dos incidentes ocorridos. Estes são espontâneos e se referem a incidentes ocorridos nas redes que avisaram a CERT.br espontaneamente).

30 Veja http://oglobo.globo.com/tecnologia/brasil-perde-16-bilhoes-por-ano-com-ciberataques-6280831#ixzz2BZTx7kkV.

lugar na região da ALC, como fonte e alvo dos ataques digitais. O mesmo vale para toda sorte de infrações cibernéticas cometidas através da informática, a exemplo de códigos maléficos, *spam zombies, phishing hosts* e *botnets*, entre outros. Estas tendências grassam a taxas alarmantes. A cibercriminalidade no Brasil evoluiu a passos largos na última década, sendo que as firmas de segurança dos Estados Unidos e Europa identificaram o Brasil como um dos países mais problemáticos desde 2006 por suas atividades com o cibercrime.[31] Os principais cibercrimes cometidos no Brasil na atualidade incluem a difusão de vírus ou *malware* (68 por cento), *hacking* de perfis na mídia social (19 por cento) assim como o *phishing* (11 por cento).[32] Embora o Brasil confirme sua grande atividade com *spam* (3,4 por cento dos fluxos globais em 2012, colocação modesta em comparação com a liderança, EUA com 42,2 por cento), os fluxos vêm decrescendo visivelmente e já não são problema grave entre os usuários.[33]

A fraude bancária é quase que uma especialidade no Brasil, em parte por motivo do tamanho do setor de serviços bancários no país.

A Federação Brasileira de Bancos – FEBRABAN relata que as perdas totais das instituições financeiras em 2011 atingiu R$ 750 milhões. A mesma observou também que 60 por cento do incremento anual nas fraudes bancárias ocorreram através da Internet, telefonia móvel, operações das centrais de atendimento e cartões de crédito. Um relatório da Kapersky Labs em 2011 colocou o Brasil na frente da China e da Rússia no emprego do *trojan horse* para penetrar nas contas bancárias através da rede: 16,9 por cento do total em ataques anuais partiram contra usuários no Brasil, contra 15,8 por cento na Rússia e 10,8 por cento na China.[34] Não obstante, grande parte destas fraudes foram perpetradas fora dos meios digitais, através de fraudes com telefones e cartões de crédito (US$ 450 bilhões). Diz-se que foram perdidos US$ 150 milhões através da Internet e do

31 Veja http://www1.folha.uol.com.br/tec/1143535-cibercriminoso-brasileiro-promove-ataque-sofisticado-a-banco-on-line.shtml.

32 Ibid. Em 2012 o Brasil constava em quarta colocação nos ataques de *phishing* (4%), atrás apenas dos EUA (29%), do Reino Unido (10%) e Austrália (5%). As perdas totais daquele ano por esta classe de fraude foram de US$ 10,5 bilhões. Fonte: Veja http://www1.folha.uol.com.br/mercado/1181392-ataques-ciberneticos-causam-perdas-de-us-21-bilhoes-a-empresas.shtml (RCA/EMC data).

33 As estatísticas de spam são criadas através de informações adquiridas por via de reclamações ao SpamCop e remetidas ao CERT.br. Veja http://cetic.br/seguranca/index.htm e http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=33298&sid=4#.UXpdF6LU_Io.

34 Vejahttp://www1.folha.uol.com.br/tec/1163431-custo-anual-do-cibercrime-no-brasil-e-de-r-16-bilhoes-diz-estudo.shtml (dados Kapersky).

*e-banking* móvel. Outros US$ 150 milhões foram furtados mediante pagamentos digitais de faturas de cartões de crédito.[35] Em algumas regiões o Brasil supera a América do Norte e a Europa Ocidental em segurança digital do setor bancário: por exemplo, a alteração dos sistemas de senhas, verificação em dois estágios e a biométrica se tornaram padrão.

O Brasil se tornou um porto seguro de outras espécies de cibercrimes identificados pela International Telecommunications Union (ITU). Entre estes, os principais são aqueles perpetrados contra empresas e negócios,[36] relativos a conteúdo[37] assim como infrações contra direitos autorais e marcas registradas.[38] Os custos globais do crime via Internet no Brasil, inclusive fraude e furto de informações bancárias, atinge cerca de US$ 8 bilhões anualmente (ou 7 por cento do total de perdas globais geradas pela cibercriminalidade).[39] Tais estimativas sugerem que o país seja o terceiro mais afetado em todo o mundo pelas atividades digitais ilícitas. O Brasil é de longe o alvo número um na América Latina: O México fica atrás do Brasil com perdas anuais de cerca de US$ 2 bilhões por conta da cibercriminalidade.

35 Vejahttp://info.abril.com.br/noticias/seguranca/brasil-perde-bilhoes-com-crimes-ciberneticos-04112012-13.shl.

36 PricewaterhouseCoopers (PwC) definiu que 32% das empresas brasileiras são vítimas de alguma forma de cibercrime a cada ano. Valor mais elevado do que a média global (223%). A PwC calculou que 39% (a maioria dos negócios atingidos) sofreu perdas entre US$ 100,000 e US$ 5 milhão. Cerca de 5% sofreram perdas de até US$ 1 bilhão. A demais, apenas 24% das empresas brasileiras afirmaram poder detectar e conter o vazamento de dados sensíveis sobre seus clientes e fornecedores. Veja http://www1.folha.uol.com.br/tec/1163431-custo-anual-do-cibercrime-no-brasil-e-de-r-16-bilhoes-diz-estudo.shtml (dados da PricewaterhouseCoopers) e http://www1.folha.uol.com.br/fsp/tec/90924-empresas-falham-na-protecao-de-dados-admitem-executivos.shtml.

37 Veja dados no portal da Safernet (http://indicadores.safernet.org.br/). A Safernet é uma ONG brasileira que centraliza relatórios sobre infrações digitais no Brasil relativos a conteúdo.

38 Pouco se sabe sobre o âmbito e a escala deste mercado cinzento no Brasil, porém podemos colher informações da International Intellectual Property Alliance (IIPA), a qual concluiu em um relatório recente que a Internet é o principal vetor da pirataria no Brasil, com crescimento exponencial. A mesma acrescentou que esta atividade ilícita dá origem a "perdas globais na economia que totalizam US$ 4,16 bilhões." Cerca de um bilhão de canções são baixadas de modo ilícito todo ano no Brasil, sem mencionar outras formas de propriedade intelectual e artística. Veja IIPA "2012 Special 301 Report on Copyright Protection and Enforcement".

39 Veja Norton/Symantec "*Norton Cybercrime Report 2012*" http://www1.folha.uol.com.br/tec/1163431-custo-anual-do-cibercrime-no-brasil-e-de-r-16-bilhoes-diz-estudo.shtml.

## Cibercrime complexo

■ Outra categoria da cibercriminalidade acha-se nas chamadas *infrações cibernéticas complexas* – em especial as ameaças às instituições governamentais.[40] Suas dimensões e natureza no Brasil ainda não se acham muito claras. Há uma falta de pesquisas quantitativas e qualitativas que ilumine a escala destas "ameaças", embora os especialistas demonstrem preocupação. Em seu lugar, há evidência empírica de infrações complexas passíveis de servirem como indicação de fenômenos mais amplos. Tais infrações são as que mais preocupam os governos federal, estaduais ou municipais, além das forças armadas e da segurança pública, até certo ponto. As mesmas também informam e orientam as escolhas dos governos no tocante à formação de infraestrutura da cibersegurança. Os maiores preocupados com as infrações cibernéticas complexas reproduzem estatísticas e empirismos repetidas vezes, porém sem apresentar evidências ou dados de corroboração. Há três infrações cibernéticas merecedoras de atenção especial.

Primeiro, ao contrário das formas benignas do ativismo digital, As autoridades no Brasil visam a ação dos hackers com grande suspeita. Não estão claras as dimensões dos danos físicos e econômicos ocasionados pelos hackers, sejam oriundos de alterações na aparência dos portais governamentais ou do setor privado, ou ataques contra a infraestrutura (DDoS). A maior preocupação das autoridades reside sem dúvida no furto e divulgação de informações oficiais sensíveis. Na forma dos casos Assange e Snowden, as informações obtidas por estes meios poderão ser divulgados e espalhados com rapidez e eficiência. Em outras ocasiões as informações poderão servir para negociações, extorsões e chantagens. No Brasil, governo (a Presidência e diversos ministérios, inclusive o Itamaraty), as forças de segurança (inclusive exército e forças policiais),[41] assim como empresas públicas e privadas (Petrobras e bancos, a exemplo do Banco do Brasil, Itaú e Bradesco), alvos frequentes dos hackers.[42]

---

40 São definidas pela ITU as infrações complexas ou combinadas, como tipos de cibercrimes passíveis de serem enquadradas em mais de uma categoria entre as que seguem: *Infrações contra a confidencialidade, integridade e disponibilidade de dados de computação e sistemas; infrações relativas a conteúdo; infrações relativas à computação; e infrações relativas a direitos autorais e marcas registradas.* Veja ITU (2009), pags. 51-59.

41 Veja http://www1.folha.uol.com.br/cotidiano/1211459-hackers-invadem-perfil-de-gcm-e-divulgam-dados-pessoais-em-rede-social.shtml.

42 Veja alguns outros casos e exemplos em http://www.bloggingsbyboz.com/search/label/cyber-security.

Os grupos de hackers mais em evidência no Brasil são os Anonymous e LulzSec, embora o segundo tenha supostamente suspendido suas atividades.[43] Devido ao desejo de preservar o anonimato assim como a estrutura descentralizada e não hierarquizada, os integrantes dos grupos são de difícil aproximação. Quando se manifestam, justificam seus atos com base em ideais tênues,[44] a exemplo de sua contrariedade às "desigualdades difundidas na América Latina" (em se tratando de grandes empresas e instituições financeiras) e "contra a manipulação generalizada de informações pelas autoridades."[45] Em outras ocasiões, os hacktivistas objetivam mais a realização de trotes e promoção de traquinagens. Os ataques do gênero eram mais frequentes em 2011 e no início de 2012 (Mais de 1250 casos).[46] No decorrer de 2012 e início de 2013 a incidência se reduziu rapidamente. A ação dos hackers tende a ocorrer em situações específicas, como a votação de um projeto controverso no Congresso. Não causa surpresa que durante os protestos de rua em meados de 2013 houve um surto expressivo este ativismo, visando a mídia preponderante do país, inclusive Globo e Veja.[47] A Copa das Confederações de 2013 e a Copa do Mundo de 2014, promovidas pela FIFA, se tornaram alvos.

Segundo, o governo brasileiro detectou ataques crescentes contra os sistemas e redes do estado. Tais ameaças alarmam as autoridades, em especial a administração pública federal bem como as forças armadas. O Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSI-PR) é o responsável pela primeira e garante "a disponibilidade, integridade, confidencialidade e autenticidade" das informações e comunicações nesta esfera. Desde 2009, o Diretor do DSIC e chefe da cibersegurança no Brasil, Raphael Mandarino,[48] aludiu diversas vezes a algo como 2000 ataques lançados por hora contra as 320 redes públicas federais. Embora raramente se mencione a origem dos ataques, Mandarino argumenta

43 Veja http://idgnow.uol.com.br/seguranca/2011/06/27/lulzsec-encerra-atividades-depois-de-50-dias-de-caos/.

44 Com efeito, durante os protestos de 2013, a ação do grupo Anonymous no local adotou uma postura de pouca relevância, sem muitos objetivos nítidos. Veja http://www.diariodocentrodomundo.com.br/o-ultrarreacionarismo-do-anonymous-do-brasil/.

45 Veja http://www.google.com/hostednews/afp/article/ALeqM5jyNoFn4ZXfibMLdscIqXDnIXVDjw e http://itdecs.com/2011/06/brazil-suffers-its-biggest-cyber-attack-yet/.

46 Veja Wyss (2011) e Kishetri (2013), p. 145.

47 Veja http://www.anonymousbrasil.com/brasil/twitter-da-veja-e-hackeado/ e http://www.tecmundo.com.br/Ataque-hacker/42249-Perfil-do-G1-no-Twitter-e-hackeado-por-ativistas.htm.

48 Veja http://www.gsi.gov.br/sobre/quem_e_quem/quem_e_quem_secretaria_executiva.

que 70 por cento constituem esforços para se obter informações financeiras dos bancos públicos.

Outros 10 por cento visam a INFOSEG no Ministério da Justiça, rede fechada que abriga quantidades de dados sobre investigações e processos criminais. Mais 15 por cento destinam-se a desvendar dados pessoais de funcionários públicos.[49] O General José Carlos dos Santos, antigo comandante do CDCiber, com frequência chamou a atenção às dimensões dos ataques contra as redes militares, de cerca de 30.000 diárias.[50] Surpreende o fato de que parte preponderante (30 por cento) destas redes estão sob a administração de provedoras privadas e das redes civis,[51] revelação inquietante à luz da sensibilidade das informações militares. Em que pese tamanha escala dos ataques diários perpetrados contra estas redes – muitos com motivação criminosa ou econômica – apenas dois casos lograram o vazamento de informações para o domínio público.[52]

A terceira ameaça cibernética complexa é o ciberterrorismo e a ciberguerra. Invoca-se regularmente a ameaça terrorista pelos governos e forças armadas em todo o mundo, para justificar a securitização do ciberespaço de um país. Por exemplo, os militares dos Estados Unidos elegeram a cibernética com a quinta mais importante prioridade do campo de batalha. No Brasil, um par de fatores são frequentes para justificar a postura rígida das autoridades com a cibersegurança. O primeiro e a proteção das *infraestruturas nacionais críticas*. As revelações sobre o *worm* Stuxnet infiltrado em 2010 nas instalações de enriquecimento de urânio em Natanz, no Irã, deu causa a expressiva apreensão no Brasil. De fato, circulou em Brasília uma leva de boatos infundados de que o apagão nacional há alguns anos teve origem em um ataque semelhante.[53] Com as autoridades do ramo no país incapazes de explicar os motivos dos apagões, os especialistas em cibersegurança lembraram os alegados ataques cibernéticos às redes de trans-

49 Veja http://info.abril.com.br/noticias/seguranca/redes-do-governo-tem-48-mil-ataques-por-dia-23082009-4.shl.

50 Vejahttp://www.defesanet.com.br/cyberwar/noticia/1632/CDCiber---Na-guerra-cibernetica--Brasil-adota-estrategia-do-contra-ataque.

51 Veja Canal Livre (programa de TV da Rede Bandeirantes, 29 de julho de 2011. Disponível em http://www.youtube.com/watch?v=lD8N7y86Aow.

52 O primeiro vazamento foi de informações não restritas e não sensíveis. Incluiu dados pessoais dos soldados ocupados em projetos sociais no Nordeste brasileiro. O segundo caso tratou da divulgação de detalhes pessoais de nomes e endereços de policiais com base no Rio de Janeiro, durante os protestos de 2013. Veja http://www1.folha.uol.com.br/cotidiano/2013/09/1342381--hackers-invadem-site-e-divulgam-dados-de-50-mil-policiais-militares-no-rio.shtml

53 O noticiário dos Estados Unidos jamais sustentou tais afirmações com evidências factíveis.

missão de 2005 e 2007.[54] A proteção da CNIS contra as "ameaças externas" de certa forma se assemelha à teoria convencional de dissuasão. Caso as autoridades acreditem que o "inimigo" seja capaz de danos reais – mesmo sendo mínimas a ocorrência de um ataque – as mesmas investirão nas defesas nacionais contra as possíveis ameaças.

Para as autoridades brasileiras, a grande preocupação é visibilidade de suas *redes de megaeventos*. O Brasil tem acolhido um número crescente de grandes iniciativas, inclusive eventos esportivos, conferências internacionais e festivais de arte.[55] Com isto, as principais cidades como Brasília, Rio de Janeiro e São Paulo figurarão no palco global. O CDCiber se encarrega da proteção destas redes. Como exemplo, há o papel do CDCiber em segurança na Conferência da ONU Rio+20 em 2012. A unidade se juntou à Polícia Federal para proteger as redes de ataques recorrentes durante o evento.[56] Embora a maioria das incursões partiram de criminosos comuns, houve também ataques mobilizados por grupos de hackers (por ex: o Anonymous) e outros que visavam dados sensíveis.[57] O CDCiber também atuou na coordenação da cibersegurança durante a visita ao Brasil do Papa Francisco, bem como na Copa das Confederações (2013) e a Copa do Mundo (2014) da FIFA. Persiste a questão se a ameaça do terrorismo ou um ataque solitário faz jus a uma resposta complexa.

O quarto risco em uso atualmente no aumento da securitização do ciberespaço é a *ciberespionagem*. Antes de 2013, o Brasil não registrava casos de ciberespionagem por um governo estrangeiro. De certo, não havia relatos públicos mesmo de espionagem industrial antes da figura de Edward Snowden, perto da época dos protestos digitais e de rua em meados de 2013. O que mudou por completo com as revelações da vigilância em massa pela NSA – Agência de Segurança

54 Impressiona a falta de informações precisas sobre o caso. Um documento atribui a alegação a um discurso do Presidente Obama, o qual se referiu ao caso sem dar nome ao país: "Sabemos que os intrusos acessaram nossa rede de transmissão de energia, e que em outros países tais ataques mergulharam cidades inteiras na escuridão. Agora ficou claro que esta ameaça cibernética figura como um dos mais graves desafios econômicos e de segurança nacional que a nação já enfrentou." Veja http://cii.in/WebCMS/Upload/Amaresh%20Pujari,%20IPS548.pdf.

55 Os eventos incluem por exemplo a Copa das Confederações (2013) e a Copa do Mundo (2014) da FIFA, além dos Jogos Olímpicos no Rio de Janeiro (2016).

56 Vejahttp://g1.globo.com/tecnologia/noticia/2012/06/anonymous-ataca-sites-ligados-ao-governo-em-protesto-contra-rio20.html.

57 O grupo Anonymous lançou a operação #OPHackInRio durante a Rio+20. Veja http://g1.globo.com/tecnologia/noticia/2012/06/anonymous-ataca-sites-ligados-ao-governo-em-protesto-contra-rio20.html.Vejahttp://g1.globo.com/tecnologia/noticia/2012/06/anonymous-ataca-sites-ligados-ao-governo-em-protesto-contra-rio20.html.

Nacional dos Estados Unidos. De acordo com uma série de artigos do *Guardian* e demais agências de notícias, milhões de telefonemas e emails de brasileiros foram interceptados pela NSA.[58] Em se tratando da intensidade da vigilância cibernética patrocinada pela NSA, o Brasil se coloca em segundo lugar atrás dos Estados Unidos.[59] Diz-se que as autoridades de inteligência dos Estados Unidos justificaram esta vigilância devido à ocupação pelo Brasil de posição estratégica na administração de uma estrutura global de telecomunicações (i.e. linhas de transmissão e cabos de fibra óptica). Não se tratava de inimigos, retrucaram, mas apenas a "proteção" destes ativos críticos. Ao mesmo tempo houve alegações de interceptação de telefonemas e emails da Presidente Dilma Rousseff, de autoridades do Ministério de Minas e Energia e de altos executivos da Petrobras,[60] as quais conduziram ao cancelamento da visita de estado da Presidente aos Estados Unidos e acusações na ONU.[61]

Naturalmente, o governo brasileiro não é totalmente inocente no tocante à ciberespionagem. Ao passo que as autoridades do país expressaram sua indignação contra a vigilância pela NSA, foram autorizados ABIN e CDCiber – os responsáveis pela proteção do país precisamente contra este tipo de interferência – a monitorar as atividades das mídias sociais no Brasil relativas aos protestos em massa de junho a agosto de 2013.[62] A ABIN recebeu críticas por não antecipar os eventos que deram origem aos protestos de 2013. Mesmo assim, a ABIN introduziu a plataforma Mosaico, de monitoramento da mídia social, para rastrear usuários e se adiantar aos novos acontecimentos. O sistema de monitoramento é controverso aos olhos de alguns ativistas da Internet, pois poderá levar à autocensura bem como a pressões sobre os movimentos sociais legítimos.[63] O mesmo se

58 Vejahttp://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934.

59 Veja http://oglobo.globo.com/infograficos/volume-rastreamento-governo-americano/.

60 Veja http://noticias.uol.com.br/internacional/ultimas-noticias/2013/10/06/ministerio-de-minas-e-energia-foi-espionado-por-canadenses.htm.

61 A Presidente Dilma Rousseff instou a ONU a se adiantar e regular a conduta dos estados no tocante aos TICs e declarou que o Brasil "apresentaria propostas para a definição de uma estrutura civil multilateral de governança e emprego da Internet, em garantia da proteção efetiva de dados que transitam através da rede" (veja maiores detalhes na seção quatro). Veja o discurso completo em http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf.

62 Veja http://oglobo.globo.com/pais/exercito-monitorou-lideres-de-atos-pelas-redes-sociais-9063915.

63 Veja http://www.estadao.com.br/noticias/cidades,abin-monta-rede-para-monitorar-internet,1044500,0.htm.

diz do programa Guardião elaborado pelos militares no CDCiber.[64] No entanto, o Brasil avança na consolidação de seu controle sobre seu ciberespaço. O governo brasileiro possui parceria com Portugal de um c abo de fibra óptica de US$ 185 milhões, em garantia de maior autonomia sobre o tráfego de Internet a partir de e para o país.[65]

**Formas emergentes da cibercriminalidade e lacunas de conhecimento.** Antecipar e rastrear as ameaças cibernéticas se tornou um desafio de peso para governos e empresas. As ameaças tratam das probabilidades, se existem e quando e onde poderão ocorrer. A abordagem crítica destas duas dimensões poderá contribuir para esclarecer o que as instituições deixam de enxergar e o que não desejam enxergar em razão de interesses mesquinhos. Há uma série de áreas carentes de maior debate, apenas para alargar o diálogo no Brasil sobre os delitos digitais. É importante levá-los em conta, de forma a contestar as reações mal concebidas.

Em primeiro lugar, há a questão de quem são os infratores. O especialista em cibersegurança Mikko Hypponen, da F-Secure, afirma que os governos perdem a batalha contra os infratores porque não investem o suficiente para determinar quem são eles. Os estados tampouco possuem indícios de sua motivação, natureza organizacional ou mesmo seu tipo de atividade. Este conhecimento é essencial na elaboração de estratégias eficazes de restrição, administração, prevenção e redução da cibercriminalidade. Em seu lugar, há a tendência de combinar as categorias de infratores, o que levaria a uma reação genérica ao cibercrime e não ao reconhecimento da natureza heterogênea da prática de crimes. Seus integrantes adaptam com frequência suas ferramentas e métodos, para contornar os novos mecanismos de defesa cibernética.

A Polícia Federal no Brasil criou uma base de dados de pessoas sujeitas a processos em razão de cibercrimes. Com a promulgação da nova legislação contra a cibercriminalidade, este conjunto de dados irá aumentar e cobrir uma gama ampliada de infrações cibernéticas. Organizar e colocar em prática estes dados é fundamental. Ao invés de recorrer a uma rede de arrasto, o conjunto auxiliará informar e moldar as estratégias de cibersegurança de modo a aliviar determinadas ameaças. Já temos ciência de alguns fatos através dos dados existentes:Tipicamente, os meliantes brasileiros são homens de boa formação, de classe média alta entre 25 e 35 anos de idade. No entanto, estas informações têm

64 Vejahttps://protestos.org/2014/06/18/exercito-usou-software-guardiao-para-monitorar-redes-sociais/.

65 Veja http://www.bloomberg.com/news/2014-10-30/brazil-to-portugal-cable-shapes-up-as-anti-nsa-case-study.html.

como base uma pequena amostragem de 177 pessoas presas e acusadas de fraudes cibernéticas entre 2010 e 2012.[66]

De acordo com a Polícia Federal, não há registros públicos de ataques por pessoas ou por grupos estrangeiros,[67] porém, estas incursões poderão tomar vulto. Devido em parte à realização no país de diversos megaeventos, à sua classe média em ascensão e à digitização dos serviços financeiros, os brasileiros com certeza irão enfrentar ataques mais freqüentes da cibercriminalidade estrangeira.[68] Há também evidências de que desde 2004, que a infração cibernética incrementou suas atividades estrangeiras.[69] Portugal e Espanha se tornaram alvos principais, embora a cibercriminalidade do Brasil tenha dado maior atenção a um mais amplo conjunto de comunidades de língua portuguesa e espanhola nos Estados Unidos, no Reino Unido e nas Américas do Sul e Central.[70]

O *modus operandi* dos hackers nacionais passou a ser entendido através de uma série de revelações recentes. Um antigo hacker no Brasil relatou como os grupos do cibercrime tendem a se organizar em grupos de três a cinco pessoas. Estas poderão se encontrar em uma única cidade, estado ou país, ou mesmo em diversos países. Muitos deles também integram fóruns de cibercriminalidade na *Deep Web*, a parte da Internet não acessada pelas ferramentas de buscas padrão. No entanto, estes fóruns começaram a rarear em razão da infiltração pelas autoridades de segurança pública e de inteligência, internacionais e dos Estados Unidos. Em geral há um contato chave de intermediação direta com grupos criminosos organizados, o qual fornece os recursos para criar os códigos maléficos. Há casos de traficantes de drogas, por exemplo, que pagam programadores de software para a criação de portais ilícitos,[71] facilitando a venda de narcóticos. Um excelente exemplo é a SilkRoad[72], embora existam muitos outros.

66 Veja http://info.abril.com.br/noticias/seguranca/brasil-perde-bilhoes-com-crimes-ciberneticos-04112012-13.shl?2.

67 Entrevista com o antigo chefe da Unidade da Polícia Federal de Repressão à Cibercriminalidade, o Delegado Sobral. O CERT.br relata que apenas 20% dos ataques em sistemas e redes no Brasil têm origem no exterior. Isto não significa que os ataques sejam necessariamente perpetrados por brasileiros, com o emprego dos IPs remotos fora do território nacional.

68 Entrevista com o Delegado Sobral.

69 Veja Glenny (2009).

70 Veja http://goo.gl/orTW9.

71 A *Deep Web* constitui um vasto ecossistema de portais e comunicações normalmente não catalogados pelas ferramentas de buscas convencionais, e com frequência acessíveis apenas remotamente. As estimativas definem a mesma em 500 vezes do tamanho da Rede "visível" ou de superfície. Veja, por exemplo, http://en.wikipedia.org/wiki/Deep_Web.

72 Diz-se que a SilkRoad foi derrubada por um hacker em 2013. Veja http://www.bbc.co.uk/news/technology-22381046.

Há outrossim conhecimento da *migração do crime organizado tradicional para o ciberespaço.* As quadrilhas têm marcado maior presença virtual – em especial nos portais da mídia social. Os traficantes e grupos de milícias publicam periodicamente testemunhos de seus feitos e inimigos no Facebook, Twitter e YouTube.[73] São exibidos clips frequentes dos chamados *funks proibidões,* enaltecendo a violência virtual.[74] Mais nefasto, os grupos do crime organizado já adotaram novas técnicas de expansão não apenas das redes de drogas, prostituição e contrabando, mas também da intimidação, coerção e proteção do território. Houve a migração para os crimes com caixas automáticas – passando pela remoção de máquinas inteiras de suas fixações até a prática delicada de clonagem dos cartões de crédito.[75]

De sua parte, a Polícia Federal e outras começaram a rastrear o movimento do crime organizado e das quadrilhas virtuais, inclusive nas cidades grandes e médias. Embora haja apenas poucos exemplos de grupos de cidadãos que empregam ferramentas de *crowd-mapping* para detector crimes bem como a vitimização (principalmente por temor de retribuição[76]), as agências de segurança têm investido em peso na analítica de previsão e em sistemas de fusão de dados para prever tendências e padrões da criminalidade.

A principal preocupação das autoridades brasileiras é a *lavagem de dinheiro*. Estimativas recentes sugerem que a lavagem abrange entre US$ 2,5 e 4 bilhões por ano no Brasil.[77] O ciberespaço facilita o movimento, segmentando e dispersando os recursos anonimamente. Embora não considerado como um "grande" crime cibernético no Brasil, a questão é levada muito a sério pela Polícia Federal e o Ministério da Justiça. Por exemplo, o governo designou *laboratórios de tecnologia contra a lavagem de dinheiro* (LAB-LDs),[78] os quais empregam ferramentas digitais para análise, interpretação e investigação. Estas novas tecnologias são utilizadas para rastrear os crimes de colarinho branco a exemplo da sonegação fiscal, além de atividades sistêmicas de lavagem de dinheiro.

---

73 Veja http://www.vice.com/read/mexicos-drug-cartels-are-using-the-internet-to-get-up-to-mischief.

74 Veja por exemplo, http://www.youtube.com/watch?v=u2thkZZvyos e http://www.youtube.com/watch?v=GtAGrAhnfu4.

75 Informações fornecidas pela URCC da Polícia Federal durante entrevista.

76 Veja Muggah e Diniz (2013).

77 Veja Ollinger (2013).

78 Veja http://goo.gl/2u1Uz e a estratégia nacional contra a corrupção e lavagem de dinheiro (ENCCLA) desde 2006.

Um objetivo central das instituições nacionais de segurança é a proteção da integridade da CNIS. Embora os sistemas como a SCADA[79] e outros sejam de fato desligados da Internet, sua vulnerabilidade a ataques não fica inteiramente limitada. Algumas autoridades do país reconhecem que a sua CNIS depende menos de sistemas de controle informatizado em comparação com países mais desenvolvidos,[80] o que paradoxalmente protege sua infraestrutura contra ataques. Embora aqui haja vantagem em termos de cibersegurança (justamente em razão da menor interconectividade com outras redes), o governo não alardeia este fato, passível de transmitir fraqueza na condição de potência emergente. Neste meio tempo, emerge outro plano nacional de proteção da infraestrutura crítica, distinto da atual arquitetura da cibersegurança nacional.[81]

## A MÃO PESADA DO ESTADO

■ O Brasil desenvolve uma infraestrutura de cibersegurança que tende em maior grau às prioridades militarizadas e securitizadas. O foco durante o processo visa em especial alguns tipos específicos de ameaças cibernéticas, visivelmente desconhecendo outras. Tais escolhas possuem expressivas consequências para a governança cibernética no Brasil. Com efeito, as decisões tomadas pelas instituições públicas influenciam a escala e o âmbito da vigilância, questões de neutralidade da rede, proteção (ou sua ausência) da privacidade assim como os direitos à informação pelos cidadãos. Logo, torna-se importante saber como o Brasil desenvolve sua arquitetura de cibersegurança. Ademais, torna-se crítico analisar as regras e práticas que regem a governança cibernética no país.

79 SCADA é a sigla de "controle de supervisão e aquisição de dados". Trata-se de um sistema de controle industrial informatizado de monitoramento e controle dos processos mecânicos em situações reais [O que é um "processo mecânico em situação real?" -NT] que ocorre em indústrias e demais instalações como a CNIS.

80 Informações fornecidas por um dos nossos entrevistados. O Brasil não aparece no documento elaborado pela TrendMicro a pedido da OAS CICTE, que avalia o grau de "conectividade" da CNIS nos países da América Latina. Veja TrendMicro (2013).

81 Há em andamento um Plano para a Segurança da Infraestrutura. Por enquanto há apenas uma referência disponível ao público sobre como o governo pretende proteger a infraestrutura de informações críticas, de autoria do DSIC: http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf.

## A arquitetura institucional de cibersegurança do Brasil

■ Há uma variedade de órgãos públicos que se ocupam da administração da cibersegurança nacional. Muitas destas visam apenas administração os sistemas, o desenvolvimento técnico e o aperfeiçoamento das ferramentas. Temos como exemplos o CSIRT (CERT.br) local, o Centro de Informações de Rede (NIC.br, encarregado de administrar os principais nomes de domínio no país) o Centro Renato Archer para Segurança da Informação, do Ministério de Ciência e Tecnologia, SERPRO e INI, entre outros. Uma pequena parcela trata do campo da cibersegurança como um todo. A depender da agência, a mesmo poderá se ocupar da elaboração de normativos, tomar decisões políticas ou autorizar iniciativas desde o nível nacional ao local.

Há uma hierarquia de instituições de estado que se ocupam da administração da cibersegurança nacional. No topo da pirâmide se encontra o *Gabinete de Segurança Institucional* (GSI). Diretamente ligado à Presidência, o GSI é o órgão governamental chave que trata de todos os aspectos civis de cibersegurança. É responsável também por outras áreas, inclusive assuntos militares e defesa cibernética (integra o *Conselho de Defesa Nacional* – CDN). As ramificações do GSI incluem o *Departamento de Segurança da informação e Comunicações* (DSIC), voltado para garantir a disponibilidade, integridade, confidencialidade e autenticidade da informação e comunicações na administração pública federal. Há uma coordenação muito próxima com a *Casa Civil*, também voltada à supervisão da concessão de certificados de segurança digital (para a infraestrutura pública chave). Ademais, encontram-se no GSI a *Secretaria de Assuntos Estratégicos* (SAE) assim como a *Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo* (CREDEN), comissão de assessoria da Presidência. O conjunto DSIC, SAE e CREDEN é o protagonista chave na formulação dos debates sobre a cibersegurança no país.[82]

Outras instituições que influenciam a pauta de cibersegurança no Brasil incluem o *Departamento de Polícia Federal* (DPF), sob a supervisão do *Ministério da Justiça* (MJ). Embora seu papel primordial seja a segurança pública em nível federal, ela também possui unidades voltadas para a cibersegurança. De igual maneira, a *Agência Brasileira de Inteligência* (ABIN) que monitora a mídia social, assumiu competências criptográficas na proteção das instituições públicas.

82 Os mesmos propuseram recentemente a elaboração para o país de uma estratégia nacional de longo prazo para a cibersegurança e defesa cibernética.

Tal atividade é conduzida através da *Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações* (CEPESC). Por fim, há o *Ministério da Defesa* (MD) que supervisiona as forças armadas e serve de ligação entre civis e militares. O papel do MD na formulação da arquitetura de cibersegurança nacional passa por análise mais pormenorizada nas seções seguintes. O MD abriga também o Estado-Maior Conjunto das Forças Armadas (EMCFA), com um papel também na coordenação da reação cibernética.

## Reações normativas às ameaças cibernéticas

■ O Brasil agiu com celeridade na elaboração de leis sobre a Internet bem como a cibercriminalidade. Há no momento mais de 1000 projetos de lei sobre o tema em trâmite no Congresso Nacional. [83] O *Marco Civil da Internet* é de longe o mais importante e de mais amplo conhecimento. O *Marco Civil* é a "Declaração dos Direitos" da Internet nacional e a primeira do gênero em todo o mundo.[84] A iniciativa no Brasil tem grande aprovação popular e recebeu expressivo apoio dos usuários da Internet durante sua elaboração inicial. Sua formulação se deu mediante um processo participativo, com contribuições de todo o país. O *Marco Civil* estabelece os princípios fundamentais para Internet, inclusive a liberdade de expressão, neutralidade da rede e proteção à privacidade. O projeto recebeu aprovação em abril de 2014 e espera-se que o mesmo fortaleça e preserve os direitos dos usuários, que por sua vez será passível de se contrapor a práticas mais nefastas que solapam os direitos dos usuários.

O Congresso Nacional deveria ter aprovado o *Marco Civil* já em 2012, porém as divergências com relação a duas questões chave detiveram o andamento do processo. A primeira destas versava sobre a *neutralidade da rede*. As empresas de telecomunicações procuraram obstruir e debilitar o princípio da neutralidade da rede, tentando limitar as proteções jurídicas.[85] O segunda questão controversa era sobre infrações aos *direitos autorais*. Os setores dependentes da manutenção dos direitos autorais desejavam o poder de exigir a remoção pelas ISPs de conteúdo ilícito sem ordem judicial. E apesar da oposição das telecoms e dos setores de direitos autorais, o Congresso agiu para conservar a neutralidade da rede e impedir

83 Veja http://observatoriodainternet.br/link-estadao-pls-de-internet-no-pais.

84 Veja o portal da MCI em http://edemocracia.camara.gov.br/web/marco-civil-da-internet.

85 O argumento do ramo de telecom era de que no mínimo a "redução das conexões rigorosamente por motivos técnicos" deveria ser permitida de modo explícito. Veja *Le Monde Diplomatique Brasil*, N. 65, dezembro de 2012.

a retirada arbitrária de conteúdo (salvo nos casos de vingança e pornografia). Não admira que atualmente o Brasil talvez seja a liderança mundial em solicitações para a retirada de conteúdo do Google.[86]

Outro elemento chave na formação da segurança cibernética e atualmente sob discussão na estrutura do *Marco Civil*, é o chamado *log register.* O mesmo é mecanismo fundamental das investigações cibernéticas e perícias correlatas. O que se acha em jogo durante as supra referidas deliberações legislativas era durante quanto tempo as ISPs e provedores de conteúdo deveriam manter "registros de conexões" para análise pelas autoridades. Diversos especialistas defendiam que a agência regulatória das telecomunicações no Brasil (ANATEL) deveria servir de órgão controlador, embora outros opinavam que o Congresso deveria ditar as regras.[87] Os primeiros venceram e o Congresso Nacional determinou que as ISPs deveriam conservar seus dados durante um ano, os provedores de conteúdo conservando-os por até seis meses. Surgiram também preocupações com a administração dos cibercafés. De um lado, estes desempenham uma função crítica no sentido de facilitar o acesso à Internet para grupos de baixa renda. Por outro lado, são frequentados de modo rotineiro pela cibercriminalidade. No final, a questão não recebeu tratamento direto no *Marco Civil.*

Embora a intenção primitiva do *Marco Civil* era estabelecer garantias e salvaguardas constitucionais relativas à administração do ciberespaço brasileiro, o mesmo se tornou um incentivo para a legislação agressiva de prevenção da cibercriminalidade.[88] Com efeito, foram promulgadas as primeiras leis contra a cibercriminalidade no país em razão da ira popular sobre um caso amplamente divulgado de ativismo por hackers, relativo ao vazamento de fotografias pessoais da conta de email de uma conhecida atriz de novelas. [89] O clamor da mídia tradicional e social atiçou crescentes ansiedades com relação à questão ainda não definida da privacidade digital. O Congresso convocou uma sessão de emergência e promulgou um projeto de lei redigido em 2011 (além de mais outro que dormi-

86 Veja https://knightcenter.utexas.edu/blog/00-13690-brazil-tops-googles-transparency-report-most-requests-censor-online-content

87 Veja http://www1.folha.uol.com.br/tec/2013/06/1295456-analise-rede-esta-virando-uma-ferramenta-de-vigilancia.shtml?utm_source

88 O Brasil foi um dos últimos países na América Latina a adotar a legislação contra a cibercriminalidade. Veja o portal OAS REMJA em http://www.oas.org/en/sla/dlc/remja/cyber_crime.asp

89 A atriz em questão era Carolina Dieckmann, da TV Globo, em 2012.

tava desde 1999). O primeiro projeto de lei – posteriormente lei no. 12,373/12[90] – possui expressivas implicações para os bens da cibernética no Brasil. Um segundo projeto de lei – atualmente a lei no. 12,735/12 – sofreu tantas emendas que sua validade é questionada.[91] Embora alguns críticos[92] argumentem que a legislação é confusa e incoerente, as leis definem com sucesso e elaboram controles e penalidades relativas às atividades na Internet. Por exemplo, é ilícito atualmente "invadir aparelhos de TI", "obter dados privados", ou "interferir ou prejudicar serviços de TI".[93] Muitos aspectos permanecem pouco claros.

Vale a pena observar que estas estruturas e leis mais recentes foram aprovadas em época na qual as autoridades brasileiras começaram a repensar a legislação criminal, a qual remonta a 1940. O novo código penal será votado no próximo ano e embora o mesmo inclua disposições contra a cibercriminalidade, estas não parecem solucionar as contradições e lacunas nas leis em vigor.[94] Há outros 40 projetos de lei relativos à luta contra a cibercriminalidade, que aguardam aprovação pelo Congresso.[95] O estoque em atraso reflete um problema de amplo conhecimento relativo ao excesso de legalismo do sistema político do Brasil; destaca também como o governo do país continua mal aparelhado para reagir ao panorama dinâmico e em célere mutação do cibercrime.

## Reações da segurança pública às ameaças cibernéticas

■ As autoridades policiais e militares do país acham-se em vias de investimentos substanciais com a cibersegurança no território. No entanto, parece haver um descompasso entre os tipos de ameaças ao ciberespaço brasileiro e a natureza das reações pelas autoridades se segurança. O crime organizado é uma das principais

90 Veja a lei integral em http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm

91 Veja http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm.

92 Entrevista com Walter Capanema. Veja http://goo.gl/59zMo.

93 A clonagem ou furto de dados de cartões de crédito já foi abordado por leis que criminalizam a falsificação de documentos.

94 Informações fornecidas por Walter Capanema durante o evento SEGINFO 2012 (setembro). Disponível em: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=31777&sid=18.

95 Talvez a questão mais importante para a cibersegurança seja o projeto de lei que visa proteger os dados pessoais do usuário. Há uma expectativa entre ativistas de que a mesma seja uma lei equilibrada, que proteja a privacidade enquanto fortaleça e proteja novos serviços importantes para a sociedade digital, a exemplo da computação nas nuvens e a *big data*. Veja http://goo.gl/PqZOF.

ameaças ao ciberespaço nacional, porém são dirigidos recursos no país em disparidade com as soluções militares que melhor serviriam à (um tanto excepcional) hipótese de guerra convencional. Há menos ênfase na ampliação da capacidade da segurança pública do dia a dia, de modo a identificar e reagir aos grupos do crime organizado. Em razão da ausência de uma posição uniforme do governo sobre a questão, e de dados confiáveis, o Brasil possui uma abordagem pouco coerente sobre a cibersegurança. Em seu lugar, poucos órgãos e pessoas que exercem influência estão à frente dos debates de modo a determinar no fundo o futuro da arquitetura nacional da cibersegurança.[96]

A *Unidade de Repressão à Cibercriminalidade* (URCC) da Polícia Federal é a autoridade máxima de segurança pública encarregada da prevenção e reação aos cibercrimes. Suas competências abrangem desde a investigação de crimes contra instituições públicas federais às infrações com ramificações interestaduais e internacionais. Dado que na cibercriminalidade quase sempre figuram pessoas e tecnologias de diversos estados assim como protagonistas no exterior, a Polícia Federal torna-se um agente operacional crítico de certa forma.A mesma se ocupa de investigar fraudes eletrônicas (*e-banking* e golpes com cartões de crédito) bem como redes virtuais criminosas de maus tratos de crianças. Em decorrência da supra referida lei nº. 12,373/12, a Polícia Federal em breve se responsabilizará pelo acesso não autorizado dos sistemas e redes de TI.

A URCC, com base em Brasília, também administra a aparelhagem de ciberinteligência[97] com equipes localizadas na maioria dos estados. Trata-se de grupos de pequeno porte (a própria URCC possui cerca de 20 policiais) e não necessariamente integrados por especialistas em cibersegurança. No entanto a URCC coordena as redes internacionais de segurança pública de forma a facilitar o intercâmbio de informações e administrar protocolos operacionais. Ademais, a agência está ligada diariamente 24 horas por dia à Cooperação Policial de Emergência da Interpol e à Ameripol, podendo também alavancar acordos bilaterais para a cooperação jurídica. A URCC parece operar bem no intercâmbio de informações sobre assuntos operacionais, com as autoridades de segurança pública do exterior e com os tribunais.[98] Em contrapartida, se um caso exigir a colaboração das empresas privadas de Internet nos Estados Unidos, a exemplo de Google ou

96 Vale mencionar dois exemplos, inclusive Raphael Mandarino Jr. (DSIC) e o General José Carlos dos Santos, antigo comandante do CDCiber. Este foi substituído em 2014 pelo General Paulo Sergio Melo de Carvalho.

97 Centro Integrado de Inteligência Policial e Análise Estratégica da Polícia Federal (Cintepol).

98 Entrevista pelos autores com o Delegado Sobral (URCC-DPF).

Facebook, surgem com frequência grandes demoras e entraves.[99] Estas empresas tendem a evitar colaborar com a segurança pública em razão das obrigações jurídicas e contratuais nos países que abrigam seus serviços chave e servidores.[100]

A URCC já realizou operações contra diversos grupos do cibercrime, inclusive Trojan Horse, Matrix, Ponto.com, Liontech e Azahar.[101] Para aperfeiçoar sua capacidade investigativa, a Polícia Federal implantou dois projetos, o *Tentáculos* (de filtração de dados cruzados visando a redução da quantidade de processos em avaliação) e o *Oráculo*, elaborado em especial para a Copa do Mundo da FIFA. O *Oráculo* constitui um sistema analítico prognóstico de inteligência, para a avaliação de ameaças futuras e informações básicas sobre os prováveis autores.[102] A URCC administra também o Centro de Monitoramento em busca de atividades digitais suspeitas. Durante o evento Rio+20 de 2012, a URCC logrou fundir o Centro de Monitoramento com a ala de cibersegurança das Forças Armadas, obtendo mais uma camada de apoio. [103]

As autoridades de segurança pública dos 26 estados do Brasil e do Distrito Federal, acham-se cada vez mais engajados contra a cibercriminalidade em nível subnacional. O agente Alexandre Wendt, identificou oportunidades assim como desafios que confrontas as forças militares bem como da polícia civil.[104] Do lado positivo Alexandre observou o estabelecimento crescente no decorrer da década, de unidades policiais especializadas para combater o cibercrime. Cidadãos e empresas tomaram maior conhecimento destas unidades especializadas e em diversos

99 A Polícia Federal chegou a prender o presidente da filial da Google no Brasil em 2012, após a mesma se negar a retirar o vídeo do YouTube que comprometia um político do país (observação de Daniel Oppermann). Para maiores informações sobre o episódio, veja: http://economia.ig.com.br/empresas/2012-09-26/presidente-do-google-no-brasil-e-preso-pela-policia-federal.html.

100 As autoridades de segurança pública dos Estados Unidos acessam dados das empresas registradas naquele país quando munidos de um mandado da justiça, o que confere aos mesmos uma vantagem estratégica.

101 Azahar foi uma operação contra a rede de pedofilia, que atuava basicamente através da Internet. A operação foi deflagrada em 2006, em 30 países ao mesmo tempo. Veja http://idgnow.uol.com.br/mercado/2006/02/21/idgnoticia.2006-02-21.5692495488/.

102 Veja http://www.sagapolicial.com/2012/01/saiba-mais-da-pf-projeto-oraculo.html.

103 Observado por Clayton da Silva Bezerra durante o evento SEGINFO 2012 (setembro). Disponível em http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=31793&sid=18#.Ue3JyI21HNw.

104 Observado por Alexandre Wendt durante o evento SEGINFO 2012 (setembro). Disponível em http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=31750&sid=18#.Ue3JhY21HN.

casos procuram auxílio com as mesmas.[105] Ao mesmo tempo, Wendt se preocupa de que a polícia exiba capacidade investigativa e de perícia deficientes.[106] Os problemas variam da ausência de infraestrutura técnica e recursos financeiros, até pessoal com treinamento deficiente, cooperação limitada entre os órgãos de segurança pública assim como a resistência das empresas privadas a divulgar as dimensões da cibercriminalidade. As ameaças persistem, em especial a f alta de padronização na coleta de evidências e procedimentos periciais, bem como a capacidade restrita de realizar a ciberinteligência. Por fim, há em aberto questões sobre como administrar a cibercriminalidade em uma estrutura federal complexa, na qual permaneça pouco claro quem é o encarregado de encabeçar as investigações ou administrar os processos jurídicos.

## Reações das forças armadas às ameaças cibernéticas

■ A intensidade do preparo dos militares em face da ciberguerra não se coaduna com a possível ameaça de conflito armado. Sem dúvida, o Brasil não se viu engajado em uma guerra em seu território desde 1870 e jamais se tornou alvo do terrorismo internacional.[107] No entanto, o governo brasileiro prepara suas forças armadas para assumir um papel de liderança na proteção do ciberespaço do país, embora seu principal propósito seja civil. Houve expressivos investimentos no aperfeiçoamento da cibercapacitação militar – com certeza maior do que no setor de segurança pública. E embora outros poderes de expressão tenham adotado uma abordagem semelhante,[108] o grau de envolvimento do setor militar do país em matéria de cibernética não é adequado ou inevitável. Na América Latina onde o autoritarismo era a regra desde a década de 60 até a de 80, apenas a Colômbia incentivou o papel das forças armadas neste campo, a um grau igual ao do Brasil.

105 Importante observar que as forças policiais estaduais achavam-se no meio de uma controvérsia durante os protestos de 2013 no país. Por exemplo, a unidade policial do Rio de Janeiro especializada em cibercrimes (DRCI) prendeu preventivamente manifestantes que planejavam protestosnasruas.Vejahttp://oglobo.globo.com/rio/doze-ativistas-deixam-complexo-penitenciario-de-bangu-na-madrugada-desta-quinta-feira-13284027.

106 A polícia no Brasil não depende de operações secretas, visto que as mesmas não são regulamentadas pelo governo (logo, a polícia prefere não se arriscar) [observação do Delegado Sobral]. As operações secretas são fundamentais em outros locais para combater a cibercriminalidade (veja Glenny, 2011).

107 O país sofreu 21 anos de ditadura militar (1964-1985), época caracterizada pelos abusos dos direitos humanos por parte dos agentes do estado.

108 EUA, França, Israel, Reino Unido, Rússia e China, por exemplo.

Há diversas razões para o Brasil adotar a arquitetura de defesa da cibersegurança por meios militares. Primeiro, as forças armadas procuram com afinco ampliar seu papel de protagonista chave ao moldar o rumo das relações do país. Ao passo que o sistema democrático do Brasil continua a se consolidar, os militares também se reestruturam e procuram um novo papel no futuro interno e externo do país.[109] Esta visão implica mudar o foco de atenção para as ameaças extra fronteiras (inclusive a cibercriminalidade) e realizar operações de segurança interna. A crescente influência das forças armadas nos assuntos civis ainda passará por prolongadas análises internas. Com certeza as forças armadas brasileiras desfrutam de inusitado apoio favorável pela população. Em que pese o histórico da ditadura militar no país, as forças armadas são tidas pela maioria do povo como a mais confiável instituição nacional.[110]

Parte pelo menos do motivo sobre a necessidade de debate acerca do papel das forças armadas nacionais na cibersegurança, tem a ver com o segredo que acoberta boa parte de suas atividades. Não há registro público ou informações detalhadas sobre quando o exército iniciou o desenvolvimento de sua capacidade operacional no ciberespaço. Somente a partir de 2008, este campo passou a fazer parte oficialmente da doutrina militar. Naquele ano a cibernética foi designada um dos três grandes pilares da renovação das forças armadas, junto com o setor aeroespacial e a energia nuclear.[111] De lá para cá, o Ministério da Defesa investiu recursos expressivos no setor. Recentemente o mesmo lançou a *Política de Defesa Cibernética* nacional, documento que enumera os princípios, objetivos e diretrizes que nortearão suas atividades com a matéria nos próximos anos.[112] O Ministério da Defesa indicou o Exército para liderar o desenvolvimento da capacidade de defesa cibernética (a Marinha tem a seu cargo o setor nuclear e a Aeronáutica o setor aeroespacial).

Especificamente, o Exército recebeu o controle de uma aparelhagem de supervisão dos assuntos civis: o CDCiber. O mesmo foi constituído em 2010 e se tornou operacional no final de 2011. Criou-se o CDCiber com o fim de coordenar as atividades de defesa cibernética. Conforme o observado, o CDCiber se situa entre os níveis estratégicos e operacionais da arquitetura brasileira da defesa ciber-

109 Consulte http://g1.globo.com/brasil/noticia/2012/08/em-transformacao-exercito-planeja-estar-totalmente-equipado-em-10-anos.html.

110 Veja http://fgvnoticias.fgv.br/node/2847.

111 Veja a Estratégia Nacional de Defesa (END), a partir de 2008.

112 O conteúdo do documento consta em http://www.defesanet.com.br/cyberwar/noticia/9128/MD---Politica-Cibernetica-de-Defesa.

nética, em coordenação com o MD, o qual por sua vez recebe ordens do GSI-PR. Esta estratégia inclui as atividades cibernéticas de cinco áreas chave: Inteligência, Ciência e Tecnologia, Capacidade Operacional, Doutrina e Recursos Humanos. O objetivo principal do CDCiber é a proteção das redes militar e governamental contra ataques internos assim como externos. Eventualmente, o mesmo tratará de proteger a integridade da infraestrutura nacional de informática. O CDCiber possui um simulador de ciberguerra, um laboratório de análise códigos virtuais maléficos, além de quase cem especialistas com treinamento em cibersegurança.[113] De igual forma, o CDCiber é convocado para garantir a segurança durante megaeventos internacionais e cumpre a legislação nacional que delega às forças armadas a segurança em eventos oficiais e públicos, "em especial os que contarão com a participação de chefes de governos/estados estrangeiros."[114]

## Equilíbrio entre ameaças e reações

■ Uma grande indagação trata da reação às ameaças cibernéticas pelo estado brasileiro quanto às dimensões dos riscos correlatos. Há preocupações de que a reação das forças armadas e da segurança pública poderá ser não apenas desproporcional, mas servir para solapar as liberdades civis conquistadas a duras penas. Há uma boa quantidade de motivos para fortalecer a capacidade de lidar com as ameaças cibernéticas, sendo que não todas estas digam respeito a ameaças reais palpáveis. Antes, o Brasil utiliza as ameaças cibernéticas para reforçar suas habilidades internas e ampliar sua influência geopolítica. Há diversos riscos relativos à atual abordagem.

Primeiro, a arquitetura da cibersegurança no país outorga competências nítidas a seus principais agentes em um campo por natureza mal definido. Teoricamente a Polícia Federal está encarregada de combater a criminalidade comum (inclusive as investigações), ao passo que o Exército deveria se preparar para a ciberguerra (inclusive a defesa do ciberespaço nacional contra a ciberguerra e o ciberterrorismo, formulando iniciativas ofensivas caso necessário). No entanto, a questão da atribuição continua extremamente difícil no ciberespaço. Com frequência, continua impossível definir com certeza absoluta quem ou o que esteja por trás de uma grave ação do cibercrime, detectar sua origem ou que motivou

113 Veja http://www.estadao.com.br/noticias/nacional,exercito-se-arma-para-defender-o-espaco-cibernetico-brasileiro,729291,0.htm.

114 Veja o Decreto no. 3897 de 2001 em http://www.planalto.gov.br/ccivil_03/decreto/2001/d3897.htm.

seus autores. Com efeito, a cibercriminalidade é com frequência recrutada pelos governos para uma ampla gama de atividades. Tal fato poderá levar o Exército a se ver em situações onde não haverá de se colocar, em termos lícitos ou operacionais. O que também indica a razão crítica da colaboração entre agências – em especial em inteligência.

Segundo, o discurso de segurança das agências que se ocupam da cibersegurança e de ações de defesa é por natureza tendenciosa. A maioria dos órgãos de segurança sustenta que todos os riscos cibernéticos acima referidos são bastante reais, perigosos e iminentes. Grande parte dos militares fazem alusão a "espaços sem governo" e "faroeste" ao se referir ao ciberespaço. Regra geral, tal terminologia vem acompanhada de afirmações sobre a necessidade de conquistar e controlar este espaço.[115] Por exemplo, o General José Carlos Santos, antigo comandante do CDCiber, observou que seria possível empregar a ciberinteligência do Exército para informar outras autoridades sobre "movimentos suspeitos e mobilização em torno de protestos sociais passíveis de subverter a ordem pública…" [116] Conforme observamos, foi este o caso quando o CDCiber e a ABIN deram início ao monitoramento sistemático da mídia social no Brasil através dos programas Guardião e Mosaico. Dada a experiência recente do país com o autoritarismo, este tipo de retórica e prática dá causa a desconforto por parte de muitas pessoas.[117] A matéria se torna ainda mais problemática, visto que no futuro próximo os militares poderão ter acesso a dados civis. Com certeza, recentemente o governo anunciou que as redes da administração pública federal estarão ao alcance do CDCiber, algo que na atualidade é responsabilidade de um órgão civil, o DSIC.[118] Tais acontecimentos surtem maiores preocupações no tocante ao controle democrático das forças armadas e a ampliação dos direitos à privacidade.[119]

Terceiro, há iniciativas em elaboração e implantação despidas de estratégia nítida, uniforme e previsível. Toda a documentação oficial com orientações ou diretrizes relativas à cibersegurança são mais descritivas do que normativas. Observe-se em especial o *Livro Verde: Segurança Cibernética no Brasil* (2010) e

115 Estas reivindicações são observadas na República Federativa do Brasil, Presidência da República, Secretaria de Assuntos Estratégicos (2011). Veja por exemplo páginas 16, 31 e 32.

116 Entrevista em janeiro de 2014.

117 Veja http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00-GENERAL+JOSE+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.html.

118 Veja http://www.estadao.com.br/noticias/nacional,exercito-se-arma-para-defender-o-espaco-cibernetico-brasileiro,729291,0.htm.

119 Veja http://oglobo.globo.com/pais/exercito-monitorou-lideres-de-atos-pelas-redes-sociais-9063915.

*SAE Desafios Estratégicos para a Segurança e Defesa Cibernética* (2011).[120] Do seu lado, a *Estratégia Nacional de Defesa* (2008) não deixou claro como integrar a cibersegurança em uma estratégia abrangente, mesmo que o documento eleva a cibernética como esteio do estamento militar nacional no século vinte e um. O *Livro Branco de Defesa Nacional* (2012b)[121] deverá verter luz sobre estas questões, porém aguarda a aprovação da Presidência. A atual *Política Cibernética de Defesa* do Ministério da Defesa apenas estabelece princípios, objetivos e diretrizes elementares para a consolidação cibernética em específico na esfera da defesa.

Por fim, recursos escassos são desviados com regularidade das grandes prioridades e gastos de forma inadequada. Embora as ameaças principais ao ciberespaço nacional estejam provavelmente ligadas ao crime econômico e deverão resultar em iguais aumentos na alocação de recursos para a segurança pública, as forças armadas vem recebendo a maior parcela de apoio.[122] Por exemplo, além dos custos de seu lançamento, o CDCiber recebeu US$ 60 milhões em 2012[123] e receberá mais US$ 200 milhões no decorrer de 2015.[124] Conforme estimativas constantes do *Livro Branco de Defesa Nacional*, o orçamento esperado para a defesa cibernética é de cerca de US$ 420 milhões até 2035, tratando-se na verdade de uma pequena parcela de todo o orçamento militar projetado para este prazo.[125]

120 O Livro Verde da Segurança Cibernética (2010) é fruto de um grupo de trabalho no GSI. O mesmo expõe o que considera os aspectos chave da cibersegurança no Brasil (veja mais na nota de rodapé 161). "Desafios Estratégicos para Segurança e Defesa Cibernética" (2011) é o documento resultante da conferência da alto nível organizada pela Secretaria de Assuntos Estratégicos da Presidência (SAE). O mesmo traz colaborações de especialistas e autoridades brasileiras do campo da cibernética.

121 O Livro Branco de Defesa Nacional é o primeiro do gênero no Brasil. Sua produção foi antecedida de consultas dentro do governo, e também junto à sociedade civil. O mesmo abrange todos os aspectos da política de defesa nacional e articula a visão estratégica de longo prazo das forças armadas.

122 É desconhecido o total de recursos dirigidos à segurança pública. Não obstante, há indícios através de informantes chave de que o valor investido com a polícia acha-se bem abaixo do que se aplica com as forças armadas. Torna-se difícil quantificar o apoio à polícia, em razão da forma de distribuição dos recursos a múltiplas forças policiais.

123 Em 2012, alocou-se R$ 5 milhões com um aplicativo de simulação de software (de autoria de um empresa brasileira). Trata-se de parte da estratégia de integrar a cibersegurança com projetos mais amplos de desenvolvimento no país, conforme proposta constante do Livro Verde de cibersegurança. Veja República Federativa do Brasil, Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações (2010). Veja também http://g1.globo.com/brasil/noticia/2012/08/em-transformacao-exercito-planeja-estar-totalmente-equipado-em-10-anos.html.

124 Veja http://www.tecmundo.com.br/tecnologia-militar/37801-exercito-deve-receber-r-400-milhoes-para-prevencao-de-guerra-cibernetica-.htm.

125 Veja República Federativa do Brasil, Ministério da Defesa (2012b) .

Há também preocupações legítimas de que a forma de aplicação destes recursos é ineficiente e nada eficaz.[126] Divulgações recentes constataram que o orçamento do país para 2012 não foi inteiramente aplicado,[127] tendo sido quase todo empregado na construção das instalações do CDCiber.[128] O valor alocado foi mínimo no desenvolvimento de tecnologias, capacidade de imóveis a treinamento de pessoal. O motivo comunicado pelo Ministério da Defesa foi que "aplicar US$ 50 milhões para a defesa cibernética nos dias de hoje significa que o Brasil terá que adquirir tecnologia de fora."[129]

## PROJEÇÃO DO *SOFT POWER* INTERNACIONALMENTE

■ Um fator chave que influencia os investimento brasileiros na cibersegurança é seu desejo de se posicionar como protagonista global em assuntos internacionais de paz e segurança. O *status* mais ou menos recente do Brasil como potência emergente vem criando um real impacto internamente. Em sua procura de afirmação no cenário internacional, o Brasil fortalece seu arsenal de poder duro, ou militar. O Brasil também decididamente começa a alavancar seu poder brando no exterior, com o emprego de sua capacidade civil. Por exemplo, o Brasil procura destacar iniciativas bem sucedidas de política interna em setores chave, para angariar influência geopolítica. Governança e segurança cibernética são novas, desejáveis na linguagem popular, áreas de exploração. Possuem também a vantagem de serem bastante econômicas em comparação, por exemplo, com a ampliação das habilidades militares ou de manutenção da paz. O ciberespaço continua em evolução, o que permite aos novos participantes adotar medidas pioneiras e liderar as agendas multilaterais.

126 Embora os militares recebam mais recursos do que a segurança pública, não significa necessariamente que seja adequado. O Brasil é uma potência séria e deveria ser capaz de custear questões internacionais de cibersegurança (não restritas pela geografia) e fortalecer suas reações a questões legitimamente nacionais. De um orçamento de defesa total de US$ 30 bilhões (2012-2015), o orçamento específico de US$ 250 milhões em cibernética é minúsculo em face das atuais ameaças cibernéticas. Veja http://g1.globo.com/jornal-da-globo/noticia/2013/07/governo-destina-baixo-orcamento-para-seguranca-cibernetica.html.

127 Uma fonte da mídia indicou que houve aplicação de apenas 8,9% do orçamento de 2012. Veja http://noticias.terra.com.br/brasil/brasil-usou-89-do-orcamento-para-defesa-cibernetica,76b782fb0acdf310VgnVCM3000009acceb0aRCRD.html.

128 Veja http://www.bloggingsbyboz.com/2013/07/brazils-cybersecurity-budget-is-mess.html.

129 Veja http://www1.folha.uol.com.br/mundo/2013/07/1312345-gastar-r-100-mi-em-ciberdefesa-significa-comprar-tecnologia-de-fora-diz-amorim.shtml.

Há uma série de reivindicações por parte do Brasil com relação ao incremento de suas habilidades de poder duro e brando no ciberespaço. Por exemplo, o CDCiber é a primeira unidade cibernética militar exclusiva na América Latina. As URCCs da Polícia Federal, embora em formação, oferecem um modelo de segurança pública e colaboração judicial internamente e entre os países e regiões. O Brasil também ostenta o desenvolvimento e aplicação de estratégias de cibersegurança projetados para Megaeventos. Ademais, em breve o Brasil pode ter em breve uma estratégia nacional de segurança e defesa cibernética das mais abrangentes no mundo. E talvez o mais expressivo, o Brasil criou a primeira Declaração dos Direitos digital[130] e lançou a iniciativa da ONU de promover a soberania digital. Todas estas atividades, embora não necessariamente coerentes ou coordenadas internamente, sugerem que o país reivindica seu crédito na formulação das agendas internacional e regional sobre cibersegurança.

Ao mesmo tempo as autoridades nacionais têm criticado ativamente e procuraram reformular o regime atual de cibersegurança. Por exemplo, o governo tem criticado a *Convenção da Cibercriminalidade* (Convenção de Budapeste de 2001) do Conselho da Europa, o qual até a data é o único conjunto de normas internacionais legalmente válidas que regem questões relativas à cibercriminalidade. O Brasil alega que o processo de redação excluiu propositadamente os não integrantes do Conselho, e logo se opõe aos países fora da União Europeia. Entretanto, o Brasil se adiantou juntamente com a UNODC na redação de uma convenção internacional sobre a cibercriminalidade, tendo angariado o apoio de outros países da América Latina e do Caribe. Tomou-se esta decisão durante o 12º Congresso da ONU sobre a Repressão ao Crime e Justiça Criminal, realizado em 2010 em Salvador, Bahia, embora o processo evolua mais lentamente do que se esperava.[131]

Há também inquietação sobre as negociações globais do Brasil acerca da soberania digital bem como o potencial de balcanização da Internet. Vejamos, o Brasil apoiou até certo ponto a China e o Irã durante a Conferência Internacional da ITU em Dubai (2012). O Brasil estava a favor da regulamentação da Internet através de um tratado internacional sob a supervisão da ONU. No entanto, há receio de que esta abordagem daria poderes excessivos aos governos e levaria à regulamentação potencialmente morosa, restritiva e invasiva. Estas preocupações

130 Inclui o reconhecimento especial recente por Tim Berners Lee. Veja http://www1.folha.uol.com.br/poder/2013/05/1280037-criador-da-web-elogia-brasil-por-projeto-que-vai-regular-a--internet.shtml.

131 Veja http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/.

se tornam intensas pelo fato de que o controle da Internet pelos Estados Unidos e pela Internet Corporation for Assigned Names and Numbers (ICANN), com base nos Estados Unidos, está em fase de se afrouxar de modo a permitir demais governos, ONGs e ISPs o desempenho de um papel mais proeminente. Ademais, a ITU suscitou a possibilidade de permitir a *deep package inspection* (DPI), o primeiro passo para a censura, já em vigor em alguns países.[132] No entanto, são alvissareiros os sinais de que a abordagem do Brasil poderá mudar. Juntamente com a Alemanha e a ICANN, o governo brasileiro patrocinou recentemente um evento de alto nível, o NetMundial, em São Paulo. O Brasil propôs o estabelecimento de um *Marco Civil* global e pediu mais *multistakeholderism* com relação à governança da Internet.[133]

No nível regional, o Brasil colabora estreitamente com esforços de combate ao cibercrime, em coordenação com a Organização dos Estados Americanos (OEA) e sua *Estratégia Interamericana de Combate às Ameaças contra a Cibersegurança* (adotada pela Assembleia Geral da OEA em 2004). *O Brasil não apenas adotou os pilares da cibersegurança esboçadas pela OEA, mas também trabalha com afinco no aperfeiçoamento das medidas propostas. O país organizou conferências com os três departamentos da OEA que administram a implantação da Estratégia e com frequência desloca especialistas em apoio de missões de assistência técnica, participando de eventos em toda a América Latina bem como o Caribe.134 Em sua própria região da América do Sul, o Brasil promove a agenda dentro da UNASUR – União das Nações Sul-Americanas.* Reuniões entre os Ministros da Defesa, Justiça e Interior dos 12 estados-membro visaram a criação de mecanismos de promoção da cooperação contra o crime organizado transnacional, em especial a cibercriminalidade.[135]

O Brasil também lidera no desenvolvimento da cooperação bilateral de administração da cibersegurança e defesa cibernética. O país celebrou com a Rússia em 2010 o Tratado de Não Agressão com Armas de Informática, o primeiro tratado bilateral do gênero. Além de resultar no tratado de não agressão, o mesmo dispõe do intercâmbio aperfeiçoado de informações, fortalecimento de capacidade e exercícios conjuntos de ciberguerra. Embora o tratado soe estranho, há sinais

132 Veja http://www1.folha.uol.com.br/colunas/ronaldolemos/1210826-brasil-se-alinha-a-china-e-ira-em-leis-da-internet.shtml A posição do Brasil sobre a DPI continua pouco clara.

133 Para maiores informações sobre os resultados do evento, veja http://netmundial.br/.

134 Veja Diniz e Muggah (2012).

135 Veja http://www.unasursg.org/index.php?option=com_content&view=article&id=516:ultima-unasur-debate-cooperacion-regional-en-crimen-trasnacional-organizado-y-nuevas-amenazas&catid=66:noticias-unasur.

de cooperação em alta com a cibersegurança, entre os integrantes dos BRIC.[136] Ao mesmo tempo os Ministros de Defesa de Argentina e Brasil assinaram em 2011 uma Declaração Conjunta de revisão da cooperação bilateral no setor de defesa, inclusive com relação à informática e cibersegurança. De igual forma, os Ministros de Defesa de Brasil, Chile e Colômbia realizaram sessões restritas no Pentágono dos EUA, destinadas a revisar as ameaças cibernéticas, e solicitaram apoio para o fortalecimento da resiliência das redes de hardware e software contra violações.

## CONCLUSÕES

■ O Brasil vem incrementando sua arquitetura de cibersegurança e ao mesmo tempo consolidando sua posição de potência emergente. As autoridades públicas visam não apenas a cibercriminalidade interna e o ciberativismo, mas também a expansão da habilidade do estado para a redução das ameaças cibernéticas, em nível internacional. Na reação estratégica do Brasil a ambos os riscos, acha-se o CDCiber na condição de pilar básico. No entanto, a ênfase na reação militar poderá ser fora de propósito com as ameaças reais (e não existenciais) que assombram o país e a sociedade como um todo. O fato permanece de que o Brasil enfrenta relativamente poucas ameaças cibernéticas por governos estrangeiros ou grupos terroristas. No entanto, o aumento dos protestos digitais e de cibercriminalidade está mais do que evidente, porém recebem relativamente menor atenção e investimentos. Urge a necessidade de uma leitura mais informada e com base em evidências das ameaças contra o país, e sua abordagem através da cuidadosa apreciação do equilíbrio entre a segurança pública e os direitos individuais.

A arquitetura de cibersegurança do Brasil acha-se ainda em evolução. Há ainda linhas conflitantes de responsabilização entre as instituições, prioridades distorcidas de custeio, debate público confuso, medidas legislativas opostas e a importação sem critério de soluções estrangeiras para os desafios internos. Há críticos que argumentam que a "reação" do estado às ameaças cibernéticas é mal concebida e não se coadunam com os reais desafios que o país enfrenta. Em seu lugar, os militares "capturaram" recursos para a defesa cibernética, que implicam em perigos, de modo geral, para as liberdades civis. Outro importante desafio se encontra na ausência de coordenação entre as instituições do governo e a frag-

136 Veja http://www.scmp.com/news/china/article/1276995/brics-emerging-economies-expand-co-operation-internet-security.

mentação das reações. E ainda, o engajamento limitado no Brasil da sociedade civil nos debates sobre a cibersegurança significa que as forças armadas estão desimpedidas para a ampliação de seus interesses corporativos.[137] Em seu lugar, estas tendem a adotar também abordagens estanques, com algumas tendências com foco em questões de defesa, outras em policiamento, e ainda outras em soberania digital, liberdades civis, etc. O essencial é a estratégia equilibrada da cibersegurança que avalie com precisão as ameaças em curso, ao mesmo tempo elaborando reações proporcionais e prospectivas.

O primeiro passo seria a concentração nas lacunas de conhecimento. Há um debate vivo no Brasil sobre as múltiplas realizações positivas com relação à *e-governance*, cidades inteligentes, soberania digital e demais TICs novas.[138] Há, por estranho que pareça, silêncio sobre questões relativas a cibersegurança e defesa cibernética. Quando há debates, estes tendem a permanecer confinados aos mais altos níveis de governo, forças armadas, órgãos de segurança pública e meios acadêmicos de banda estreita. Caso o Brasil desenvolva uma reação mais equilibrada e proporcional contra as ameaças emergentes, a cibersegurança deverá ser aceita como característica integral da governança cibernética e determinante chave dos direitos civis, sociais e políticos. No mínimo, os estudiosos brasileiros necessitam de um melhor entendimento da dinâmica dos hackers e dos grupos da cibercriminalidade, das formas do crime tradicional migrar para a rede, das maneiras de adaptação pelas forças de segurança de novas tecnologias de vigilância e demais questões. Significa também que o governo deverá incentivar um mais amplo debate com uma estratégia clara de comunicações sobre as exigências da cibersegurança e quais as suas formas.

O segundo passo é iniciar o debate sobre o conteúdo das estratégias ponderadas e eficientes para fazer face às ameaças cibernéticas. Visto que os orçamentos alocados às questões relativas à cibernética são flexíveis e de difícil previsão, há bastante concorrência burocrática por verbas. Os órgãos militares, de segurança pública e civis são passíveis de exagerar os riscos de modo a aumentar seu acesso às verbas. As negociações mais informadas contribuiriam para um carteira mais equilibrada de cibersegurança. As principais prioridades no Brasil incluem a melhora na capacidade investigativa das polícias federais e estaduais, inclusive no

137 Veja em Diniz e Muggah (2012) a visão geral da maneira da sociedade civil lidar com a cibersegurança na América Latina.

138 Veja por exemplo as obras dos grupos de pesquisa, como ITS-Rio, CTS-FGV, UFABC (Grupo de pesquisa "Cultura Digital e Redes de Compartilhamento") e UNICAMP (Grupo de pesquisa "Políticas Públicas de Acesso à Informação").

tocante às perícias cibernéticas. De igual modo, torna-se essencial aperfeiçoar a coordenação entre as polícias estaduais de modo a melhor se antecipar e lidar com os crimes cibernéticos. Talvez mais radical, porém estratégia adotada em outros países, será identificar e recrutar hackers brasileiros que colaborem no aperfeiçoamento das habilidades do estado. O Ministro de Ciência e Tecnologia no Brasil já seu sinais nesta direção, e convidou hackers a avaliar os riscos de segurança na rede do governo federal. O CDCiber também realizou movimentos neste sentido.[139] No entanto, o czar da cibersegurança no Brasil determinou que todo hacker é criminoso (e que o hacker nacional não possui a habilidade do estrangeiro).[140]

Em terceiro lugar, o Brasil deverá dar início a um debate sofisticado sobre o que constitui uma ameaça cibernética bem como os tipos de reação necessárias. Há uma tendência de simplificar o debate sobre ameaças cibernéticas e cibercriminalidade. Em algumas hipóteses, diversas atividades se combinam. Em outras, a tendência é exagerar o foco em determinada categoria de ameaça. Caso o Brasil adote uma abordagem mais progressiva, será necessária maior ênfase na melhora de qualidade de educação e debate. O fato é que a consciência sobre cibersegurança no Brasil é bastante baixa.[141] Há necessidade de um esforço organizado para elevar a compreensão e comprometimento, como ocorre na América do Norte e Europa, entre outros. Os debates do gênero deverão ser acessíveis a uma gama de interesses e possuir base em dados empíricos comprovados. Caso o Brasil deseje uma arquitetura de cibersegurança adequada a seus fins, torna-se imperativo o debate de qualidade.

Robert Muggah é diretor de pesquisas do Instituto Igarapé, encarregado de pesquisas na SecDev Foundation e principal cientista social do SecDev Group.

Misha Glenny é autor internacional sobre assuntos que variam dos Balcãs e do Brasil ao crime organizado e aos crimes cibernéticos.

Gustavo Diniz foi investigador adjunto no Instituto Igarapé.

139 Veja http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00-GENERAL+JOSE+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.html.

140 Veja http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=27324&sid=21 e http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=27454&sid=15#.UaKzStLU-Io.

141 Diz-se que cerca de 42% dos brasileiros desconhecem que os vírus de computadores passam despercebidos (a média global é de 40%). Veja Norton/Symantec "*Norton Cybercrime Report 2012*".

## REFERÊNCIAS

CANONGIA, C. e MANDARINO, R. Segurança cibernética: o desafio da nova Sociedade da Informação. *Parceria Estratégica*. Brasília-DF, vol. 14, n. 29, p. 21-46, jul-dez, 2009.

DINIZ, G. e MUGGAH, R. *A Fine Balance: Mapping Cyber-(In)security in Latin America*. Strategic Paper 2. Igarapé Institute: Rio de Janeiro, junho, 2012. Disponível em http://igarape.org.br/a-fine-balance-mapping-cyber-insecurity-in-latin-america/

FGV-CPS . *Mapa da Inclusão Digital*. Marcelo Neri (Coord). Rio de Janeiro, 2012a. Disponível em: http://www.cps.fgv.br/cps/telefonica/

FGV-CPS. *O Início, o Fim e o Meio Digital: Cobertura, Capacidades e Conectividade*. Marcelo Neri (Coord). Rio de Janeiro, 2012b. Disponível em: http://www.cps.fgv.br/cps/vivo/

GLENNY, M. *Dark Market:* Cyberthieves, Cybercops and You, 2011.

GLENNY, M. *McMafia:* A Journey Through the Global Criminal Underworld. Nova York: Random House, 2009.

INTERNATIONAL INTELLECTUAL PROPERTY ALLIANCE – IIPA. *Special 301 Report on Copyright Protection and Enforcement: Brazil,* fevereiro, 2012. Disponível em http://www.iipa.com/rbc/2012/2012SPEC301BRAZIL.PDF

INTERNATIONAL TELECOMMUNICATION UNION. *Understanding Cybercrime: A Guide for Developing Countries*. Genebra: ITU-D ICT Applications and Cybersecurity Division, 2009.

KISHETRI, N. *Cybercrime and Cybersecurity in the Global South*. Palgrave MacMillan: Reino Unido, 2013.

MUGGAH, R. e GLENNY, M. Brazil´s Cybersecurity Conundrum, Council on Foreign Relations, janeiro 2015, http://blogs.cfr.org/cyber/2015/01/12/guest-post-brazils-cybersecurity-conundrum/.

MUGGAH, R., DINIZ, G. e M. GLENNY. Brasil aposta na militarização da segurança cibernética, Le Monde Diplomatique, novembro, 2014.http://www.diplomatique.org.br/acervo.php?id=3082.

MUGGAH, R. e DINIZ, G. Using Information and Communication Technologies for Violence Prevention in Latin America. In: MANCINI, F. (ed.) *New Technology and the Prevention of Violence and Conflict.* Nova York: International Peace Institute, abril, 2013. Disponível em: http://www.undp.org/content/dam/undp/library/crisis%20prevention/20130410NewTechnologyandPreventionofViolenceandConflictv2.pdf

OLLINGER, M. La Propagación del Crimen Organizado en Brasil: Una mirada a partir de lo ocurrido en la última década". In: GARZÓN. G. e

OLSON, E. (eds). *La Diáspora Criminal:* La difusión transnacional del Crimen Organizado y cómo contener su expansión. Woodrow Wilson International Center for Scholars – Latin America Program. Washington D.C, 2013. http://www.wilsoncenter.org/publication/Criminal Diaspora

REPÚBLICA FEDERATIVA DO BRASIL, Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações. *Livro Verde da Segurança Cibernética no Brasil*. Mandarino, R. e Canongia, C. (Eds). Brasília, 2010. Disponível em: http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf

REPÚBLICA FEDERATIVA DO BRASIL, Ministério da Defesa. *Estratégia Nacional de Defesa*, 2008. Disponível em http://www.mar.mil.br/diversos/estrategia_defesa_nacional_portugues.pdf

REPÚBLICA FEDERATIVA DO BRASIL, Ministério da Defesa. "Política Cibernética de Defesa". Portaria Normativa No 3389 (dezembro 21), Gabinete do Ministro. DOU Seção 1 – No. 249 (dezembro 27), 2012a.

REPÚBLICA FEDERATIVA DO BRASIL, Ministério da Defesa. *Livro Branco de Defesa Nacional*. Brasília, 2012b. Disponível em: https://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf

REPÚBLICA FEDERATIVA DO BRASIL, Presidência da República, Secretaria de Assuntos Estratégicos. Desafios Estratégicos para a Segurança e Defesa Cibernética. Brasília, 1ª edição, 2011. Disponível em http://www.sae.gov.br/site/?p=6151

TREND MICRO. *Latin American and Caribbean Cybersecurity Trends and Government Responses*. Maio, 2013. Disponível em http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends--and-government-responses.pdf

WÆVER, O. Securitization and Desecuritization. In: LIPSCHUTZ, R. ed. *On Security*. Nova York: Columbia University Press, 1995.

# Operações cibernéticas militares e as implicações perante a Lei Internacional

JULIA DORNSBUSCH

■ As operações cibernéticas têm grande importância em uma guerra e desempenham papel significativo nas relações entre os países. Este artigo pretende dar uma visão geral das implicações relevantes perante a lei internacional.

No que se refere a um regime de paz, a pergunta que se faz é em que circunstâncias as operações cibernéticas violam a proibição do uso de força militar contra outro Estado e a proibição de interferir em seus assuntos domésticos. Existe um consenso geral quanto ao fato de que apenas as operações cibernéticas que causam danos físicos podem ser consideradas como uso de força proibida. No entanto, a maioria das operações cibernéticas entre Estados são usadas para angariar informações (incluindo espionagem), o exercício da pressão política com o objetivo de fazer propaganda ou para dar apoio a operações armadas, como diversos exemplos comprovam. Ainda que envolvam um dano material considerável, não causam danos físicos. Com este pano de fundo, o artigo se concentra nas implicações legais de operações cibernéticas em tempos de paz no que diz respeito à interferência proibida em assuntos domésticos dos Estados e a noção de soberania de Estado. Neste artigo, ficará claro que os Estados precisam refinar e chegar a um acordo sobre o entendimento comum do conceito de soberania e outros princípios básicos da lei internacional para regular as operações cibernéticas.

Como as operações cibernéticas militares ganham relevância significativa em tempos de guerra, suas implicações sob a lei em caso de conflito armado não podem ser deixadas fora da equação. Assim, na terceira parte, o texto ilustra o conceito de "ataque", que tem importância crítica para a proteção de civis durante o conflito armado. A interpretação estrita de "ataque" pelos Estados dentro da lei atual será criticada, porque não inclui muitas operações cibernéticas que podem

desencadear consequências humanitárias calamitosas em tempos de guerra. Além do mais, as operações cibernéticas que possibilitam ataques armados (convencionais) e sua regulamentação seguindo as regras do engano em conflitos armados estão sendo contestadas.

O artigo conclui com uma avaliação das medidas defensivas contra operações cibernéticas sob a lei da Responsabilidade do Estado. Dentro deste contexto, destacam-se as obrigações legais dos Estados dentro da lei internacional sobre segurança cibernética e a necessidade urgente da cooperação internacional entre os Estados.

É interessante enfatizar que o artigo não se detém em operações militares por Estados ou, em outras palavras, em ataques cibernéticos que são atribuídos a um Estado dentro da lei de Responsabilidade de Estado. Portanto, em todos os exemplos discutidos, se parte do princípio que a responsabilidade dos Estados pode ser provada.

## ATAQUES CIBERNÉTICOS COMO MEIO DE PRESSÃO POLÍTICA, PROPAGANDA E ESPIONAGEM

■ Ao examinar incidentes cibernéticos na prática, fica claro que as operações cibernéticas dos Estados perseguem principalmente os seguintes objetivos: obter informação (espionagem), apoiar ou preparar ataques armados, exercer pressão política e disseminar propaganda. Seria possível questionar porque tamanha determinação dos objetivos subjacentes dos ataques cibernéticos é necessária ou até mesmo útil. Mas entender como e com que propósitos países usam operações cibernéticas nas relações internacionais é essencial para identificar as regras mais adequadas da Lei Internacional para regulamentação, para detectar incertezas legais e desenvolver estratégias adicionais para a garantia da segurança cibernética mundial. Assim, um resumo de alguns incidentes virtuais de grande relevância será apresentado a seguir.

Não há um dia em que os meios de comunicação não informem sobre algum incidente de espionagem cibernética. Há pouco tempo, o governo dos Estados Unidos, especificamente, foi acusado não só de espionar cidadãos estrangeiros, mas também de mirar na comunicação governamental de países estrangeiros. Em geral, esforços para obter dados sensíveis relacionados com as capacidades militares ou econômicas de um Estado parecem ser uma prática generalizada, com uso estendido por vários países. A relevância das operações cibernéticas na espionagem é inegável.

As atividades de engano cibernético são ainda mais importantes para operações militares durante ou imediatamente antes de conflitos armados. Por exemplo, Israel manipulou o Sistema de Defesa Aérea Síria para facilitar a entrada despercebida de seus bombardeiros em território sírio, o que facilitou o ataque a uma instalação nuclear.[1]

O maior incidente cibernético, em termos de escala, e com o objetivo claro de exercer pressão política em um governo estrangeiro, aconteceu na Estônia em 2007. A remoção do Memorial de Guerra Russo do centro da cidade de Talin desencadeou manifestações violentas de cidadãos russos. Durante esse momento de agitação civil, a Estônia enfrentou uma grande variedade de ataques DDoS (Negação de Serviço Distribuído), paralisando websites governamentais e de grandes meios de comunicação e interrompendo os sistemas bancários e instalações de comunicação.[2] O envolvimento do governo russo nunca ficou comprovado, mas essas operações indubitavelmente pretendiam mudar a política do governo estoniano em relação ao deslocamento do Memorial de Guerra. De modo similar, em conjunção com o conflito armado entre a Geórgia e a Rússia em 2008, meios de comunicação georgianos e instituições financeiras do país foram atacados por meios virtuais. Os serviços de comunicação do Governo foram interrompidos e os sites governamentais foram sabotados com objetivos de propaganda. Por exemplo, retratos do presidente da Geórgia foram substituídos por imagens de Adolf Hitler.[3] A relevância dos ataques cibernéticos para a disseminação de propaganda ficou ainda mais evidente na recente crise da Crimeia. Pouco antes do referendo sobre a unificação da Crimeia com a Rússia, os habitantes da Crimeia não apenas ficaram isolados de tudo e recebiam apenas notícias geradas pelos meios de comunicação russos – imprensa e televisão,[4] e também os sites de informação e as redes sociais foram sabotados com mensagens de propaganda e informações errôneas.[5]

Por último, o vírus Stuxnet, que ocasionou efeitos adversos na velocidade do rotor das centrífugas das instalações nucleares iranianas de enriquecimento

1 *Handler, Stephanie Gosnell*, The New Face of Battelfield, 48 Standford Journal of International Law (2012), p. 209-237, 223 (with relevant references)

2 *Tikk, Eneken/Kaska, Kardi/Vihul, Liis*, International Cyber Incidents: Legal Considerations, (2010), p.18-25

3 ibid. p. 69-79.

4 BBC, Crimeans urged to vote against ‚neo-Nazis' in Kiev (13 March 2014), disponível em: http://www.bbc.com/news/world-europe-26552066, last visited: 8 February 2015.

5 BBC, Russia and Ukraine in cyber ‚stand-off' (5 March 2014) disponível em: http://www.bbc.com/news/technology-26447200, última entrada: 8 de fevereiro de 2015.

de urânio de Natanz em 2010 e seu papel especial vai ser mencionado aqui. Stuxnet foi um dos ataques virtuais mais sofisticados que o mundo testemunhou até agora. O vírus auto-replicável foi projetado especificamente para manipular o Sistema de Supervisão de Controle de Aquisição de Dados usado em Natanz de modo que potencialmente pudesse causar danos materiais às centrífugas.[6] Obviamente, esse ataque cibernético também foi usado para aplicar pressão política no Irã e forçar esse país a mudar sua política nuclear. Stuxnet foi a primeira operação virtual que realmente tinha como meta causar destruição material de objetos do mundo real.

Dentro da lei internacional atual, este fato tem particular relevância porque só operações cibernéticas que causam danos físicos ou morte ou lesões corporais são consideradas uma violação da proibição do uso da força armada, algo que discutiremos em detalhes mais adiante, em contraposição à interrupção da infraestrutura essencial dos Estados. Dentro desse cenário, a maior parte dos ataques cibernéticos acarreta implicações para a interpretação de outros princípios ou regras da Lei Internacional, como a proibição de não intervenção ou soberania nacional.

## O REGIME DE ÉPOCA DE PAZ

■ Em épocas de paz, a lei internacional, mais especificamente *ius ad bellum*, pretende manter a paz e a segurança internacionais e, portanto, geralmente proíbe o uso unilateral de força (militar) como meio político nas relações entre Estados.[7] Um Estado só pode recorrer à força para repelir um ataque armado, exercendo assim seu direito inerente à autodefesa.[8] Além disso, em função do fato de que a lei internacional é aplicável entre Estados igualmente soberanos, reconhece o direito de todo Estado de escolher seu sistema político, econômico, social e cultura, sem nenhuma interferência de outros Estados.[9] Deveria enfatizar-se que o princípio

6 *Buchan, Russell*, Cyber Attacks: Unlawful Uses of force or Prohibited Interventions?, 17 Journal of Conflict & Security Law (2012), p. 211-227, 219-220 (with relevant references).

7 Art. 2 (4) Carta das Nações Unidas.

8 Art. Carta das Nações Unidas; outra exceção seria a autorização de um Estado pelo Conselho de Segurança da ONU para o uso de medidas violentas de acordo com o Art. 39 e 42 da Carta das Nações Unidas.

9 Declaração dos Princípios da Lei Internacional sobre Relações Amigáveis e Cooperação entre os Estados, de acordo com a Carta das Nações Unidas, Resolução da Assembleia Geral da ONU 2526 anexo (XXV) (24 de outubro 1970), que é considerado direito consuetudinário (doravante: Friendly Relations Declaration); ver Art. 2 (7) da Carta da ONU.

da não intervenção e a proibição do uso da força são aplicados exclusivamente no nível interestatal, isto é, só se aplicam a atos que possam ser atribuídos a um Estado.

Como ficou demonstrado acima, as operações cibernéticas são usadas para propósitos de propaganda, espionagem e para exercer pressão política, o que suscita a pergunta sobre até que ponto essas operações são compatíveis com os princípios declarados da Lei Internacional. Aqui, o princípio da não-intervenção e da soberania do Estado têm interesse especial. Em relação à proibição do uso da força, a perturbação da infraestrutura cibernética, ocasionando meramente uma perda de funcionalidade e não a destruição (parcial) de um objeto, é algo controverso.

## INTERRUPÇÃO DA INFRAESTRUTURA CIBERNÉTICA – O USO DA FORÇA

■ Os ataques cibernéticos violam potencialmente o uso da força, se seus efeitos forem comparáveis aos das operações militares convencionais, que são considerados incompatíveis com o Artigo 2 (4) da Carta das Nações Unidas.[10] Afinal de contas, não pode fazer diferença, se pessoas morrem porque uma represa foi destruída por bombardeio aéreo ou porque os portões foram abertos por meio de um ataque cibernético. As consequências típicas (e portanto relevantes aqui) do uso da força militar são a morte ou lesões em pessoas ou danos físicos de objetos. Portanto, os ataques cibernéticos que causam diretamente mortes ou ferimentos em pessoas ou prejuízos materiais, são violações potenciais do Artigo 2 (4) da Carta da ONU, pressupondo que se mantenha um certo grau de severidade.[11] Existe o consenso de que as operações cibernéticas sem consequências na esfera física, por exemplo, a mera manipulação ou furto de dados, não podem ser consideradas como uso de força.[12]

Mais problemática é a classificação legal dos ataques cibernéticos que não têm como resultado algum dano físico, mas que levam à perda da sua funcionalidade. Parece seguro pressupor que a lei internacional não diferencia, por exemplo, se o fornecimento de eletricidade de um Estado for interrompido porque uma central elétrica foi destruída ou porque um ataque virtual prejudicou sua

10 *Schmitt, Michael* (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare (2013), Rule 11.
11 ibid. Rule 11, para. 8 + 9 a).
12 *Dinniss, Heather Harrison*, Cyber Warfare and the Laws of War (2012), p.74.

operação. No entanto, a lei atual não parece dar suporte para um tratamento igual nos dois casos. Ainda que as operações cibernéticas que levem à perda de funcionalidade de um objeto com frequência acarretem danos materiais consideráveis, como a paralisação de uma bolsa de valores, elas não violam a proibição do uso da força *de lege lata*.[13] À primeira vista, esta conclusão parece arbitrária, mas a proibição estabelecida no Artigo 2 (4) deve ser interpretada considerando-se seu objetivo e papel dentro do *ius ad bellum*. Primeiro, o esboço do histórico da estipulação reflete a intenção dos Estados, como legisladores da Lei Internacional, de excluir coerção econômica ou política.[14] Além do mais, considerando-se que alguns Estados não distinguem entre um ataque armado que desencadeia o direito de usar força militar em defesa própria, e um uso de força em escala menor, uma interpretação estrita do Artigo 2 (4) da Carta da ONU parece apropriada. Se tivermos em mente o objetivo principal do *ius ad bellum* – geralmente, proibir unilateralmente o uso da força como um meio político nas relações interestatais – o resultado de certa forma ambivalente em relação à operação cibernética que apenas perturba a infraestrutura cibernética, precisa ser aceito por enquanto. Os Estados, como legisladores, precisam considerar se a perturbação da infraestrutura virtual deveria ser incluída na proibição do uso de força no futuro e até que ponto. Uma restrição, por exemplo, para certos objetos de infraestrutura nacional crítica,[15] ou seja, ativos ou sistemas que sejam "essenciais para a manutenção das funções vitais da sociedade, saúde, segurança, bem-estar econômico ou social da população, como por exemplo, centrais elétricas, redes de transporte e redes governamentais,[16] seria algo convincente. Ademais, é evidente que um certo grau de intensidade da perturbação, tornando-a comparável à destruição do objetivo físico seria necessária.[17] A prática de Estado vai mostrar se uma abordagem mais consistente dos ataques cibernéticos e o uso da força em relações internacionais vai prevalecer.

13 *Buchan* (fn. 6), p. 212;

14 *Simma, Bruno/Khan, Daniel-Erasmus/ Nolte, Georg/ Paulus, Andreas* (eds.), Charter of the United Nations - A Commentary, 3ª edição (2012), Vol I, Art. 2 (4), p. 18.

15 ver *Roscini*, *Marco*, Cyber Operations and the Use of Force in International Law (2014), p. 55-63; *Ziolkowski, Katharina*, General Principles of International Law as Applicable in Cyberspace, in: Ziolkowski, Katharina (ed.), Peacetime Regime For State Activities in Cyberspace (2013), p. 135-188, 173

16 Diretiva 2013/40/EU sobre ataques contra sistemas de informação (12 de agosto 2013), Diretiva do Parlamento Europeu e do Conselho, Official Journal of the European Union L 218/8 – 14, p 4.

17 ver *Ziolkowski* (fn. 15), p. 173.

## INTERVENÇÃO NOS ASSUNTOS INTERNOS DE UM ESTADO ESTRANGEIRO

■ A Lei Internacional de tempos de paz estipula a obrigação dos Estados de refrear qualquer intervenção nos assuntos domésticos de uma nação estrangeira. O escopo exato e o conteúdo do princípio de não-intervenção é alvo de controvérsia. A lei internacional não proíbe toda e qualquer interferência, mas exige que a intervenção seja de caráter coercitivo e que afete exclusivamente os assuntos nacionais de um Estado.[18]

O significado desses dois elementos qualificadores, porém, não está completamente claro. Em particular, a linha divisória entre assuntos nacionais e internacionais é uma linha tênue,[19]pois a lei internacional cada vez mais se "infiltra" no *domaine réservé* dos Estados.[20] Geralmente, aos Governos é permitido que escolham suas próprias políticas (dentro dos limites da lei internacional) em relação aos temas que a lei internacional deixa para a livre determinação. Para que a intervenção seja considerada ilegal, o Governo afetado precisa ser forçado por uma nação estrangeira a adotar uma determinada política; o nível exato de coerção, porém, não está estabelecido de modo definido.[21] Evidentemente, monitoramento ou subtração de dados de informações sensíveis sobre segurança nacional em si não preenchem o padrão de coerção, já que em nenhum aspecto forçam um Estado a fazer ou deixar de fazer alguma coisa.[22]

Apesar dessas incertezas, as implicações legais dos ataques virtuais em relação ao princípio da não-intervenção podem ser examinadas concentrando-se em alguns tipos de ações reconhecidas como intervenções ilegais sob a lei internacional atual. Essas são ações militares muito próximas do uso da força ou que envolvem a ameaça do uso de força, o apoio de atividades subversivas ou armadas de atores não estatais com o objetivo de derrubar o Governo de outras nações e o impedimento coercitivo do exercício das funções estatais centrais por parte do Governo de outra nação.[23]

---

18 ICJ, Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America), Merits, Judgement of 27 June 1986, ICJ Reports p. 14, p. 205 (doravante: Nicaragua case)

19 *Gill, Terry*, Non-Intervention in the Cyber Context, em: Ziolkowski, Katharina (ed.), Peacetime Regime for State Activities in Cyberspace, p. 217-238, 217.

20 Especially due to the development of Human Rights and International Criminal law.

21 *Ziolkowski* (fn. 15), p. 165.

22 *Gill* (fn. 19), p. 232.

23 ibid. p. 222.

Em relação ao último fato discutido acima, os ataques cibernéticos que afetam infraestruturas essenciais, mas não causam danos materiais são particularmente relevantes. As perturbações sistemáticas que não sejam de curto prazo de uma infraestrutura crítica têm o potencial de coagir um Estado a mudar sua política e se objetivo era precisamente esse, provavelmente constituem intervenções proibidas. Os ataques de negação de serviço perpetrados contra a Estônia em 2007, que paralisaram sistemas bancários, sites importantes do Governo e páginas de meios de comunicação, atrapalhando a comunicação do Governo com seus cidadãos e também com o mundo exterior, pretendiam sem dúvida mudar a política da Estônia em relação à remoção do Memorial da Guerra da Rússia. Além disso, se estenderam por três semanas, o que deveria ser intensidade suficiente para que se considerassem esses ataques – desde que se pudesse provar a responsabilidade da Rússia – como intervenções ilegais.[24]

Outras ações claramente proibidas pelo princípio da não-intervenção são aquelas que ajudam a atores não estatais, com o objetivo de derrubar o regime de outro Estado por meios violentos.[25] A proibição não engloba apenas assistência financeira ou logística durante uma revolta em ebulição, mas simplesmente a incitação à derrubada violenta do Governo já é proibida. Isso leva à pergunta sobre a disseminação de propaganda por meios virtuais. O espaço cibernético oferece uma grande variedade de possibilidades de disseminação de informações falsas ou propaganda por meio de redes sociais ou e-mails. Além disso, os ataques cibernéticos que desfiguram sites e perturbam ou manipulam a mídia ou sistemas de transmissão ao vivo, ocorreram repetidamente no passado recente, como por exemplo na Crise da Crimeia ou na guerra Rússia-Geórgia em 2008.

Para ser considerada uma violação do princípio da não-intervenção, a propaganda disseminada por uma nação estrangeira precisa ser de natureza subversiva no sentido de instigar o uso da violência para forçar a mudança de Governo ou regime. O mero apoio político a um movimento de oposição ou desaprovação da política externa de outro país não é suficiente para tanto.[26] Considerando esse padrão, campanhas difamatórias, por exemplo, ou a sabotagem de sites governamentais, normalmente não serão consideradas uma intervenção ilegal.[27] De fato,

24 *Buchan* (fn. 6), p. 225-226.

25 Friendly Relations Declaration (fn. 9); Nicaragua case (fn. 18), para. 205.

26 *Gill* (fn. 19), p. 223; *Pirker, Benedikt*, Territorial and Integrity and the Challenges of Cyberspace, in: Ziolkowski, Katharina (ed.), Peacetime Regime for State Activities in Cyberspace, p. 189-216, 201.

27 *De Brabandere, Eric*, Propaganda, in: Wolfrum, Rüdiger (ed.), Max Planck Encyclopedia of Public International Law (2012), Vol. VIII, p. 510-511.

os fatos específicos de cada caso precisam ser levados em conta. Em épocas de agitação contínua, será mais provável que a disseminação de propagandas ou de informações enganosas seja definida como campanha subversiva.[28] Na ausência de perturbações civis, a propaganda precisa incitar claramente ao uso da violência porque uma campanha defendendo um regime de paz não seria qualificada como uma intervenção proibida.[29] O conteúdo da propaganda ou da informação disseminada, portanto, é crucial neste aspecto.

Dentro deste contexto, o status especial da propaganda relacionadas com processos eleitorais em outros países deveria ser enfatizado. Mesmo que simpatizar com um movimento oposicionista ou com um partido em geral não seja suficiente para violar o princípio da não-intervenção, campanhas com o potencial de minar o processo eleitoral constituem uma interferência ilegal nos assuntos internos de um Estado, mesmo que não incitem ações violentas.[30] Portanto, ataques cibernéticos que censuram e sabotam sites de meios de comunicação e de mídias sociais com propaganda pró Rússia antes e durante o referendum sobre a secessão da Crimeia e da Ucrânia no dia 16 de março de 2014[31] - desde que a responsabilidade dos russos pelos ataques fique comprovada – deve ser considerada ilegal.

Como já foi demonstrado, na prática muitas operações cibernéticas constituem interferências ilegais em temas nacionais de um país estrangeiro. No entanto, perturbações em pequena escala da infraestrutura cibernética, propaganda que não procure incitar mudanças violentas de regime e a mera intrusão de uma rede, espionagem ou manipulação de dados que não leve ao mau funcionamento ou à perda de infraestrutura não se configuram como violações da proibição, já que não têm natureza coercitiva ou não alcançam o patamar de grandeza que influências semelhantes precisam ter para potencialmente forçar um país a mudar sua política.

28 ver *Gill* (fn. 19), p. 234.

29 *De Brabandere* (fn. 27), p. 509.

30 Respect for the Principles of National Sovereignty and Non-Interference in Internal Affairs of a State in Their Electoral Processes, Resoluções da Assembleia Geral A/RES/44/147 (15 de dezembro 1989); A/RES/45/151 (18 Dezembro1990); A/RES/46/130 (17 December 1991); *Gill* (fn. 19), p. 223.

31 The Telegraph, Ukraine crisis proves cyber conflict is a reality of modern warfare (19 de abril 2014), disponível em: http://www.telegraph.co.uk/technology/internet-security/10770275/Ukraine-crisis-proves-cyber-conflict-is-a-reality-of-modern-warfare.html., última entrada: 10 de fevereiro 2015.

Significa isso, então, que essas atividades cibernéticas não são regulamentadas pela lei internacional de forma alguma? Se considerarmos a noção de igual soberania entre os Estados como o princípio subjacente à ordem legal internacional, esse resultado parece insatisfatório; particularmente quando se leva em conta o impacto adverso que a obtenção de dados sensíveis relacionados às capacidades militares ou econômicas de outro Estado pode ter na segurança nacional (em um sentido amplo) do primeiro.[32] O papel e a importância do princípio de soberania dos Estados nesse contexto vão ser discutidos no próximo parágrafo.

## RESPEITO À SOBERANIA DE UMA NAÇÃO ESTRANGEIRA

A soberania dos Estados é, por um lado, o princípio subjacente mais importante da lei internacional. Por outro lado, porém, é também o mais 'obscuro'. O conceito é frequentemente usado com propósitos argumentativos por autoridades governamentais e por tribunais sem que o escopo nem o conteúdo exato do princípio estejam definidos. Para que um ato internacional de responsabilidade de um Estado seja considerado arbitrário, uma obrigação, ou seja, uma regra específica da lei internacional, precisa ser desrespeitada.[33] Portanto, é necessário que se determinem as regras precisas que derivam do princípio de soberania da nação.

A soberania dos Estados sob a lei internacional geralmente é entendida como referência à dimensão territorial, ou seja, a integridade territorial de um país. Além da inviolabilidade das fronteiras nacionais, o Estado tem o direito exclusivo de prescrever e aplicar leis[34] e regulamentar a entrada e o trânsito por seu território. Poder-se-ia pressupor que a soberania não é interessante do ponto-de-vista cibernético, considerando-se que as redes e as atividades virtuais em geral não são interrompidas nas fronteiras territoriais. No entanto, o espaço cibernético não

32 Sobre a relevância da espionagem virtual para a segurança nacional, ver *Ziolkowski, Katharina*, Peacetime Cyber Espionage – New Tendencies in Public International Law, em: Ziolkowski, Katharina (ed.), Peacetime Regime For State Activities in Cyberspace (2013), p. 425-464, 447-450.

33 Art. 2 International Law Commission (ILC) Draft Articles on Responsibility of States for Internationally Wrongful Act, ILC Yearbook 2001, Vol. II, part 2 (doravante: ILC Articles on State Responsibility), p. 26-30; *Gill* (fn. 19), p. 226.

34 A Jurisdição de Estado não se restring ao seu território (solo, mar territorial e o espaço aéreo sobrejacente). Um Estado tem jurisdição sobre seus cidadãos no exterior, sobre aviões e navios registrados e sobre atividades extraterritoriais que ameaçam os interesses do governo central. A aplicação da lei se restringe ao território do país.

pode ser entendido como um domínio comum, livre de soberania.[35] Os Estados têm reafirmado a jurisdição sobre atividades cibernéticas trans-fronteiriças, como os casos em tribunais nacionais e internacionais têm demonstrado.[36] Além disso, os componentes físicos do ciberespaço, por exemplo os servidores, se estiverem localizados no território de um Estado, estão claramente sujeitos à jurisdição do Estado em questão.

Em relação às operações cibernéticas, pode-se dizer que violam a soberania de um Estado quando há um 'efeito físico perceptível'.[37] A lei internacional atual ainda não conseguiu esclarecer se esses efeitos precisam alcançar certo grau de severidade.[38] A necessidade de um certo patamar de gravidade parece algo razoável, considerando-se que a lei internacional não protege um Estado de qualquer impacto negativo que Estados estrangeiros possam ocasionar em seu território. Em um sistema legal de soberanias iguais, a soberania não pode ser absoluta.

Quanto à mera intrusão em uma rede, monitoramento de dados ou manipulação, argumenta-se que a interferência em uma infraestrutura virtual localizada em outro país pode ser equiparada ao exercício de jurisdição em um Estado estrangeiro, o que constituiria uma violação da soberania territorial.[39] Esta interpretação parece convincente na medida em que leva ao tratamento igualitário de dois casos que parecem comparáveis. Por que deveria fazer diferença se um Estado agente está no território de um país estrangeiro, conecta um pen drive e copia dados ou se ele obtém os mesmos dados por meio de *hacking* não autorizado de um computador em cima de uma mesa dentro do seu próprio país? 'O que há de tão especial no cibernético?' A atual lei internacional, porém, trata as duas situações acima de modo diferente. Em primeiro lugar, em função da interpretação (tradicional) do conceito de soberania quando se refere ao território físico de um país.[40] Em segundo lugar, devido ao fato de que espionagem, sem a presença física no território estrangeiro não está regulamentada pela lei internacional; não existe uma proibição geral, nem uma regra permissiva.[41] Alguns países, como os EUA, parecem ter uma visão ampla e consideram uma mera intrusão da suas redes

35 *Heintschel von Heinegg, Wolf,* Territorial Sovereignty and Neutrality in Cyber Space, 89 International Law Studies US Naval War College (2013), p. 123-156, 133.
36 Por exemplo: França LICRA v Yahoo (2000); ECJ, Google v Espanha (2014).
37 *Ziolkowski* (fn. 32), p. 485.
38 *Heintschel von Heinegg* (fn. 35), p. 129.
39 ibid. p. 128.
40 ver *Buchan* (fn. 6), p. 222-223.
41 *Ziolkowski,* (fn. 32), p. 445-446.

como uma violação da sua soberania.[42] Não existe, porém, nenhum acordo oficial dos Estados sobre este tópico.

Essas dúvidas deixam claro que os Estados, ao refinar e até mesmo reinterpretar o conceito de soberania, podem esclarecer como e até que ponto as operações cibernéticas estão regulamentadas pela lei internacional. O reverso da compreensão tradicional, estritamente territorial da soberania parece útil.[43] Curiosamente, a Alemanha se refere a 'soberania tecnológica' (sem nenhum esclarecimento adicional) na sua Estratégia de Segurança Cibernética.[44] De acordo com o Plano de Ação do Canadá para a Estratégia de Segurança Cibernética, 'resguardar de modo efetivo os sistemas [do governo] e os dados contidos neles, é […] um assunto de segurança nacional e soberania.'[45] Cabe aos Estados proporcionar padrões internacionais claros para as operações cibernéticas e suas implicações na soberania das nações.

## O REGIME DE TEMPOS DE GUERRA

■ Embora muitas operações cibernéticas que buscam exercer pressão política e disseminar propaganda sejam ilegais em tempos de paz, essas operações frequentemente estarão em conformidade com a lei internacional durante tempos de guerra. O fato não surpreende, se considerarmos os diferentes objetivos que o *ius ad bellum* e o *ius in bello* perseguem. O primeiro pretende possibilitar a coexistência pacífica dos Estados, enquanto o segundo se aplica quando os países estão em 'guerra' e usam força militar uns contra os outros. O *ius in bello* ou

42 The President of the United States of America, International Strategy for Cyberspace -Prosperity, Security, and Openness in a Networked World (Maio de 2011), p.12 ff, disponível em: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, 5.Fev. 2015; *Heintschel von Heinegg,* (fn. 35), p. 129; *Ziolkowski* (fn. 32), p. 459, fn. 193.

43 *Joyner, Christopher/Lotrionte, Catherine*, Information Warfare as International Coercion: Elements of a legal Framework, 12 European Journal of International Law (2001), p. 825-865, 843-845; see also *Buchan* (fn. 6), p. 222-223; stressing the potential need for reinterpretation of principles under international law with regard to cyber operations: *Heintschel von Heinegg* (fn. 35), p. 127.

44 German Ministry of Internal Affairs, Cyber-Sicherheitsstrategie für Deutschland (February 2011) p. 12, available at: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile, last vistited: 5 February 2015.

45 Canada's Action Plan on Cyber Security Strategy (2010-2015), p. 5, available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx, last vistited: 5 February 2015.

Lei Internacional de Conflito Armado (LOAC em inglês) não regulamenta se e quando a força pode ser usada, mas estipula como pode ser usada, tentando limitar as calamidades da guerra[46] enquanto permite o combate armado efetivo. Em relação às operações virtuais durante um conflito armado, a noção de 'ataque' no Artigo 49 do Primeiro Protocolo Adicional das Convenções de Genebra (API) é de particular importância: desencadeia a aplicação dos princípios centrais e regras da LOAC no que diz respeito à proteção de civis e de objetos civis. Além disso, em um conflito armado, os ataques cibernéticos podem ser usados para fins de distração, possibilitando ataques armados convencionais.

## ACIONANDO A PROTEÇÃO – DEFINIÇÃO DO ATAQUE

■ Um dos princípios cardinais da LOAC é o princípio da distinção, que obriga os Estados a distinguir entre objetivos civis e militares. Além disso, a LOAC estabelece regras específicas para proteger a população civil, como a proibição de atacar objetivos indispensáveis à sobrevivência da população civil.[47] Atos hostis durante um conflito armado estão sujeitos apenas a estas regras, se constituem um ataque segundo a definição que está no Artigo 49 API, por exemplo, um ato de violência, tanto de ofensiva quanto de defesa. Para determinar se as operações cibernéticas se qualificam como um ato de violência, as consequências pretendidas e as reais devem ser comparáveis às consequências de um ataque com meios de guerra convencionais.[48] Afinal de contas, as regras em questão pretendem proteger civis dos efeitos generalizados das hostilidades (tanto quanto o permitem as necessidades militares), então não pode fazer diferença se meios convencionais de guerra ou operações cibernéticas são usadas, se levam exatamente ao mesmo resultado.[49] Fica portanto aberto o debate sobre que efeitos um ato precisa ter para ser considerado um ataque. Claramente, (mais uma vez) operações cibernéticas que previsivelmente ou diretamente tenham como resultado morte ou lesão de pes-

46 Preâmbulo da Declaração de São Petersburgo (1868).

47 Art. 54 (2) API.

48 *Turns, David*, Cyber Warfare and the Concept of Attack under International Humanitarian Law, em: Saxon, Dan (ed.), International Humanitarian Law and the Changing Technology of War, 41 International Humanitarian Law Series (2013), p. 209-227, 225-226; *Schmitt, Michael*, Cyber Operations and the Jus In Bello, 41 Israel Yearbook on Human Rights (2011), p. 113-135, 118-120.

49 Uma justificativa convincente e detalhada desta abordagem e sua inerência em LOAC, *Schmitt,* ibid. p. 118-119.

soas ou em danos materiais[50] de objetivos constituem ataques segundo o Artigo 49 API.[51] A questão particularmente interessante aqui é o nível de imediatismo e objetividade que as consequências precisam ter para serem relevantes para a determinação da existência de um ataque. Sob a lei atual, os efeitos secundários, mesmo que sejam previsíveis até um certo ponto, e consequências de longo prazo, não são incluídos no teste. Por exemplo, as consequências de uma interrupção prolongada do fornecimento de eletricidade, como o impedimento de produção de comida e de armazenamento de comida, não são levados em conta, embora possam – em casos extremos -- acarretar risco de vida. Realmente, o objetivo da LOAC não é proteger a população civil de qualquer inconveniência durante conflitos armados.[52] No entanto, o autor não está convencido de que uma abordagem mais inclusiva (*de lege ferenda*), contradiga o objetivo principal e a praticabilidade da LOAC.[53] É inegável que atos que não têm potencial de risco de vida e não têm efeitos posteriores observáveis no mundo real, para além de espalhar o medo e o horror, como a mera desconfiguração de websites ou manipulação de dados ou comunicações, deveriam ser excluídos. No entanto, a privação de eletricidade ou água por um período mais prolongado, tem previsivelmente consequências humanitárias calamitosas.[54] Outrossim, como o conceito de ataque precisa ser entendido dentro do contexto do objetivo das regras às quais se aplica – a proteção da população civil dos efeitos das hostilidades – os Estados deveriam adotar uma abordagem mais inclusiva.

Além disso, uma interpretação ampla de 'ataque' parece oportuna quando consideramos a importância de operações baseadas em efeito para a Lei (moderna) de seleção[55]. Ao contrário dos meios de guerra tradicionais, que se concentravam em enfraquecer progressivamente as forças militares dos oponentes, as operações baseadas em efeito são lançadas contra alvos em função dos efeitos

50 A interpretação de 'dano' é suscetível a controvérsia, para uma interpretação extensa: *Dörmann, Knut*, The Applicability of the Additional protocols to Computer Network Attacks: ICRC Viewpoint, em: Byström, Karin, 2004 International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law (2005), p. 139-153, 142-143; para uma interpretação estrita *Schmitt*, (fn. 48), p. 121.

51 *Schmitt*, ibid. p. 120.

52 ibid. p. 121.

53 Arguing a devaluation of the law and its objectives, *Turns*, (fn. 48), p. 227.

54 *Geiß, Robin*, War and Law in Cyberspace, American Society for International Law Proceedings 2010, p. 371-374, 373.

55 Em geral *Henderson, Ian*, The Contemporary Law of Targeting (2009), p.125-146; *Schmitt, Michael,* Targeting and Humanitarian Law: Current Issues, 80 International Law Studies, p. 151-194.

sistemáticos que a destruição ou interrupção desses alvos têm no comportamento do oponente. Isso 'pode levar à tentação de atacar alvos que não sejam de natureza militar'.[56] Além disso, na moderna arte de guerra objetivos de uso dual ou até mesmo objetivos civis são mais prováveis de serem atacados. Um entendimento amplo do conceito de ataque, desencadeando a aplicação das regras de proteção mencionadas acima, garantem uma proteção efetiva da população civil durante um conflito armado.

Além disso, um desvio para uma abordagem mais humanitária da definição de ataque não necessariamente diminuiria a efetividade ou praticabilidade da LOAC, porque a qualificação de um ato como um ataque não leva automaticamente à proibição. Se for dirigido contra um objeto militar, ou se os padrões de proporcionalidade forem seguidos, esses ataques são considerados legítimos.[57] Consequentemente, uma definição abrangente pode atender às realidades da guerra e permitir uma guerra efetiva.

## OPERAÇÕES CIBERNÉTICAS QUE PERMITEM ATAQUES ARMADOS (ENGANO)

■ Operações cibernéticas militares frequentemente são usadas como uma preparação para medidas de apoio que possibilitam ataques armados (convencionais). Por exemplo, o bombardeio de uma central nuclear elétrica por Israel em 2007 teve o auxílio da perturbação do sistema de defesa aéreo sírio através de meios virtuais para possibilitar a entrada não detectada de aeronaves de combate em espaço aéreo sírio. Hoje, as regras quanto à trapaça na guerra, que valem independentemente da existência de um ataque,[58] são particularmente relevantes. A operação israelense citada acima precisa ser qualificada como uma estratagema de guerra permitida, que devem distinguir-se de atos de perfídia, proibidos. Atos pérfidos são caracterizados como atos que buscam despertar a confiança do oponente, para levá-lo a acreditar que existe uma situação em que estão sendo aplicadas as regras de proteção da LOAC, com a intenção de trair a confiança conquistada.

O espaço cibernético permite uma extensa gama de usos das operações enganosas. A origem da atividade cibernética pode ser facilmente dissimulada

56 *Dinniss* (fn. 12), p. 25.
57 ver *Geiß*, (fn. 54), p. 373.
58 Art. 37 API; *Roscini* (fn. 15), p. 217.

usando táticas como os *botnets*[59], por exemplo.[60] No contexto militar, a manipulação das comunicações das forças inimigas é altamente relevante. Pouco antes da invasão em 2003, os EUA *hackearam* o sistema de e-mails do Ministério de Defesa iraquiano 2003 e enviaram mensagens encorajando os funcionários iraquianos a largar as armas e reforçando a ideia de que os EUA pretendiam apenas tirar Saddam no poder e não tinha intenção de prejudicar as forças armadas locais.[61] Aqui, o conteúdo da mensagem é o critério crucial para delimitar a fronteira entre perfídia e estratagemas de guerra. As mensagens para os funcionários iraquianos são estratagemas legítimos, já que não implicavam em estar em conformidade com as regras protetoras sob a LOAC. Em comparação, operações cibernéticas que, por exemplo, fingem ter status civil ou fingem a rendição do inimigo, seriam ilegais, desde que incluam outros requisitos da proibição ou perfídia. Não apenas é necessário demonstrar a busca de confiança, mas também a intenção de traí-la. Além disso, o ato pérfido precisa ter como consequência a captura, a morte ou a lesão de uma pessoa. Dado o estreito escopo de interpretação da aplicação da proibição ou da perfídia, as regras que definem o uso impróprio dos emblemas reconhecidos no Artigo 38 API parecem ter maior relevância prática.

O último proíbe o uso inadequado dos sinais de proteção e afirma que endereços de domínio como 'icrc.org', desde que essa ideia seja aprovada pela prática futura do Estado, estão englobados na proibição.[62] Realmente, endereços de domínio em determinados níveis 'mais baixos' são ativos que podem ser obtidos no mercado livre e portanto mudam seus usuários com frequência. No entanto, em função da governança do ICANN – Corporação da Internet para Atribuição de Nomes e Números, especialmente os domínios de segundo nível sob os domínios genéricos do 1º nível, como por exemplo 'icrc.org', são atribuídos exclusivamente à instituição em questão e, portanto, funcionam como uma função de identificação comparável a emblemas.

---

59 Uma botnet é uma rede de computadores comprometidos, 'the bots', controlados remotamente por um intruso, o 'botherder', usado para conduzir operações ou crimes cibernéticos. Não há limite prático para o número de bots que pode ser 'recrutado'para entrar em uma botnet. *Schmitt* (fn. 10), Glossário, p. 257.

60 *Pool, Phillip*, 47 International Lawyer (2013), p. 299-323, 309; *Roscini* (fn. 15), p. 215;

61 *Gervais, Michael*, Cyber Attacks and the Laws of War, 30 Berkeley Journal of International Law (2012), p. 525-579, 547.

62 *Boothby, Bill*, Cyber Deception and Autonomous Attack – Is There a Legal Problem?, Podins, Karlis /Stinissen, Jan/Maybaum, Markus (eds.), 5th International Conference on Cyber Conflict (2013), p. 245-261, 256; *Dinniss* (fn. 12), p. 265.

E por último, assim como em tempos de paz, a compilação de informações por meios cibernéticos – espionagem cibernética – como preparação para atos hostis durante conflito armado também carece de um arcabouço regulatório. Não existe nenhuma proibição de espionagem e a LOAC aborda a espionagem exclusivamente em relação à presença física do espião em território controlado pelo oponente.[63]

## CONCLUSÃO

### Obrigações dos Estados quanto à Segurança Cibernética

■ Como foi definida anteriormente aqui, a soberania igualitária é o princípio subjacente da lei internacional. Assim, a soberania de uma nação só pode chegar até onde a soberania de outro país não seja infringida. E, principalmente, a lei internacional também fornece obrigações positivas dos Estados para protegerem mutuamente as respectivas soberanias. O princípio da prevenção é particularmente interessante no âmbito do espaço cibernético.

De acordo com o princípio da prevenção, 'cada Estado tem a obrigação de não deixar, intencionalmente, que seu território seja usado para atos contrários aos direitos de outros Estados'[64]. Além disso, um Estado precisa tomar todas as medidas necessárias disponíveis para interromper operações virtuais em curso contra uma nação estrangeira originadas em seu território, a partir do momento em que o país fique ciente dessas operações adversas ou onde uma situação impõe esse conhecimento. No entanto, essa obrigação se aplica apenas às operações virtuais que causem prejuízos significativos em outro Estado.[65] Aqui, mais uma vez não fica claro se o prejuízo não perceptível no mundo real, como o monitoramento ou manipulação de dados, está incluído ou não.

Mas os países também são obrigados a adotar medidas para impedir que uma infraestrutura cibernética em seus territórios sejam usadas para ataques cibernéticos que causem prejuízos significativos a outro país. Essas medidas podem ser de

63 Art. 46 API , sobre o status de prisioneiro de guerra para espiões.

64 ICJ, The Corfu Channel Case, (United Kingdom v Albania), Merits, Judgement of 9 April 1949, ICJ Reports 1949, p. 4, 22.

65 Ver Trail Smelter Arbitration (United States v Canada) (1938/1941), Reports of International Arbitral Awards, Vol. III p. 1905-1982, p.1965; ICJ, Case concerning Pulp Mills on the River Uruguay (Argentina v Uruguay), Judgement of 10 April 2010, ICJ Report 2010, p. 14, para. 101; ILC Draft Articles on Prevention of Transboundary Harm from Hazardous Activities (2001), ILC Yearbook 2001, Vol. 2, Part 2, p. 148-170, Art 1.

natureza regulatória, legal, administrativa, política ou técnica.[66] Por exemplo, a adoção de leis criminais e o estabelecimento de mecanismos de monitoramento são algumas possibilidades. É importante o fato de que as nações precisam se certificar de que essas medidas estejam em concordância com as obrigações de direitos humanos sob a lei internacional ou nacional, como o direito à privacidade, liberdade de expressão e de informação. E a extensão até onde um Estado é obrigado a adotar medidas preventivas permanece em aberto. Como a obrigação está restrita às medidas disponíveis para o país em questão e as capacidades tecnológicas dos países diferem, o padrão vai variar de acordo com isso. Com frequência debate-se se há uma obrigação de maior alcance da *'due diligence'* dos Estados para preservarem a segurança cibernética.[67] Podem ser estabelecidos paralelos para o princípio da precaução, desenvolvido na área da lei internacional ambiental. De acordo com este princípio, os Estados ainda precisam adotar medidas preventivas, mesmo que não exista ainda uma certeza científica em relação aos potenciais efeitos adversos de uma determinada atividade para o meio ambiente.[68] 'Se traduzirmos' o conceito para a esfera virtual, os Estados não apenas seriam obrigados a impedir prejuízos significativos, mas também seriam, de modo geral, solicitados a identificar potenciais ameaças à segurança cibernética e adotar medidas de prevenção.[69] O enfoque preventivo, no entanto, está sujeito a controvérsias quanto à sua natureza, sua base normativa e seu conteúdo exato.[70] Portanto, ser parte do direito consuetudinário é questionável. Mesmo enfatizando o alto potencial que esse enfoque preventivo possa ter para a regulamentação das atividades cibernéticas no futuro,[71] não há

66 Para exemplos dessas medidas, ver *Ziolkowski* (fn. 15), p. 169.

67 *Heintschel von Heinegg*, *Wolf,* Legal Implications of Territorial Sovereignty in Cyberspace, in: Czosseck, Christian/ Ottis, Rain/Ziolkowski, Katharina (eds.), 4th International Conference on Cyber Conflict (2012), p. 7-19, 17-18.

68 Por exemplo

: Principle 15 Rio Declaration (1992), Art. 3.3 UN Framework Convention on Climate Change (1992), Preamble of the Convention on Bio Diversity (1992), Art 1 Stockholm Convention of Persistent Organic Polluters (2001).

69 *Marauhn*, *Thilo,* Customary Rules of International Environmental Law - Can They Provide Guidance for Developing a Peacetime Regime for Cyberspace?, em: Ziolkowski, Katharina (ed.), Peacetime Regime for State Activities in Cyberspace (2013), p. 465-484, 475-476

70 Com relação à natureza, não está claro ainda se a precaução é um princípio ou apenas um enfoque. Além disso, ainda está em aberto a questão sobre se é um princípio de direito consuetudinário ou um princípio geral dentro do significado do Artigo 38 (1)(c) do Estatuto. Em relação ao conteúdo, se debate se leva a uma mudança do ônus da obra ou se é uma obrigação stricto sensu, *Dupuy, Pierre-Marie/ Viñuales, Jorge E.*, International Environmental Law: A Modern Introduction (publicado em Abril 2015), capítulo 3.

71 *Marauhn,* (fn. 69), p. 475.

evidências suficientes de que a segurança virtual internacional seja (já) considerada um interesse jurídico da comunidade internacional como tal, como acontece com a preservação do meio ambiente. As diferentes iniciativas (políticas), como as resoluções da Assembleia Geral da ONU,[72] em relação à segurança cibernética demonstram que essa visão está evoluindo. Porém, pressupor que há um princípio operando normativamente que obrigará os Estados a proteger a segurança cibernética internacional como tal, parece algo prematuro.

No entanto, o princípio da prevenção obriga os países a adotarem medidas disponíveis para impedir prejuízos significativos no território de outro Estado causados por operações cibernéticas geradas a partir de infraestrutura dentro do seu território. Outrossim, os Estados têm deveres processuais, por exemplo, informar outro país quando tiver conhecimento de atividades cibernéticas sendo iniciadas em seu território, realizar avaliações de impacto e cooperar com o país em questão.

## Contramedidas eficazes contra Operações Cibernéticas

■ Se as violações da lei internacional forem cometidas, um conjunto de regras internacionais secundárias, – a lei de responsabilidade de Estado – fornece contramedidas ao país ofendido, que deverão induzir o 'Estado-perpetrador' a retornar ao comportamento legalizado. Como já se mencionou aqui, o chamado ato iníquo deve ser uma violação de uma regra específica da lei internacional. Além disso, os organismos de um Estado precisam ter cometido o ato ou ele precisa ser atribuído a um Estado.[73] A lei de responsabilidade de Estado determina os critérios para uma atribuição semelhante e fornece os requisitos e limites das medidas defensivas.

No ambiente acadêmico, já foi enfatizado que os critérios de atribuição, sob a lei internacional atual, foram elaborados de modo muito estreito e portanto não estão adequados à esfera virtual.[74] Realmente, a maior parte dos incidentes

72 Por exemplo: Creation of a global culture of cybersecurity, UN General Assembly resolution 57/239 (20 Dec 2002); Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, UN General Assembly resolution 64/211 (21 Dezembro de2009).

73 Para os critérios de atribuições de atos (de atores não-Estado) para um Estado, ver Art. 4-11 ILC Articles on State Responsibility (fn. 33).

74 *Heintschel von Heinegg, Wolf,* Cyberspace- Ein völkerrechtliches Niemandsland, em: Schmidt-Radefeldt, Roman/Meissler, Christine (eds.), Automatisierung und Digitalisierung des Krieges, p. 159-174, 172.

cibernéticos na prática não podem ser atribuídos a um Estado sem que haja sombra de dúvida. O ciberespaço proporciona uma extensa gama de possibilidades para tornar anônima ou ocultar a autêntica fonte das atividades cibernéticas. No entanto, até agora, os Estados não concordaram em um padrão diferente, especial de atribuição para atividades cibernéticas maliciosas. De modo geral, o problema de atribuição parece ter uma natureza mais técnica do que legal.

Mesmo que seja possível identificar o Estado responsável, medidas defensivas sob a lei de responsabilidade de Estado não necessariamente constituem ferramentas efetivas para repelir operações cibernéticas porque é preciso também cumprir com os requisitos de necessidade e proporcionalidade.[75] As investigações de incidentes cibernéticos frequentemente continuam por longo tempo após a cessação da atividade cibernética ilegal. No entanto, depois que o estado de legalidade é restaurado, as contramedidas, que perseguem o único objetivo de induzir o comportamento legal, e não contemplam punição, talvez não cumpram com o padrão exigido de necessidade sob a lei internacional.[76] Dado esse escopo restrito da aplicação (temporária) das contramedidas e os problemas relacionados com a atribuição de atividades cibernéticas a um país, uma abordagem mais preventiva da segurança cibernética parece oportuna. Os Estados precisam especificar suas obrigações sob o princípio da prevenção e desenvolver fóruns e procedimentos para possibilidade a cooperação.

## Necessidade de Cooperação no desenvolvimento de padrões aceitos para a Segurança Cibernética

■ A análise das implicações das operações cibernéticas sob a lei internacional (feita acima) deixa claro que existe a necessidade de esclarecimentos adicionais ou até mesmo da reinterpretação dos princípios e regras legais. Os princípios subjacentes da ordem legal internacional, como o princípio da não-intervenção, o conceito de soberania de Estado e o princípio da prevenção geralmente são aplicados às operações virtuais, mas muitas incertezas ainda permanecem. Para fechar essas "brechas" as nações precisam se reunir e chegar a um acordo sobre os entendimentos comuns dos princípios fundamentais da lei internacional, que a longo prazo poderia possibilitar a formulação de obrigações específicas dos Estados no tópico segurança cibernética.

75 Art. 51-52 ILC Articles on State Responsibility (fn. 33).
76 Art. 49 (1) and Art. 52 (3) ILC Articles on State Responsibility (fn. 33).

A ênfase deveria estar em determinar as medidas que um Estado deve ser solicitado a adotar para impedir atividades cibernéticas adversas originadas de infraestrutura virtual sobre o seu controle. Afinal, o escopo e a extensão das obrigações sobre o princípio da prevenção não podem variar segundo o critério individual de cada Estado. Os países precisam chegar a um acordo não apenas sobre um padrão mínimo, mas sim preparar um catálogo de medidas preventivas. Uma revisão periódica desse catálogo pelos Estados permitiria que se incluíssem respostas a novos desenvolvimentos tecnológicos. Adicionalmente, as diferentes capacidades tecnológicas dos Estados deverão ser levadas em consideração. Seguindo os exemplos de tratados de leis meio-ambientais, nos quais os países em desenvolvimento são submetidos a obrigações menos estritas,[77] os Estados poderiam ser submetidos a diferentes padrões de acordo com seu *know-how* tecnológico. Em linhas gerais, se deve oferecer suporte aos países com menos capacidade tecnológica.

No entanto, uma regulamentação assim tão detalhada, em forma de um tratado de segurança cibernética, parece muito distante da realidade. Os Estados relutam em compartilhar suas conquistas tecnológicas relacionadas com a esfera virtual, em função dos potenciais benefícios de ataques cibernéticos durante conflitos armados e em ações de política de dissuasão.

Além disso, os países não compartilham um entendimento comum dos temas mais básicos e dos conceitos legais. Será que a segurança cibernética é um interesse legal em comum dos Estados ou apenas um objetivo político? Como a segurança virtual se relaciona com a soberania? A soberania deveria ser entendida para além da questão meramente territorial? Esclarecimentos adicionais também são necessários no que diz respeito à relação entre direitos humanos e segurança cibernética, como a liberdade de informação e de expressão e o direito à privacidade. A Rússia, por exemplo, tem uma interpretação peculiar de 'segurança de informação', que inclui o direito de um Estado à censura, o que aparentemente contradiz os padrões de direitos humanos nas democracias ocidentais.[78] Considerando as extensa competências da ASN no quesito monitoramento de dados, os EUA parecem ser da opinião de que as preocupações com a segurança (virtual) justificariam amplas restrições do direito à privacidade, o que não se encaixa nos padrões de proteção garantidos em outros países.

77 Por exemplo: o Protocolo de Kioto para a Convenção do Marco das Nações Unidas para Mudanças Climáticas (1998) ou o Protocolo Montreal para Substâncias que afetam a Camada de Ozônio (1987).

78 *Schaller, Christian*, Internationale Sicherheit und Völkerrecht im Cyberspace, 18. Studie der Stiftung Wissenschaft und Politik (2014), p. 28.

Todas as inconclusões em relação à aplicação das normas internacionais e as diferentes interpretações dos conceitos legais mais amplos expõem a necessidade urgente de que se intensifiquem as consultas e a cooperação entre os Estados no tema de segurança cibernética. O trabalho da Assembleia Geral da ONU em relação ao assunto é um ponto de partida proveitoso, como bem ilustra a adoção de uma resolução 'O direito à privacidade na era digital[79] em 18 de dezembro de 2014, introduzida pelo Brasil e pela Alemanha.

Julia Dornsbusch é Pesquisadora Assistente do Institute for International Peace and Security Law, da Universidade de Colônia.

79 Resolução da Assembleia Geral das Nações Unidas A/RES/69/166 (18 de Dezembro 2014).

# Publicações anteriores dos *Cadernos Adenauer*

Eficiência energética (n. 3, 2014)

Governança e sustentabilidade nas cidades (n. 2, 2014)

Justiça Eleitoral (n. 1, 2014)

Relações Brasil-Alemanha / Deutsch-Brasilianische Beziehungen (caderno especial, 2013)

Novas perspectivas de gênero no século xxi (n. 3, 2013)

Candidatos, Partidos e Coligações nas Eleições Municipais de 2012 (n. 2, 2013)

Perspectivas para o futuro da União Europeia (n. 1, 2013)

Democracia Virtual (n. 3, 2012)

Potências emergentes e desafios globais (n. 2, 2012)

Economia verde (n. 1, 2012)

Caminhos para a sustentabilidade (edição especial, 2012)

Municípios e Estados: experiências com arranjos cooperativos (n. 4, 2011)

Ética pública e controle da corrupção (n. 3, 2011)

O Congresso e o presidencialismo de coalizão (n. 2, 2011)

Infraestrutura e desenvolvimento (n. 1, 2011)

O Brasil no contexto político regional (n. 4, 2010)

Educação política: reflexões e práticas democráticas (n. 3, 2010)

Informalidade laboral na América Latina (n. 2, 2010)

Reforma do Estado brasileiro: perspectivas e desafios (n. 1, 2010)

Amazônia e desenvolvimento sustentável (n. 4, 2009)

Sair da crise: Economia Social de Mercado e justiça social (n. 3, 2009)

O mundo 20 anos após a queda do Muro (n. 2, 2009)

Migração e políticas sociais (n.1, 2009)

Segurança pública (n. 4, 2008)

Governança global (n. 3, 2008)

Política local e as eleições de 2008 (n. 2, 2008)

20 anos da Constituição Cidadã (n. 1, 2008)

A mídia entre regulamentação e concentração (n. 4, 2007)

Partidos políticos: quatro continentes (n. 3, 2007)

Geração futuro (n. 2, 2007)

União Europeia e Mercosul: dois momentos especiais da integração regional (n. 1, 2007)

Promessas e esperanças: Eleições na América Latina 2006 (n. 4, 2006)

Brasil: o que resta fazer? (n. 3, 2006)

Educação e pobreza na América Latina (n. 2, 2006)

China por toda parte (n. 1, 2006)

Energia: da crise aos conflitos? (n. 4, 2005)

Desarmamento, segurança pública e cultura da paz (n. 3, 2005)

Reforma política: agora vai? (n. 2, 2005)

Reformas na Onu (n. 1, 2005)

Liberdade Religiosa em questão (n. 4, 2004)

Revolução no Campo (n. 3, 2004)

Neopopulismo na América Latina (n. 2, 2004)

Avanços nas Prefeituras: novos caminhos da democracia (n. 1, 2004)

Mundo virtual (n. 6, 2003)

Os intelectuais e a política na América Latina (n. 5, 2003)

Experiências asiáticas: modelo para o Brasil? (n. 4, 2003)

Segurança cidadã e polícia na democracia (n. 3, 2003)

Reformas das políticas econômicas: experiências e alternativas (n. 2, 2003)

Eleições e partidos (n. 1, 2003)

O Terceiro Poder em crise: impasses e saídas (n. 6, 2002)

O Nordeste à procura da sustentabilidade (n. 5, 2002)

Dilemas da Dívida (n. 4, 2002)

Ano eleitoral: tempo para balanço (n. 3, 2002)

Sindicalismo e relações trabalhistas (n. 2, 2002)

Bioética (n. 1, 2002)

As caras da juventude (n. 6, 2001)

Segurança e soberania (n. 5, 2001)

Amazônia: avança o Brasil? (n. 4, 2001)

Burocracia e Reforma do Estado (n. 3, 2001)

União Europeia: transtornos e alcance da integração regional (n. 2, 2001)

A violência do cotidiano (n. 1, 2001)

Os custos da corrupção (n. 10, 2000)

Fé, vida e participação (n. 9, 2000)

Biotecnologia em discussão (n. 8, 2000)

Política externa na América do Sul (n. 7, 2000)

Universidade: panorama e perspectivas (n. 6, 2000)

A Rússia no início da era Putin (n. 5, 2000)

Os municípios e as eleições de 2000 (n. 4, 2000)

Acesso à justica e cidadania (n. 3, 2000)

O Brasil no cenário internacional (n. 2, 2000)

Pobreza e política social (n. 1, 2000)

Para assinar ou adquirir os Cadernos Adenauer, acesse: www.kas.de/brasil

Este livro foi composto por
Cacau Mendes em Adobe Garamond c.11/14 e
impresso pela Stamppa em papel offset LD 75g/m²
para a Fundação Konrad Adenauer
em julho de 2015.