**UniCEUB – Centro Universitário de Brasília**
**Instituto CEUB de Pesquisa e Desenvolvimento - ICPD**
**Programa de Mestrado em Direito e Políticas Públicas**

**Ronaldo Bach da Graça**

# POLÍTICAS PÚBLICAS DE DEFESA CIBERNÉTICA:
OS LIMITES ENTRE O DIREITO À PRIVACIDADE
E O PUGILATO CIBERNÉTICO

**Brasília**
**2016**

**Ronaldo Bach da Graça**

# POLÍTICAS PÚBLICAS DE DEFESA CIBERNÉTICA
OS LIMITES ENTRE O DIREITO À PRIVACIDADE E O PUGILATO CIBERNÉTICO

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Direito e Políticas Públicas pelo Programa de Pós-Graduação em Direito do Centro Universitário de Brasília – UniCEUB.
Orientador: Prof. Dr. Carlos Augusto Ayres de Freitas Britto.

**Brasília**
**2016**

GRAÇA, Ronaldo Bach da.
POLÍTICAS PÚBLICAS DE DEFESA CIBERNÉTICA: os limites entre o direito à privacidade e a defesa cibernética. Ronaldo Bach da Graça, 2016. 182 f.

Orientador: Prof. Dr. Carlos Augusto Ayres de Freitas Britto.
Dissertação (Mestrado) – Centro Universitário de Brasília. Programa de Mestrado em Direito e Políticas Públicas, Brasília, 2016.

**Ronaldo Bach da Graça**

# POLÍTICAS PÚBLICAS DE DEFESA CIBERNÉTICA
OS LIMITES ENTRE O DIREITO À PRIVACIDADE
E O PUGILATO CIBERNÉTICO

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Direito e Políticas Públicas pelo Programa de Pós-Graduação em Direito do Centro Universitário de Brasília – UniCEUB.
Orientador: Prof. Dr. Carlos Augusto Ayres de Freitas Britto.

Brasília, 30 de junho de 2016.

Banca examinadora:

_____
Prof. Dr. Carlos Augusto Ayres de Freitas Britto
Orientador

_____
Prof.ª Dr.ª Maria Edelvacy Pinto Marinho
Examinadora

_____
Prof. Dr. Márcio Nunes Iorio Aranha Oliveira
Examinador

_____
Prof. Dr. Jefferson Carús Guedes
Suplente

## AGRADECIMENTOS

Agradeço a Deus, a minha família (em especial a meus pais), aos amigos, aos professores Carlos Augusto Ayres de Freitas Britto, Maria Edelvacy Pinto Marinho, Jefferson Carús Guedes, Márcio Nunes Iório Aranha Oliveira, Antonino dos Santos Guerra Neto. Aos amigos da Assessoria para Contratos de Defesa (ACODE) e a todos os demais que contribuíram de alguma forma com o presente trabalho – são muitos. Muito obrigado!

Agradeço ainda a todos que investiram e investem seu tempo lendo o presente estudo. É meu desejo que ele contribua para um mundo melhor.

A todos, paz e bem!

“Não perca mais tempo com o que não faz a vida valer a pena”.

Eugênio Jorge

## RESUMO

O presente trabalho tem por objetivo analisar o pugilato cibernético custeado pelo Estado e sua contribuição para a preservação do Estado democrático de direito ordeiro e progressista. Dentre os riscos inerentes à sociedade em rede decorrentes do uso do ciberespaço, destaca-se a ameaça ao direito à privacidade. Propõe-se que o desafio de lidar com o pugilato cibernético tenha como uma de suas finalidades a mitigação de riscos por meio de políticas públicas. São estudados aspectos ligados a inteligência de Estado, como os denunciados por Edward Snowden e pelo sítio Wikileaks, relacionando-os com o pugilato cibernético financiado pela sociedade. O trabalho aborda aspectos do direito à privacidade relacionados com o pugilato cibernético, contribuindo para a busca do equilíbrio entre as garantias constitucionais, da segurança jurídica e do bem-estar comum. Realizou-se pesquisa bibliográfica e documental, incluindo-se nas fontes de pesquisa decisões judiciais de cortes brasileiras que enfrentaram o tema. Apresenta-se a possibilidade de mitigação dos riscos no espaço cibernético a partir de políticas públicas que fomentem a inovação na segurança de redes por meio de investimentos visando ao incremento das tecnologias estratégicas para o êxito no pugilato cibernético. Observou-se que a defesa cibernética deve ter caráter preventivo, a fim de garantir segurança aos cidadãos na busca do bem-estar comum. Concluiu-se que a defesa cibernética é instrumento significativo de preservação do Direito em um Estado democrático que visa ao bem-estar da população.



**Palavras-chave:** Pugilato cibernético. Defesa cibernética. Direito à privacidade. Direito nas redes de computadores. Riscos na sociedade em rede.

**ABSTRACT**

This work aims to analyze the cyber boxing supported by the State and its participation to the conservation of a lawful and progressive democratic State of rights. Among the risks in the network society caused throw the cyberspace, the threat to the right of privacy stands out. It is proposed that the challenge of dealing with the cyber boxing has as one of its purposes to mitigate the risks through public policies. They are studied the aspects related to the intelligence of State, as reported by Eduard Snowden and the website Wikileaks, linking them to the cyber boxing funded by the by the society. The study addresses aspects of the right to privacy related to the cyber boxing, contributing to the search for balance of the constitutional guarantees, legal security and common welfare. It was done bibliographic and documental research, including in the search sources the court decisions of Brazilian courts which handled the matter. It is presented the possibility of mitigation of risks in cyberspace by public policy that promote the innovation in networks from investments aiming to increase the strategic technologies to the success in the cyber boxing. It is observed that cyber defense should be preventive, to ensure security for citizens in the pursuit of common welfare. It was concluded that cyber boxing is significant tool for the preservation of law in a democratic state that aims to population welfare.

**Key words:** Cyber boxing. Cyber defence. Right to privacy. Rights in networks. Rights in the network society.

## LISTA DE ABREVIATURAS

ADI – Ação Direta de Inconstitucionalidade

Art. – artigo

BNDES – Banco Nacional do Desenvolvimento

CADE – Conselho Administrativo de Defesa Econômica

CCOMGEX – Centro de Comunicações e Guerra Eletrônica do Exército

CDCiber – Centro de Defesa Cibernética

CDMA – *code division multiple access* (acesso múltiplo por divisão de código)

CEO - sigla inglesa de *Chief Executive Officer*, Diretor Executivo em Português.

CR – Constituição da República Federativa do Brasil

CGI – Comitê Gestor da Internet

CIGE – Centro de Instrução de Guerra Eletrônica

CNN – *Cable News Network* (canal de notícias norte americano)

CTI – Centro de Tecnologia da Informação

DARPA – Defense Advanced Research Projects Agency of the U.S.

DCT – Departamento de Ciência e Tecnologia

EB – Exército Brasileiro

END – Estratégia Nacional de Defesa

ENGESA - Engenheiros Especializados S/A (extinta)

FBI - *Federal Bureau of Investigation* ou Agência Federal de Investigação em português

GCHQ – *Government Communications Headquarters* (Quartel general de comunicações do governo inglês)

GCiber –guerra cibernética

GE –guerra eletrônica

GLO – Garantia da Lei e da Ordem

GPS – *global position system* (sistema de posicionamento global)

HC – *habeas corpus*

ICANN – *Internet Corporation for Assigned Names and Numbers* (Corporação da Internet para Designação de Nomes e Números)

ICT – Instituição Científica e Tecnológica

IFSC – Instituto Federal de Santa Catarina

IOS – *iPhone operating system* (sistema operacional do iPhone)

MC – medida cautelar

MCTI – Ministério da Ciência, Tecnologia e Inovação

MD – Ministério da Defesa

MDIC – Ministério do Desenvolvimento, Indústria e Comércio Exterior

MS – mandado de segurança

NSA – *National Security Agency* (Agência de Inteligência Americana)

OCDE – Organização para a Cooperação e Desenvolvimento Econômicos

P&D – pesquisa e desenvolvimento

RE – recurso extraordinário

REsp – recurso especial

S. A. – Sociedade anônima

SIGINT – *signal intelligence* (inteligência de sinais)

SIMOC – Simulador de Operações Cibernéticas

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

STM – Superior Tribunal Militar

TIC – tecnologia da informação e comunicação

TRF – Tribunal Regional Federal

*v. g. – verbi gratia*

SUMÁRIO

# INTRODUÇÃO

Atualmente, a segurança das pessoas ou mesmo do Estado pode ser ameaçada por meio de um campo de batalha que não existia há algumas décadas: dentro de redes de computadores, que hoje controlam inclusive sistemas estratégicos na sociedade. Trata-se de um novo teatro de operações de guerra, no qual essa forma contemporânea de combate pode ocorrer a qualquer momento, mesmo em contextos aparentemente pacíficos.

Com uma guerra declarada, fica evidente a possibilidade do uso da estrutura da guerra cibernética, no entanto para que as ameaças cibernéticas se mostrem presentes, não é usual uma declaração formal de guerra. Outra característica deste espectro de combate relativamente recente é o fato de que a guerra não acontece necessariamente contra um outro Estado: a guerra pode se dar, por exemplo, contra um grupo organizado como um grupo de terroristas, e supostamente em tempo de paz, ou ao menos guerra não declarada. Em tempos de crise, grupos antagônicos também podem se utilizar das redes cibernéticas para auferir alguma vantagem na relação beligerante. Como as batalhas podem ocorrer independentemente da situação declarada – paz, crise ou guerra –, utilizar-se-á neste trabalho o termo pugilato cibernético.

Percebe-se que, quanto mais avançada tecnologicamente são os meios disponíveis de uma sociedade, maior sua vulnerabilidade cibernética; visto que as sociedades mais adiantadas costumam depender de forma mais intensa de dados processados por meios informáticos. A principal forma de defesa que a sociedade constituída possui contra ataques cibernéticos oponentes, além do preparo técnico de seus sentinelas, é a monitoração do que acontece na rede, o que necessariamente suscita mitigação da privacidade de quem a utiliza[1].

As redes de computadores são hoje uma realidade da vida. O *Livro Verde: segurança cibernética no Brasil*, declara que a segurança cibernética hoje se impõe como função estratégica de Estado, sendo essencial para a manutenção de infraestruturas fundamentais de um país, tais como o funcionamento das redes elétricas, estrutura de defesa, modal de transportes, telecomunicações, sistema bancário, sistemas

[1] CLARKE, Richard A. *Cyberwar*: The Next Threat to National Security and What to do About It. New York: Ed. Ecco, 2012. p. 179-218.

de informações[2]. Quase tudo pode estar conectado à internet ou outro tipo de rede de computadores ou afins: carros, geladeiras, *smartphones, tablets*, televisões, rádios, fogões, telefones, equipamentos médicos etc. Por meio de um computador ligado à internet, pode-se muito mais do que acessar uma câmera do outro lado do mundo, sendo possível ligar ou desligar importantes sistemas de um Estado.

Com a importância que ganham as redes de computadores, a sua manutenção desempenha papel estratégico na segurança pública e na segurança de um Estado (segurança nacional). Pode-se dizer que os meios informáticos podem ajudar a sociedade a implementar e gerir os projetos por ela escolhidos e materializados por políticas públicas, ou, por outro lado, ameaçar a cada um deles.

Em razão da mudança ocorrida nas estruturas sociais face à difusão do uso das redes informáticas, o Estado deve assegurar que tais redes sejam utilizadas sempre em benefício da comunidade, considerando os valores e direitos conforme consignados pela Magna Carta brasileira de 1988.

Diante deste cenário, questionou-se: quais os riscos inerentes à sociedade em rede? Quais os limites entre o pugilato cibernético e o direito à privacidade? E ainda: quais os meios de se mitigar os riscos intrínsecos ao pugilato cibernético?

Não se pretende abordar polêmicas de nomenclatura, a exemplo da indefinição de qual o melhor termo técnico para se referir ao pugilato cibernético: se guerra cibernética, guerra informática ou guerra virtual, ou ainda guerra de computadores. Abordar-se-ão como pugilato cibernético os termos ratificados pelo Decreto nº 6.703/2008, o qual aprovou a Estratégia Nacional de Defesa confirmando o entendimento do Ministério da Defesa (MD) sobre o tema em pauta.

Igualmente, este estudo não se aprofundará na discussão epistemológica quanto ao emprego do termo "cibernético": se seria muito amplo, por exemplo. O significado de Guerra Cibernética está relacionado ao uso de computadores em rede para alcançar vantagens, conforme conceito adotado pelo MD, qual seja:

> (...) o conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informações e redes de computadores.

[2] BRASIL. *Livro verde*: segurança cibernética no Brasil. Brasília: GSIPR/SE/DSIC, 2010. p. 13.

> Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil[3].

No âmbito militar, consagrou-se a expressão "Guerra Cibernética". No entanto, para o público em geral, pode soar estranho adotar-se o termo "guerra" para atividades que acontecem inclusive em tempo de paz, sem uma declaração formal de guerra. Utilizou-se, então, o conceito de Guerra Cibernética adotado pelo MD para definir o Pugilato Cibernético no presente trabalho, pois o termo "pugilato" facilita a compreensão da continuidade (no tempo), típica da atividade cibernética nos dias de hoje.

Em tempos de paz, também é necessário assegurar o uso das redes de computadores na jurisdição do Estado brasileiro segundo normas e padrões estabelecidos, por meio de técnicas de monitoração e defesa da rede, ou mesmo em atuação comissiva em hipóteses, onde for necessário atuar ativamente. Trata-se de atividade de mera vigilância, em regra, que busca assegurar o uso das redes dentro da lei e da ordem que se espera em tal ambiente. É evidente que ameaças significativas a redes de computadores podem acontecer a qualquer momento, como se poderá constatar pela leitura deste estudo.

A despeito de uma caracterização possível da guerra cibernética como um evento entre Estados[4], verifica-se que a definição proposta pelo MD, mais abrangente, adequa-se melhor aos referenciais deste trabalho. A escolha se baseia no fato de que qualquer ataque cibernético que ponha em risco a segurança nacional merece vigilância e reação do Estado em favor da sociedade.

Outro termo de grande relevância para este trabalho é a privacidade. Ela será explorada em seu contexto constitucional, conforme previsão do art. 5º, X, da CR/88[5].

Ressalte-se a diferenciação entre intimidade e privacidade. A intimidade relaciona a pessoa consigo mesma: alguém cantando no banheiro, alimentando seu

---

[3] BRASIL. *Portaria Normativa nº 196/EMD/MD, de 22 de fevereiro de 2007*. MD35-G-01. 2007.

[4] A esse respeito, uma definição de guerra cibernética como evento entre Estados pode ser encontrada em CLARKE, Richard A. *Cyberwar*: The Next Threat to National Security and What to do About It. New York: Ed. Ecco, 2012.

[5] Art. 5º, CR/88. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

diário, dormindo ou tomando um chá solitariamente. Quando entra um segundo ou um terceiro na relação, já não há que se falar em intimidade, mas em privacidade. A privacidade relaciona o indivíduo com aqueles que lhe são próximos. A troca de e-mails, por presumir mais de um indivíduo na comunicação, é atinente ao conceito de privacidade. A despeito de serem situações jurídicas diferentes, o direito protege as duas: protege a pessoa sozinha, consigo mesma (intimidade); e protege o indivíduo se relacionando com outros (privacidade)[6].

O Pugilato Cibernético protege potencialmente tanto a intimidade quanto a privacidade. Pode proteger a intimidade ao assegurar que informações íntimas, sejam elas escritas ou de qualquer modo armazenadas em um meio informático, não serão subtraídas do autor. Concomitantemente, protege a privacidade quando assegura que os dados que transitam em rede somente serão acessados por aqueles a quem se espera que tenham acesso às aludidas informações: numa troca de e-mails, seriam o expedidor e o destinatário.

O presente estudo tratará da privacidade em sentido amplo, compreendendo a intimidade e a privacidade propriamente dita, a despeito da distinção feita pelo ordenamento jurídico.

Outro termo cuja definição é de grande relevância para este trabalho é democracia. Para tanto, utilizou-se o conceito proferido por Abraham Lincoln, ex-presidente estadunidense, em seu discurso em Gettysburg, em 1863[7] – governo do povo, para o povo e pelo povo –, atualizado pelo doutrinador constitucional Carlos Ayres Britto, para quem este "povo" deve ser encarado como a comunidade que pretende ser. Exclui-se, portanto, qualquer sentido individualista que se possa aferir da definição, que não respeite a comunidade[8].

Em um contexto democrático, as pessoas que integram a comunidade devem ser respeitadas e tratadas com a consideração que sua condição humana suscita, conforme a democracia defendida por Ulysses Guimarães ao promulgar a Constituição brasileira de

---

[6] BRITTO, Carlos Ayres. Banca de qualificação de mestrado em Direito em 10 de novembro de 2015, no Centro Universitário de Brasília.
[7] PORTAL DA HISTÓRIA. *Discurso de Abraham Lincoln*. Disponível em: <http://www.arqnet.pt/portal/discursos/novembro01.html>. Acesso em: 26 jun. 2014.
[8] BRITTO, Carlos Ayres. *Teoria da Constituição*. Rio de Janeiro: Forense, 2003.

1988[9]. Trata-se da democracia que respeita a centralidade individual, tendo o ser humano como centro, mas sem abrir mão da coesão social. Estes dois últimos conceitos são abordados com maior profundidade no decorrer do trabalho.

Destaca-se por ora que o termo "pugilato" engloba períodos de exceção – previstos constitucionalmente[10] – e também os períodos em que o país não esteja envolvido em conflitos armados em seu território. Tal consideração territorialista decorre da postura internacional do Brasil: sua estratégia bélica se volta para a defesa territorial, o que faz com que, ainda que haja tropas brasileiras empregadas em áreas conflituosas, o momento atual seja considerado tempo de paz.

As políticas públicas são entendidas neste estudo como escolhas da sociedade realizadas por meio do governo em ação[11], com planejamento específico por meio de projetos, programas e ações definidas e voltadas para setores específicos da sociedade. Por certo se pode entender a atitude omissiva do governo como uma opção política. Não se pretende explorar a teoria de políticas públicas, mas apenas e tão somente trazer possibilidades de implementação de políticas públicas úteis para a sociedade num contexto em que se depende de forma significativa de redes de computadores. Em que pese não haver intenção de aprofundar, o estudo trata brevemente das políticas públicas de segurança cibernética no Estado brasileiro.

---

[9] AGENCIA BRASIL. *Marco entre a ditadura e a democracia, constituição de 1988 completa 25 anos.* Disponível em: <http://memoria.ebc.com.br/agenciabrasil/noticia/2013-10-04/marco-entre-ditadura-e-democracia-constituicao-de-1988-completa-25-anos>. Acesso em: 30 jun. 2014.

[10] Os Estados de Exceção previstos na Constituição da República de 1988 (intervenção, estado de defesa, estado de sítio), quando ocorrem, podem mitigar alguns direitos e garantias assegurados, em regra, àqueles sob jurisdição brasileira com a finalidade de que sejam atendidas necessidades na forma do texto constitucional *infra*:
**Art. 34**. A União não **intervirá** nos Estados nem no Distrito Federal, exceto para(...)
**Art. 136**. O Presidente da República pode, ouvidos o Conselho da República e o Conselho de Defesa Nacional, decretar estado de defesa para preservar ou prontamente restabelecer, em locais restritos e determinados, a ordem pública ou a paz social ameaçadas por grave e iminente instabilidade institucional ou atingidas por calamidades de grandes proporções na natureza. (...)
**I - restrições aos direitos de:**
a) reunião, ainda que exercida no seio das associações;
**b) sigilo de correspondência;**
**c) sigilo de comunicação telegráfica e telefônica;** (...)
**Art. 137**. O Presidente da República pode, ouvidos o Conselho da República e o Conselho de Defesa Nacional, solicitar ao Congresso Nacional autorização para decretar o estado de sítio nos casos de:
I - comoção grave de repercussão nacional ou ocorrência de fatos que comprovem a ineficácia de medida tomada durante o estado de defesa;
II - declaração de estado de guerra ou resposta a agressão armada estrangeira. (...)
**Art. 138**. O decreto do estado de sítio indicará sua duração, as normas necessárias a sua execução e as **garantias constitucionais que ficarão suspensas**, e, depois de publicado, o Presidente da República designará o executor das medidas específicas e as áreas abrangidas. (...) (grifo nosso)

[11] GOBERT, Muller. Políticas públicas. In: VAZ., L.G.D. *Revista nova Atenas de educação e tecnologia*. São Luiz do Maranhão: CEFET. 2007. v. 10. n. 01, jan./jun.

A privacidade *on-line* é um assunto que ganha cada vez mais importância, vez que tudo que transita na rede de computadores é suscetível de investigação. Quando não é possível a investigação do conteúdo, é possível investigar outros dados como a frequência e a convergência entre endereços. Até mesmo chefes de Estado têm sido espionados por agentes de inteligência de outros Estados. Mesmo empresas estatais, conforme denunciou Edward Snowden no caso da espionagem da Agência de Inteligência Americana (NSA) contra a Petrobrás, sofrem grandes prejuízos devido a espionagens executadas por órgãos de outros países[12].

Percebe-se que Estados podem tentar auferir todo tipo de vantagens de outros por meio de redes de computadores. Porém, essa possibilidade não se limita aos Estados. A espionagem empresarial também acontece em ambiente cibernético. Nesse contexto, a defesa de todo um país pode se ver ameaçada por um grupo de pessoas altamente especializadas, ou mesmo por um adolescente com grande conhecimento técnico em rede de computadores, que consiga entrar em sistemas estratégicos ligados em rede. Em razão das hipóteses mencionadas, a sociedade pode tomar atitudes preventivas e/ou coercitivas visando à manutenção da paz social, do Estado Democrático de Direito e a preservação da ordem econômica.

Neste ponto, deve-se fomentar o debate a respeito dos limites do respeito à privacidade por parte do Estado constituído, pois a privacidade e o Pugilato Cibernético podem tomar posições antagônicas, devendo a sociedade decidir quais as políticas públicas e os limites adequados a cada um destes institutos.

O trabalho aborda ainda alguns direitos fundamentais de interesse no contexto do assunto inclusive, discorrendo sobre direitos fundamentais de sociedades empresárias. A pauta é a busca do equilíbrio entre a preservação de conquistas civilizatórias – tais como o direito à privacidade – e outras necessidades que a comunidade também apresenta. Num rol exemplificativo, direitos fundamentais como a privacidade, dignidade, liberdade, sigilo das comunicações, a propriedade, a função social da propriedade, são de alguma forma abordados no presente estudo.

---

[12] SNOWDEN, Edward. *Milênio*: Sonia Bridi entrevista Edward Snowden. Disponível em: <http://globotv.globo.com/globo-news/milenio/v/milenio-sonia-bridi-entrevista-edward-snowden/3389933/>. Acesso em: 08 jun. 2014.

Outro aspecto abordado é a possibilidade de implementação pelo Estado de políticas públicas que potencializem ganhos necessários e úteis para a sociedade que perpassem o tema em estudo; considerando o respeito às leis e as dificuldades de manutenção da ordem jurídica em ambiente cibernético.

Bucci, ao discorrer sobre políticas públicas mostrou que seu conceito decorre de um arranjo complexo que transcende uma só disciplina, mas as evidencia como um conjunto de medidas propositais, com o objetivo de impulsionar o Estado, para que seja concretizado algum objetivo de ordem pública; materializando, assim, um direito[13]. Saravia conceitua tais políticas como um fluxo de decisões estatais que tem por escopo na manutenção de um equilíbrio social; ou ainda voltado para desequilibrar tais relações visando a mudança do *status quo*[14]. Destarte se conclui tratar de uma definição complexa e transdisciplinar, mas que pode ser simplificada numa ação estatal voltada para o atendimento de uma demanda comunitária.

O tema deste trabalho evidencia a contraposição entre privacidade e Segurança Nacional, e, eventualmente, a garantia da lei e da ordem em contexto de pugilato cibernético, abordando de forma exemplificativa riscos, possibilidade de implementação de políticas públicas, e ainda conquistas e necessidades sociais.

Estados geralmente reservam a si próprios a competência exclusiva de prover a segurança estabelecida por meio de seus cidadãos (representados ou não), o que inclui limitar a ação daqueles que tentam violar, no caso do Brasil, a ordem constitucional.

A paz é um período de preparação contínua para a guerra, identificando potenciais ameaças e buscando o aprimoramento cognitivo e de equipamentos a serem empregados em situações excepcionais: crise e guerra. Sun Tzu Sun Pin, autor do clássico *A arte da guerra*, ensinava há séculos: "se buscas a paz, prepara-te para a guerra"[15]. Mesmo sem guerra declarada, os Estados devem estar preparados para se defender de ameaças no momento em que estas ocorrerem, reforçando a ideia do

---

[13] BUCCI, Maria Paula Dallari. O Conceito de Política Pública em Direito. In: BUCCI, Maria Paula Dallari (Org.). *Políticas públicas*: reflexões sobre o conceito jurídico. São Paulo: Saraiva, 2006.

[14] SARAVIA, Enrique. *Política pública, política cultural, indústrias culturais e indústrias criativas.* In: Plano da Secretaria da Economia Criativa: políticas, diretrizes e ações, 2011 – 2014. Brasília: Ministério da Cultura, 2011. p. 93.

[15] PIN, Sun Tzu Sun. *A Arte da Guerra*. Trad. COTRIN, Ana Aguiar. São Paulo: Ed. Martins Fontes, 2002.

pugilato incessante. Pelo preparo, naturalmente as ameaças ocorrem com menor frequência.

O trabalho não foca o contexto de Estado absolutista, como descrito por Thomas Hobbes[16], nem mesmo outro modelo em que o Estado serve a um grupo de pessoas. Ao invés disso, parte-se da hipótese de eventual ameaça virtual acontecer no contexto da teoria que coloca o Estado a serviço da sociedade, com a finalidade de protegê-la: uma comunidade democrática. A grande diferença no enfoque acaba sendo no objetivo da defesa cibernética. A premissa nesta análise é de que toda preparação para a defesa cibernética só é válida se for a favor de toda a comunidade, sem privilegiar pessoas, grupos, nem classes sociais.

Para Norberto Bobbio, "nos lugares onde o Direito é impotente, a sociedade corre o risco de precipitar-se na anarquia; onde o poder não é controlado, corre o risco oposto, do despotismo"[17]. No mesmo sentido, Karl Popper formula que não existe liberdade que não seja garantida pelo Estado e, em contrapartida, só um Estado controlado por cidadãos livres pode oferecer-lhes alguma dose razoável de segurança[18]. Por sua vez, Carlos Ayres Britto[19] expõe o risco que passa a existir contra a democracia quando o Estado resolve monitorar a cultura, limitando sua espontaneidade em qualquer de suas formas de exteriorização, indicando que a Constituição da República de 1988 estatui, pelo inciso IX do seu art. 5º, que é "livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença". A

---

[16] HOBBES, Thomas. *Leviatã ou matéria, Forma e poder de um Estado eclesiástico e civil*. Trad: MONTEIRO. João Paulo e NIZZA. Maria Beatriz da Silva. São Paulo: Abril Cultural, 1984.Coleção Os Pensadores. Para HOBBES, "A única maneira de instituir um tal poder comum, capaz de defendê-los das invasões dos estrangeiros e das injúrias uns dos outros, garantindo-lhes assim uma segurança suficiente para que, mediante seu próprio labor e graças aos frutos da terra, possam alimentar-se e viver satisfeitos, é conferir toda sua força e poder a um homem, ou a uma assembleia de homens, que possa reduzir suas diversas vontades, por pluralidade de votos, a uma só vontade. O que equivale a dizer: designar um homem ou uma assembleia de homens como representante de suas pessoas, considerando-se e reconhecendo-se cada um como autor de todos os atos que aquele que representa sua pessoa praticar ou levar a praticar, em tudo o que disser respeito à paz e segurança comuns; todos submetendo assim suas vontades à vontade do representante, e suas decisões a sua decisão. Isto é mais do que consentimento, ou concórdia, é uma verdadeira unidade de todos eles, numa só e mesma pessoa, realizada por um pacto de cada homem com todos os homens, de um modo que é como se cada homem dissesse a cada homem: Cedo e transfiro meu direito de governar-me a mim mesmo a este homem, ou a esta assembleia de homens, com a condição de transferires a ele teu direito, autorizando de maneira semelhante todas as suas ações. Feito isto, à multidão assim unida numa só pessoa se chama Estado, em latim civitas."

[17] BOBBIO. Norberto. *O tempo da memória*. In: BOBBIO. Norberto. A Era dos Direitos. Rio de Janeiro: Elsevier, 2004.

[18] POPPER, Karl. *As Aventuras da Racionalidade*. (Org.) PEREIRA, Julio Cesar R. Porto Alegre: EDIPUCRS, 1995. p. 140 e 141.

[19] BRITTO, Carlos Ayres. *Teoria da Constituição*. Rio de Janeiro: Forense, 2003.

proposta de utilidade do pugilato neste estudo é contextualizada como mais um instrumento da manutenção da ordem constitucional e dos valores democráticos. Os conceitos aqui expressos evidenciam a necessidade da manutenção do Estado de Direito para que a comunidade tenha a segurança necessária para se desenvolver. O desenvolvimento social sem ordem e estabilidade tende ao insucesso. Num contexto de pugilato cibernético, fazer valer as escolhas da sociedade vai depende da melhor preparação possível para a defesa cibernética.

A pesquisa não teve como objetivo explorar aspectos de segurança pública. Por vezes, o pugilato cibernético pode proteger a sociedade em face de meros ilícitos civis, mas este não é o foco de uma defesa que pretende atuar quando estão ameaçados os valores mais caros a uma nação.

O trabalho analisa, ainda, hipóteses de risco em que o poder judiciário pode ser incapaz de fazer valer a lei por si só, propondo algumas possíveis ações governamentais que podem concorrer para a paz e prosperidade almejadas pela sociedade, a partir do pugilato cibernético.

Ameaças cibernéticas estão constantemente presentes em desfavor de pessoas e instituições em todo o planeta. Como um evento danoso pode se originar em qualquer lugar, a qualquer momento e contra qualquer pessoa, a segurança depende de prevenção e prontidão para responder de maneira proporcional. A sociedade pode exigir reações a tais ameaças inesperadas, se lhe convier. Se a reação por parte do Estado for consensual no seio da sociedade, a preparação técnica no que diz respeito ao pugilato cibernético deve ser contínua. A preparação ideal não termina, apenas se aperfeiçoa. A aptidão técnica pode se dar por meio do aperfeiçoamento técnico de equipamentos ou pela formação e preparação dos profissionais da área e seus bancos de dados. Ambas as possibilidades podem ser fomentadas por políticas públicas.

Assim como para a polícia é útil a utilização de bancos de dados e análises estatísticas para aperfeiçoar a sua atuação, quem atua profissionalmente com pugilato cibernético terá resultado sinérgico pelo uso da estatística e de bancos de dados, sem os quais o labor de análise das ameaças cibernéticas fica sem foco e sem resultado eficiente.

O trabalho de defesa cibernética certamente será repressivo, mas deve ser também – e com muito mais razão, nesse caso – preventivo, de forma a perseguir economicidade e eficiência, que são princípios da Administração Pública.

O setor cibernético é um dos setores estratégicos, de acordo com a Estratégia Nacional de Defesa[20] (END), aprovada pelo Decreto nº 6.703, de 18 de dezembro de 2008. Segundo a END, "projeto forte de defesa favorece projeto forte de desenvolvimento"[21]. Outrossim, a END não se dissocia de estratégia nacional de desenvolvimento: tais estratégias são complementares no escopo do despertar para a nacionalidade e da construção da nação. O modelo de desenvolvimento depende da estabilidade gerada pela defesa eficaz. Para que o Brasil se mostre um Estado próspero, faz-se necessária uma boa preparação contra agressões, mas também contra ameaças, visto que no mundo de hoje a intimidação tripudia sobre a boa fé. Assim sendo, não há substituto para o envolvimento da sociedade brasileira no debate e na construção de sua própria defesa.

A Defesa deve trabalhar com tecnologias de ponta, e o fomento do desenvolvimento nacional de tecnologias de Defesa acaba por desenvolver tecnologias de uso dual: usadas na defesa e em outros ambientes, agregando valor a produtos, serviços e tecnologias oferecidos no Brasil.

A Estratégia Nacional de Defesa pauta-se ainda pelo poder de dissuasão, complementando que, para dissuadir, é necessária preparação para o combate. Finalmente, a END complementa que as Forças Armadas devem ser organizadas sob a égide do trinômio monitoramento/controle, mobilidade e presença[22]. Com isso, fica claro que existe uma opção do Estado no sentido de se defender de possíveis ataques mediante preparação em tempo de paz, complementado pelo monitoramento/controle, mobilidade e presença. Daí se pode entender que o Estado ratifica a necessidade de bancos de dados que auxiliem na preparação para o combate e contribuam com a

---

[20] O Decreto nº 6.703, de 18 de dezembro de 2008, aprova a Estratégia Nacional de Defesa, observe-se:
Art. 1º Fica aprovada a Estratégia Nacional de Defesa anexa a este Decreto.
Art. 2º Os órgãos e entidades da administração pública federal deverão considerar, em seus planejamentos, ações que concorram para fortalecer a Defesa Nacional.
Art. 3º Este Decreto entra em vigor na data de sua publicação.

[21] BRASIL. Ministério da Defesa. *Estratégia Nacional de Defesa*. 2. ed. Brasília, 2008. p. 8-10.

[22] Ibidem. p. 10.

preservação da paz social, razão pela qual o pugilato cibernético é uma atividade que deve se iniciar desde o tempo de paz[23], mesmo sem qualquer ameaça em vista.

Outro ponto importante a ser tratado decorre da subordinação das Forças Armadas ao poder político como pressuposto do regime republicano e como um fator de garantia democrática, democracia que deve ser preservada em sua plenitude[24]. Pode-se afirmar que o respeito sistemático ao Estado democrático desembocará no humanismo como expressão de vida coletiva civilizada, e este responderá pela qualidade de vida de todo um povo[25].

A expressão do poder militar deve ser mais uma expressão do poder do Estado servindo ao povo, não sendo aceitável a ideia de que o Estado se sirva do povo que o sustenta. A preparação para o pugilato deve ter por norte a preservação da paz.

O objetivo de preservação da ordem democrática pode ser materializado no cumprimento da ordem constitucional decorrente de uma assembleia nacional constituinte, consoante Carlos Ayres Britto[26]. O referido autor ensina que o povo "é [realiza] o poder de tudo poder, em termos jurídicos, e no plano territorial interno", materializando a soberania. Povo sem soberania é apenas população. Povo amalgamado no seu território forma uma nação, que pode se tornar comunidade por meio de uma real comunhão de interesses. A soberania popular se manifesta no poder constituinte primário (ou inicial), que se materializa na própria Constituição. O poder constituinte originário materializa a criação de um novo Estado[27].

Hierarquicamente inferiores à Constituição, as leis (em sentido amplo) visam a normatizar a vida em sociedade. A Lei nº 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos, visa a tutelar dados existentes em banco de dados eletrônicos. Tal inviolabilidade de dados armazenados decorre também do mandamento constitucional previsto no art. 5º, X, CR/88, o qual protege o direito à privacidade e intimidade.

---

[23] BRASIL. Ministério da Defesa. Estratégia Nacional de Defesa. 2. ed. Brasília, 2008. p. 10
[24] Ibidem. p. 6-13
[25] BRITTO, Carlos Ayres. *O humanismo como categoria constitucional*. Rio de Janeiro: Ed. Forum, 2012. p. 25-29.
[26] BRITTO, Carlos Ayres. *Teoria da Constituição*. Rio de Janeiro: Forense, 2003.
[27] Ibidem. p. 20-25.

A sociedade necessita de instrumentos de controle para fazer valer suas opções materializadas nas normas. A norma materializa o que se pode entender por gestão de riscos sociais. Se determinada conduta oferece grande risco social, ela provavelmente será criminalizada, o revés acontecerá com uma conduta que pouco ou nenhum risco oferece para a sociedade.

Logo, em princípio, conhecidas as condutas que resultam em significativos riscos sociais, é usual criminalizá-las ou de alguma forma desestimulá-las. Neste ponto cabe a observação de que diferentes povos tutelam diferentes valores, o que justifica que criminalizem distintas condutas. Com este entendimento, evidencia-se que não se pode contar necessariamente com o apoio de outros Estados, quando determinada conduta fere bens caros à sociedade. Pode ser que, em outra cultura, tal bem jurídico não seja tão relevante a ponto de se conseguir apoio estrangeiro para coibir condutas indesejadas em redes de computadores. O problema é que as fronteiras na rede mundial de computadores não correspondem às fronteiras físicas.

Uma vez tipificados, os crimes cibernéticos devem ser combatidos e evitados. Terá grandes limitações o combate aos crimes cibernéticos somente pela norma jurídica estabelecida por um Estado. Tais restrições se devem, sobretudo, ao princípio da territorialidade: um crime pode ser praticado, apenas como exemplo, na China, por meio de provedores russos, por um cidadão de Kiribati, trabalhando em favor de uma sociedade empresária localizada na África, com consequências em desfavor da sociedade e instituições brasileiras e indianas. A justiça brasileira tem competência para atuar nesse caso?

Uma solução para a situação hipotética pode ser viabilizada pelo pugilato cibernético, garantindo o cumprimento das normas impostas, utilizando-se da supremacia técnica, quando se fala de rede de computadores. A necessidade técnica de um banco de dados estatal com a finalidade de otimizar a defesa (inclusive a cibernética) tem sido implementada em países centrais[28]. A filosofia da interceptação[29] pode se ver concretizada no Projeto Echelon[30], fruto de um acordo preliminar entre o

[28] No sentido de Estados com destaque político e econômico no contexto mundial.
[29] Para mais informações sobre a filosofia das interceptações: BOATTI, Giorgio; TAVAROLI, Giuliano. *SPIE: I servizi segreti delle multinazionali*: dossier, intercettazioni, guerre informatiche. Milano: Mondadori. 2008. p. 196 e ss.
[30] LAWNER, Kevin J. *Post-Sept. 11th international surveillance activity*: a failure of intelligence: the echelon interception system & (and) the fundamental right to privacy in Europe. Disponível em:

Reino Unido e os Estados Unidos da América (Pacto UKUSA), e que depois se estendeu para outros países, como Canadá, Austrália e Nova Zelândia. Inicialmente, o projeto era apenas para analisar as comunicações por rádio do adversário soviético. Hoje, há quem diga que o aparato é utilizado para espionagem econômica, contra o terrorismo e contra o crime organizado.

Há autores que afirmam que toda transmissão telefônica, de fax, internet ou mensagens eletrônicas que trafegam na rede mundial de computadores estão suscetíveis de interceptação, o que pode acontecer com a ajuda de supercomputadores que buscam palavras-chave nos dados que passam pelos sistemas[31]. Ao que parece pelo menos alguns Estados se preocupam em montar este banco de dados por diversos motivos, dentre os alegados, a segurança nacional.

Supostamente, este projeto utilizado como exemplo – pois não é o único, conforme se afirma em sítios como *Wikileaks*[32] ou mesmo por Snowden[33] – impacta na privacidade de todos aqueles que utilizam meios de comunicações modernos, inclusive comunicação de mensagens de videogames.

De forma bem clara, países centrais têm mitigado a privacidade em nome da segurança. Em época de ataques terroristas, sobretudo no contexto norte americano pós 11 de setembro de 2001, tal mitigação parece necessária, ou ao menos tem ganhado grande número de adeptos.

Se no Brasil o respeito à privacidade recebe a proteção do ordenamento jurídico, tal como previsto na Constituição da República e na Lei nº 12.965, de 23 de abril de 2014[34], em outros países essa proteção é relativizada na forma da Lei e/ou da *praxis* administrativa. Como redes informáticas não respeitam fronteiras, a proteção constitucional à privacidade oferecida em território brasileiro respeita o princípio da territorialidade. No entanto, o usuário brasileiro que acessa um provedor estrangeiro terá relativizada esta proteção na medida do ordenamento alienígena, sem que o usuário

<http://heinonline.org/HOL/LandingPage?handle=hein.journals/pacinlwr14&div=22&id=&page=>. Acesso em: 7 fev. 2016.

[31] BOATTI, Giorgio; TAVAROLI, Giuliano. *SPIE*: *I servizi segreti delle multinazionali*: dossier, intercettazioni, guerre informatiche. Milano: Mondadori. 2008. p. 71-76.

[32] wikileaks.org. Acesso em: 26 jun. 2014.

[33] Edward Joseph Snowden é um analista de sistemas, ex-funcionário da CIA e ex-contratado da NSA que tornou público detalhes de vários programas que constituem o sistema de vigilância global da NSA – Agência de Inteligência Estadunidense.

[34] Lei nº 12.965, de 23 de abril de 2014, que estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil.

tenha saído do território brasileiro. Ainda que determinada conduta seja condenada em juízo no Brasil, é possível que, em razão do respeito à soberania de outro Estado, a decisão não surta efeito prático.

O princípio da territorialidade está previsto no artigo 5º do Código Penal[35]. Pelo referido princípio, a norma penal só se aplica no território do Estado que a editou. No Brasil, se diz que a territorialidade é temperada porque o *caput* do art. 5º do Código Penal admite que tratados e regras de direito internacional mitiguem tal mandamento. Nestas hipóteses, a lei orienta que o Estado brasileiro se abstenha de aplicar a sua lei.

O princípio da extraterritorialidade é aquele a partir do qual um Estado prevê que sua norma alcance, em determinadas circunstâncias, limites fora do território onde possui soberania, fora de suas fronteiras. O art. 7º do Código Penal aduz hipóteses nas quais a Lei Penal brasileira pretende alcançar jurisdição fora do território onde detém soberania.

Percebe-se, com isso, que se Estados preveem hipóteses de aplicação de sua própria norma penal em territórios onde não possuem soberania, o que pode resultar em conflitos entre normas de diferentes nacionalidades, sobretudo em hipóteses de crimes informáticos, também conhecidos como crimes cibernéticos.

O art. 3º da Lei nº 12.965, de 23 de abril de 2014 – a qual disciplina o uso da internet no Brasil – assegura em seu inciso II a proteção à privacidade na rede. Mas o que fazer se a lesão à privacidade acontece a partir de uma agência de inteligência estrangeira? A única solução efetiva será a técnica, pois a diplomacia dificilmente conseguirá fazer valer a norma nacional em outro país. O Estado estrangeiro continuará fazendo tudo o que sua norma prevê, ainda que viole normas brasileiras e isso implique na mitigação da privacidade no Brasil. Certo é que aberrações podem ser colocadas como exemplo a ser combatido pela comunidade internacional, tais como a espionagem

---

[35] Art. 5º. Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao **crime cometido no território nacional**.
§ 1º. Para os efeitos penais, **consideram-se como extensão do território nacional** as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro onde quer que se encontrem, bem como as aeronaves e as embarcações brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto-mar.
§ 2º. É também aplicável a lei brasileira aos crimes praticados a bordo de aeronaves ou embarcações estrangeiras de propriedade privada, achando-se aquelas em pouso no território nacional ou em voo no espaço aéreo correspondente, e estas em porto ou mar territorial do Brasil. (grifo nosso)

de comunicações da Presidente da República do Brasil e da Chanceler alemã realizadas pela NSA, conforme relatado por Snowden[36].

O estadunidense *Freedom Act*, sucessor do *Patriotc Act*, a Lei canadense antiterror de 2015, o órgão chinês de combate ao terrorismo com poderes irrestritos de investigação e a norma francesa de combate ao terror podem ser colocados como exemplos de possibilidades de mitigação de privacidade e outros direitos individuais[37] de usuários de redes de computadores em qualquer lugar do planeta, independente do bem jurídico tutelado pela norma do território em que se encontram. A eficiência desses regramentos parece justificar a existência de tais normas em democracias reconhecidas, tais como Estados Unidos, Canadá e França.

Crimes e ilícitos cibernéticos podem ferir profundamente uma sociedade, pois podem ameaçar serviços públicos essenciais – como distribuição de energia elétrica e de água, centrais telefônicas, serviços hospitalares –, instituições bancárias, bolsas de valores, privacidade de cidadãos comuns e de autoridades etc. Enfim, podem ameaçar as instituições e a paz social de um Estado.

No debate deve ainda ser considerado que um governo que não respeita as leis, a ética ou seus cidadãos não é suficientemente confiável para manipular dados pessoais, visto que pode utilizar estas informações a favor de um grupo ou um partido, e não em favor da coletividade.

Pelo princípio da precaução, o ideal é que toda investigação cibernética, por ser essencialmente técnica, bem como seus resultados, passem ao largo do controle político, como forma de proteger a própria sociedade. Entende-se que as investigações devam ser dirigidas por instituições acostumadas a lidar com políticas de Estado, não se subordinando a políticas de governo.

Atualmente, alguns governos pelo mundo que se dizem democráticos não permitem o livre debate, inviabilizam a imprensa que lhes faz oposição, manipulam informações, maculam a democracia com a ajuda de seus correligionários, com atitudes nefastas que prejudicam toda a sociedade. Pode-se citar como exemplo mais

---

[36] SNOWDEN, Edward. *Milênio*: Sonia Bridi entrevista Edward Snowden. Disponível em: <http://globotv.globo.com/globo-news/milenio/v/milenio-sonia-bridi-entrevista-edward-snowden/3389933/>. Acesso em: 8 jun. 2014.

[37] PEROSA, Teresa. *O Brasil na era do terror*. In: Revista Época nº 920. São Paulo: Ed. Globo, 2016. p. 54-56.

contundente próximo ao Brasil, a Venezuela, cujos governos têm calado opositores[38]. Por certo se espera que a evolução seja um veículo para que este tipo de atitudes seja banido dos governos; porém, enquanto não o são, o corpo social de um Estado não deve permitir que interesses alheios aos interesses nacionais disponham de dados pessoais. O Estado deve servir à comunidade, e não se servir da comunidade. Se o objetivo não for claramente esse, o Estado ainda não estará preparado para manipular dados pessoais.

É inconteste que países centrais possuem centros de inteligência, e que deles dependem para assegurar seus interesses, mitigando riscos contra sua população e suas instituições. Mesmo em países desenvolvidos, pode acontecer que agentes públicos sintam-se tentados a utilizar esta forma única de prover segurança como forma de ataques e agressões contra a coletividade, fomentando qualquer coisa diferente de paz e prosperidade. Sítios como *Wikileaks* e pessoas como Edward Snowden têm declarado isto pelo mundo e sofrido consequências aparentemente pouco democráticas. Observe-se que Edward está exilado na Rússia e Julian Assange, fundador do *Wikileaks*, foi considerado por um comitê da Organização das Nações Unidas em fevereiro de 2016 como "detido arbitrariamente"[39].

A internet, apesar de passar para alguns uma impressão diferente, não é um ambiente típico para quem busca privacidade, e o usuário deve levar este fato em consideração. A maior parte dos dados da rede mundial de computadores transita sem qualquer tecnologia de segurança da informação[40]. Considere-se, ainda que muitos se utilizem da internet para divulgar o que estão fazendo, postar opiniões, fotos, informações algumas vezes íntimas. Falar de privacidade no ambiente do *Twitter* e *Facebook* é algo polêmico. Tal constatação ganha contornos ainda mais amplos diante do seguinte dado: em 2013, o *Facebook* conseguiu conquistar 83 milhões de usuários brasileiros ativos[41].

---

**38** PORTAL G1. *Canal de TV de oposição é retirado do ar na Venezuela.* Disponível em: <http://g1.globo.com/Noticias/Mundo/0,,MUL1460686-5602,00-CANAL+DE+TV+DE+OPOSICAO+E+RETIRADO+DO+AR+NA+VENEZUELA.html>. Acesso em: 30 jun. 2014.

39 ÉPOCA. *Julian Assange pode deixar embaixada do Equador nesta sexta*. Disponível em: <http://epoca.globo.com/tempo/filtro/noticia/2016/02/fundador-do-wikileaks-assange-pode-deixar-embaixada-do-equador-nesta-sexta-feira.html>. Acesso em: 6 fev. 2016.

40 HARRIS, Shon. *CISSP*. Sixth Edition. USA: Mc Graw Hill, 2013. p. 21-155

41 IDC. *Os números do Facebook, dez anos após sua criação*. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/os-numeros-do-facebook-dez-anos-apos-sua-criacao#5>. Acesso em: 26 jun. 2014.

Cria-se, desta forma, a necessidade de conciliar a necessidade de privacidade com a necessidade de que seja desempenhado o papel de quem labuta em prol da segurança da comunidade com o pugilato cibernético. A tal conflito pode se ofertar solução inspirada nos ensinamentos de Habermas[42]: toda argumentação tentará ser a "única resposta correta", mas deverá se contentar em ser apenas "aceitabilidade idealmente justificada" dos enunciados. Em outras palavras, eventualmente, uma proposta não pretende ser absoluta, mas algo que se considere aceitável por todos, sabendo-se que, quanto mais heterogênea é a sociedade, mais abstratas são as normas que a regem, fornecendo a segurança necessária para que a comunidade brasileira viva com qualidade e se desenvolva com responsabilidade e sustentabilidade.

Fazer valer os direitos assegurados aos cidadãos pelo Estado por meio do uso da força, ainda que esta força seja virtual, faz parte da vida em comunidade, e é necessário para a paz social. O Estado deve, ao menos, estar pronto para empregar este instrumento em favor dos cidadãos.

O pugilato cibernético é o meio mais eficaz de o Estado se prevenir contra ameaças advindas de redes informatizadas. Sem tal aparato, o Direito não tem como garantir que se imponham decisões judiciais, o que pode colocar em risco a lei e a paz social.

O presente estudo tem por escopo, verificando os limites entre o direito à privacidade e a defesa cibernética, abordar políticas públicas de defesa cibernética. Para que o objetivo seja cumprido, o trabalho foi dividido em quatro capítulos a saber: no capítulo primeiro são abordados os riscos inerentes à sociedade em rede decorrentes do uso do ciberespaço. São analisados riscos estratégicos, que ameaçam a sobrevivência do Estado; riscos individuais, considerados ameaças de privação de serviços públicos e de direitos fundamentais; e riscos atinentes às empresas. No segundo capítulo, aborda-se o pugilato cibernético e algumas de suas consequências no direito à privacidade sob as óticas normativa e jurisprudencial. No capítulo terceiro são analisadas algumas dificuldades jurídicas relacionadas ao direito cibernético, abordando aspectos da ADI 3059MC/RS. O quarto capítulo destina-se à análise da mitigação de riscos oriundos do pugilato cibernético a partir da atuação do Estado em favor da sociedade.

---

[42] HABERMAS, Jürgem. *Verdade e Justificação*: Ensaios Filosóficos. São Paulo: Edições Loyola, 2004. p. 267-310.

Utilizando-se de pesquisa documental e bibliográfica, seguiram-se os métodos de abordagem analítico descritivo, dedutivo e lógico-indutivo. A presente pesquisa aplicada aborda o tema de forma quantitativa e qualitativa, com objetivos exploratórios e descritivos.

# 1 RISCOS INERENTES À SOCIEDADE EM REDE DECORRENTES DO USO DO CIBERESPAÇO

Informação é poder. E, para combater o bom combate, como sugere Sun-Tzu, deve-se conhecer o inimigo e a si próprio. Em capítulo de sua obra intitulado "Da arte de vencer sem desembainhar a espada", Sun-Tzu[43] diz que faz parte do caminho da vitória conhecer e não ignorar o oponente, sendo de suprema importância atacar a estratégia do oponente na raiz. Aconselha ainda, a sondar os planos do oponente como forma de aperfeiçoamento e planejamento para o êxito.

Um dentre muitos dos ensinamentos desse estrategista da antiguidade que permanece válido nos dias de hoje é a importância da coleta de informações, sobre si e sobre o potencial adversário. A informação serve como fonte de poder de defesa e de ataque. Com a intenção de coletar dados, países que dominam tecnologias de ponta têm investido em sistemas informatizados, o que lhes permite conhecer potenciais ameaças e, consequentemente, melhor combatê-las.

Apenas para ilustrar, em 2013, de acordo com dados obtidos pelo jornalista Glenn Greenwald com o ex-técnico da NSA Edward Snowden, a então presidente brasileira foi alvo direto de espionagem realizada pela NSA, inclusive por meio da interceptação de *e-mails*[44]. Segundo Edward Snowden, a rede privada de computadores da Petrobrás foi espionada[45]. Neste exemplo, a presidente à época do Brasil e a referida empresa estatal não são inimigas dos norte americanos. Porém, a ameaça em potencial foi, aparentemente, o suficiente para motivar uma ação de inteligência de Estado.

A fim de explorar melhor os exemplos citados, cabem algumas considerações. A Petrobrás S.A. é uma sociedade empresária de economia mista de alto valor estratégico, que possui alto saber tecnológico, e que domina algumas tecnologias de ponta. A S.A. pode despertar o interesse de agências de inteligência – sobretudo norte americanas – não só pelo conhecimento tecnológico acumulado, como também para proteger o

---

[43] PIN, Sun Tzu Sun. *A Arte da Guerra*. Trad. COTRIN, Ana Aguiar. São Paulo: Ed. Martins Fontes, 2002. p. 20-34.

[44] FOLHA DE S PAULO. Caderno Mundo. 02/09/2013. *Dilma foi espionada pelos EUA, diz TV*. Disponível em: <http://www1.folha.uol.com.br/mundo/2013/09/1335522-dilma-foi-espionada-pelos-eua-diz-tv.shtml>. Acesso em: 7 fev. 2015.

[45] PORTAL G1. *Petrobras foi espionada pelos EUA, apontam documentos da NSA*. Fantástico. Edição do dia 08/09/2013. Disponível em: <http://g1.globo.com/fantastico/noticia/2013/09/petrobras-foi-espionada-pelos-eua-apontam-documentos-da-nsa.html>. Acesso em 7 fev. 2015.

patrimônio de estadunidenses que investiram em ações da empresa na bolsa de valores. Atualmente, a estatal brasileira está em crise e perdeu parte considerável de seu valor de mercado em razão de corrupção com raízes, ao que parece, no próprio Estado brasileiro[46]. Sua recuperação no mercado de ações já é perceptível, mas continua incipiente.

Sobre o outro caso citado, o Jornal *The New York Times* declara que a então Presidente Dilma Rousseff continuou sendo espionada em 2015[47], enquanto a Presidência da República declarou que decidiu ignorar denúncia de que a chefe do executivo brasileiro teria tido suas comunicações monitoradas[48].

Percebe-se, pois, que uma grande empresa brasileira – que atua em um setor estratégico – e uma das ocupantes do cargo político de maior destaque do Brasil estão suscetíveis aos ataques cibernéticos: um dos meios utilizados para as referidas ações de inteligência. Naturalmente, as informações obtidas a partir desta forma de espionagem podem ameaçar potencialmente a qualidade de vida e a economia no Estado alvo dos ataques. A coleta de dados estratégicos de um país por outro pode refletir, *v.g.*, na vantagem de competitividade empresarial e no consequente reflexo nos empregos oferecidos e na arrecadação de tributos.

Muitos são os riscos inerentes à sociedade na rede de computadores. Num rol meramente exemplificativo, podem ser citados: o risco de coleta de informações privadas as quais o autor gostaria de manter reservadas; riscos à privacidade quando da troca de dados por redes; risco de terrorismo cibernético; risco de ataque de grupos organizados, sejam eles estatais ou não; risco de ataque a estruturas de prestação de todo tipo de serviço púbico, dentre outros.

A partir do conceito de risco do *Project Management Body of Knowledge* (PMBOK), em sua 5ª edição, pode-se aduzir que o conceito de risco é relacionado a um evento ou condição não sabida que se ocorre provoca um efeito decorrente de uma ou

---

[46] IDOETA, Paula Adamo. *Como a Petrobras virou 'dor de cabeça' para governo e investidores.* Disponível em: <http://www.bbc.co.uk/portuguese/noticias/2014/03/140320_petrobras_governo_pai>. Acesso em: 7 fev. 2015.

[47] SOUZA, Beatriz. *Dilma continua sendo espionada pelos EUA, diz NY Times.* Disponível em: <http://exame.abril.com.br/brasil/noticias/dilma-continua-sendo-espionada-pelos-eua-diz-ny-times>. Acesso em 7 fev. 2015.

[48] FOLHA VITÓRIA. *Planalto decide ignorar denúncia de que Dilma continua sendo espionada*. Disponível em: <http://www.folhavitoria.com.br/politica/noticia/2015/02/planalto-decide-ignorar-denuncia-de-que-dilma-continua-sendo-espionada.html>. Acesso em: 7 fev. 2015.

mais causas, e que pode impactar de diferentes formas na realidade presente. As condições de risco devem ser observadas como de significativo impacto ao risco[49]. Trata-se de um evento possível, futuro e incerto.

Destarte, o risco cibernético é um evento ou condição relacionado com redes de meios informáticos, que se ocorre provoca um efeito que pode impactar na realidade de forma significativa. O estudo foca no risco que pode trazer prejuízos aos usuários de redes de computadores ou para a sociedade, representada ou não por meio de suas instituições.

O presente capítulo tem por finalidade identificar os riscos introduzidos no contexto social em virtude da ampliação do uso de ferramentas conectadas à rede de computadores.

## 1.1 Riscos estratégicos: ameaça à segurança do Estado

Em face dos possíveis alvos de ataques cibernéticos, há que se destacar que os governos dos dias de hoje possuem diversas estruturas conectadas à rede mundial de computadores[50], das quais depende a própria existência do Estado, tais como: defesa, segurança pública, sistemas de energia, administração da justiça e infraestrutura de transportes[51]. Os riscos estratégicos refletem vulnerabilidades do país, em nível macro, relacionadas ao bem-estar social, ao cotidiano da coletividade, à qualidade de vida dos cidadãos ou até mesmo à segurança do Estado.

Um dos riscos estratégicos é o terrorismo. Quarenta e cinco dias após o ataque às torres do World Trade Center na cidade de Nova Iorque, em 11 de setembro de 2001, o congresso dos Estados Unidos aprovou o chamado Ato Patriótico (*Patriotic Act,* posteriormente substituído pelo *Freedom Act*): norma que mitigou restrições legais e permitiu que mecanismos de vigilância considerados até então ilegais (inclusive vigilância em massa) pudessem ser legalmente utilizados. A motivação da referida

---

[49] PMI. *Um guia do conhecimento em gerenciamento de projetos*: Guia PMBOK - Project Management Body of Knowledge, 5a edição. São Paulo: Ed. Saraiva, 2014.
[50] CRUZ JÚNIOR, Samuel César da. *Tecnologias e riscos*: armas cibernéticas. Brasília: IPEA, 2013.
[51] MANDARINO JUNIOR, Raphael; CANONGIA, Claudia. *Segurança cibernética*: o desafio da nova sociedade da informação. Disponível em: <http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/349/342>. Acesso em: 14 jan. 2016.

aprovação foi o enfrentamento contra o terrorismo,[52] afinal o terrorismo é um risco estratégico para o Estado como um todo.

Com o passar do tempo, a norma de combate ao terrorismo foi ficando mais permissiva no que diz respeito à vigilância. Recordando as palavras de Sun-Tzu, para quem conhecimento é poder, nota-se que esta foi uma das formas de poder eleita para combater o terror, na busca pela manutenção do Estado de Direito.

Chamadas de voz, e-mails, redes sociais, buscas na internet: quase todas as formas de comunicação que a tecnologia permite foram se tornando alvo potencial de investigações por parte das agências de inteligência estadunidenses, tudo na forma da Lei[53]. O enfoque dado ao exemplo dos estadunidenses se deve aos indícios dessas práticas publicados nos meios de comunicação de massa, o que não significa que outros países se furtem de empregar técnicas semelhantes, como se constatará no decorrer deste trabalho.

Hoje já se admite que as tecnologias de interceptação de celulares já foram globalizadas e "democratizadas"; e uma interceptação ativa pode ser realizada com custo relativamente baixo.[54] A realidade posta evidencia que muitos podem utilizar tais tecnologias. Frise-se que um celular compõe uma rede informatizada e pode ser instrumento de redes cibernéticas.

A práxis da NSA de espionagem eletrônica foi, em parte, descrita por Edward Snowden: invasão e acompanhamento de meios eletrônicos, entrada pela "porta dos fundos" de grandes portais de internet, sob o pretexto de prover segurança. Ainda é colocado em dúvida se a espionagem acontece com ou sem anuência das grandes corporações que atuam na rede[55].

A quarta emenda à Constituição americana protege o cidadão estadunidense de qualquer tipo de investigação sobre sua vida privada sem a devida autorização

---

[52] REIS, Solange, et al. *Entre Aspas*: Privacidade na rede. GLOBONEWS. Exibido em: 11 jun. 2013.
[53] Ibidem.
[54] SOGHOIAN, Christopher; PELL, Stephanie K. *Your secret stingray's no secret anymore: the vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy*. In: Harvard Journal of Law & Technology Volume 28, Number 1 Fall 2014. Disponível em: <http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech1.pdf>. Acesso em: 14 jan. 2016.
[55] Ibidem.

judicial[56]. Paira a dúvida da sociedade estadunidense sobre os limites desta garantia praticados pelas agências de inteligência, o que se pode constatar por meio da veiculação de amplos debates na mídia daquele país, inclusive fomentados por meio de documentários como "*Terms and Conditions May Apply*".

Em 2015, o governo francês, sob o pretexto de combate ao terrorismo, aprovou com ampla maioria dos representantes do povo, uma lei que permite a espionagem telefônica e na internet de qualquer cidadão suspeito de terrorismo, sem autorização judicial. A norma francesa permite ainda a interceptação de mensagens de texto e o uso de *softwares* espiões[57]. Porém, em dezembro de 2014, o Primeiro-ministro francês havia afirmado que a proteção das informações dos usuários da internet deveria ser uma prioridade[58].

Percebe-se que a necessidade de segurança vem servindo de argumento para se relativizar direitos e garantias individuais em sociedades que foram vítimas de ataques terroristas. Pode-se dizer que esta relativização ocorre ainda que sejam necessárias alterações do ordenamento jurídico nacional. Simplesmente, pratica-se tal relativização aprovando-se uma lei mais permissiva com os direitos até então tutelados pelo Estado.

Depois do atentado aos cartunistas de Paris em 2015, esta tendência tende a aumentar, como já é constatado na França. Segundo o governo francês, até 2017, cerca de três mil pessoas serão contratadas para os serviços secretos de segurança e de justiça franceses. Outras três mil devem ser vigiadas por ligações com terroristas de forma mais

---

[56] EMENDA IV da Constituição estadunidense: O direito do povo à inviolabilidade de suas pessoas, casas, papéis e haveres contra busca e apreensão arbitrárias não poderá ser infringido; e nenhum mandado será expedido a não ser mediante indícios de culpabilidade confirmados por juramento ou declaração, e particularmente com a descrição do local da busca e a indicação das pessoas ou coisas a serem apreendidas. (Constituição americana [traduzida])

[57] Portal G1. *Aprovação de lei contra terrorismo gera polêmica na França*. Disponível em: <http://g1.globo.com/jornal-nacional/noticia/2015/05/aprovacao-de-lei-contra-terrorismo-gera-polemica-na-franca.html>. Acesso em: 10 mai. 2015.

[58] GARCIA, Gabriel. *França quer fortalecer privacidade na rede para ´equilibrar forças´*. Disponível em: <http://info.abril.com.br/noticias/internet/2014/12/franca-quer-fortalecer-privacidade-na-rede-para-equilibrar-forcas.shtml>. Acesso em: 10 maio 2015.

efetiva[59]. Segundo o canal de notícias norte americano CNN, os membros das forças de segurança da França foram orientados a apagar seus perfis nas redes sociais[60].

Os Estados também podem se tornar ameaças uns com relação aos outros. Contra os EUA, como também contra britânicos, existem indícios da provável espionagem eletrônica chinesa: conhecida por *Titan Rain*, a suposta espionagem eletrônica teria sido realizada entre os anos de 2003 e 2007. Os estadunidenses só teriam detectado falha em sua segurança em 2004. Há quem cogite haver uma "guerra fria" no ciberespaço. Um pouco mais amenos foram os ataques cibernéticos da Estônia, em 2007. Naquele país, provavelmente por obra de russos, por três semanas não houve como se utilizar do sistema bancário, meios de comunicações tradicionais, internet[61]. O rol ora apresentado, meramente ilustrativo, bem como outros casos parecidos, costumam ser negados pelos supostos atacantes.

Os riscos evidenciados por Edward Snowden também merecem análise. Segundo ele, a NSA deveria coletar informação de inteligência apenas de alvos estrangeiros por meio de operações de SIGINT[62], mas na prática estava coletando metadados de milhões de norte-americanos – registros telefônicos, informações de *e-mails* etc –, tudo sem autorização. A partir destas informações, era possível analisar a vida de pessoas, inclusive acessando dados íntimos, como redes de amigos, romances, hábitos, preferências[63]. Frise-se que o *Freedom Act* pretende, em regra, preservar

---

[59] PELAJO, Christiane. *Governo da França anuncia medidas de combate ao terrorismo no país*. Jornal da Globo. Edição do dia 21 jan. 2015. Disponível em: <http://g1.globo.com/jornal-da-globo/noticia/2015/01/governo-da-franca-anuncia-medidas-de-combate-ao-terrorismo-no-pais.html>. Acesso em 07 fev. 2015.

[60] BERCITO, Diogo. *França reforça segurança contra terrorismo*. Portal Folha. Disponível em: <http://www1.folha.uol.com.br/mundo/2015/01/1573518-franca-reforca-seguranca-contra-terrorismo.shtml>. Acesso em: 08 fev. 2015.

[61] IV SIMPÓSIO DE PÓS-GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS DO PROGRAMA "SAN TIAGO DANTAS" (UNESP, UNICAMP E PUC/SP). *Anais*. Disponível em: <http://www.santiagodantassp.locaweb.com.br/novo/images/simposio/artigos2013/gabriela_sandroni.pdf>. Acesso em: 14 jan. 2016.

[62] Os "alvos" estrangeiros a serem monitorados por meio de SIGINT (acrônimo do termo em inglês *signals intelligence*) podem ser classificados como pessoas potencialmente ameaçadoras a ponto de justificar a observação e coleta de dados pelo Estado por meio da inteligência de sinais (interceptação de sinais de comunicações). A SIGINT é hoje uma "nova tendência" da inteligência.

[63] HARDING, Luke. *Os Arquivos de Snowden*. Trad. Bruno Correia e Alice Klesck. Rio de Janeiro: LeYa, 2014. p. 14.

cidadãos estadunidenses de uma praxe de espionagem em massa que vinha sendo praticada durante a vigência do *Patriotic Act*[64].

A NSA teria ligado secretamente, com ajuda de outro órgão (GCHQ[65]), interceptadores de dados aos cabos de fibra ótica submarinos que circundam o globo. Isto para que Estados Unidos e Reino Unido tivessem acesso a maior parte das comunicações mundiais. O que Snowden chamou de "Tribunais Secretos" convenciam empresas de telecomunicações[66] e afins a entregar seus dados. Estariam envolvidos Google, Microsoft, Facebook, Apple. Segundo evidências, a NSA tinha acesso direto aos servidores das gigantes da tecnologia, dando a si mesma poderes de vigilância sem precedentes[67].

O fato narrado evidencia ainda a necessidade do cuidado que se deve tomar com a arquitetura física das redes informáticas utilizadas pela comunidade a ser protegida. Deve-se aliar a vigilância virtual à vigilância física das estruturas por onde trafegam os dados.

Em 2011, um analista da NSA teria preparado uma apresentação ultrassecreta onde descrevia usuários dos celulares modelo iPhone, da marca Apple, como zumbis: seriam consumidores pagantes que, por possuírem tais aparelhos, passavam dados como a própria geolocalização, financiando a espionagem de si mesmos e de seus próximos. A apresentação foi publicada na revista alemã *Der Spiegel*. Além dos aparelhos da Apple, a NSA mobilizou ainda equipes para trabalhar com Android, BlackBerry, Facebook, Google Earth e Yahoo Messenger. Ressalta-se que dados de geolocalização são especialmente úteis para a espionagem, pois são excelentes fontes para análise de inteligência[68].

A posse de tais dados pelo Estado pode ensejar proteção contra criminosos, no entanto, também materializa potencial ameaça contra pessoas bem-intencionadas, das

---

[64] CONDRON, Sean M. Getting it right: protecting american critical infrastructure in cyberspace. *In:* Harvard Journal of Law & Technology Volume 20, Number 2 Spring 2007. Disponível em: <http://jolt.law.harvard.edu/articles/pdf/v20/20HarvJLTech403.pdf>. Acesso em: 14 jan. 2016.

[65] Agência de Inteligência britânica similar a NSA estadunidense. Para mais informações, acessar <http://www.gchq.gov.uk/Pages/homepage.aspx> (sítio em inglês).

[66] AT&T, maior empresa de telefonia celular estadunidense, reserva-se ao direito de se utilizar de dados pessoais em algumas situações como prevenção contra descumprimentos legais em seus termos de serviço.

[67] HARDING, Luke. *Os Arquivos de Snowden*. Trad. Bruno Correia e Alice Klesck. Rio de Janeiro: LeYa, 2014. p. 14.

[68] Ibidem, p. 162.

quais os dados são coletados. Há sempre um risco que pode ser potencialmente excessivo de tais informações serem mal utilizadas.

A eventual ilegalidade de tais coletas sem mandado judicial passa a ser mais um ponto no debate. Tais dados alimentam um *software* de análise que rastreia terroristas estrangeiros fora do território dos EUA. Juízes federais estadunidenses aprovaram o *software* que supostamente espiona somente estrangeiros. São analisados dados informáticos, chamadas telefônicas, vídeos, voz etc. Ao longo da última década, os EUA vinham trabalhando para reunir praticamente todas as informações que entram e saem daquele país[69].

Assim, os atos praticados pela NSA, aparentemente violam a Constituição estadunidense e o direito à privacidade consolidado nos EUA, pois a permissão legal não engloba a espionagem irrestrita de estadunidenses. Para os mais conscientes que tentam se proteger, a NSA teria colocado *backdoors*[70] secretas em *softwares* de criptografia *on line*, enfraquecendo a segurança, inclusive, de transações bancárias[71].

O objetivo final da NSA[72] seria coletar tudo de todos, em todos os lugares e armazenar indefinidamente[73]. Quanto à privacidade, é certo que a posse de tais dados que relativizam a privacidade poderia proteger a sociedade como um todo, se bem utilizados. Levanta-se a dúvida sobre o que um grupo mal-intencionado poderia fazer com a análise destes dados.

A quarta emenda à Constituição estadunidense proíbe buscas e apreensões não justificadas contra cidadãos estadunidenses[74]. Interceptações de comunicações dependem de "suspeito específico" e de "causa provável", como condição de emissão de mandado judicial permissivo[75]. Na década de 1970, o presidente estadunidense

---

[69] HARDING, Luke. *Os Arquivos de Snowden*. Trad. Bruno Correia e Alice Klesck. Rio de Janeiro: LeYa, 2014. p. 161-166.

[70] Vírus, *backdoors*, *trojans*, *spywares* são pragas virtuais que podem ser entendidas por um leigo como armadilhas que vão fazer com que o(s) usuário(s) do equipamento infectado seja(m) levado(s) a algum prejuízo inesperado por ocasionarem atividades indesejadas no computador.

[71] HARDING, Luke. op. cit. p. 14.

[72] BAUMAN, Zygmunt. *Após Snowden*: Repensando o Impacto da Vigilância. Disponível em: <https://revistas.ufrj.br/index.php/eco_pos/article/view/2660/2225>. Acesso em: 14 jan. 2016.

[73] HARDING, Luke. op. cit. p. 14.

[74] HERMAN, SUSAN N. *Os desafios do crime cibernético*. Disponível em: <http://www.seer.ufrgs.br/index.php/redppc/article/view/46105/28721>. Acesso em: 08 jan. 2016.

[75] VERVAELE, JOHN A. E. A legislação anti-terrorista nos estados unidos: um direito penal do inimigo? Disponível em: <http://www.seer.ufrgs.br/index.php/redppc/article/view/52029/32055>. Acesso em: 08 jan. 2016.

Nixon ordenou que a NSA grampeasse telefones de compatriotas com os quais não simpatizava. A trama se tornou pública e deu origem à Lei de Vigilância de Inteligência Estrangeira, de 1978, segundo a qual a NSA não poderia monitorar comunicações que envolvessem estadunidenses, salvo com permissão em mandado judicial. No caso do GCHQ – o parceiro britânico da NSA[76] – o Regulamento de Atos de Poderes Investigatórios de 2000 foi interpretado de forma a oferecer para o GCHQ carta branca para vigilância em massa, podendo passar os resultados para a NSA, contanto que uma das partes interceptadas estivesse no exterior. Isto tudo antes do atentado de 11 de setembro de 2001 em Nova Iorque[77].

Um mapa de conexões entre pessoas, conhecido por "gráfico social", só era ilegal se envolvesse estadunidenses. Tais mapas são utilizados como ferramentas de análise de inteligência.

Sob o amparo do *Patriotic Act*, a NSA desencadeou um programa com quatro alvos operacionais: comunicações, metadados telefônicos, comunicações informáticas e metadados da internet. A intenção era de coletar a maior quantidade possível de dados. Bastasse que os dados passassem nos Estados Unidos para que fossem coletados. O codinome do programa foi "Stellar Wind", assim batizado em 4 de outubro de 2001. Oitenta e um por cento das chamadas internacionais em trânsito pelos EUA teriam sido interceptadas. É interessante saber que dados que transitam de um ponto a outro na internet, independente de origem e destino, podem passar, naturalmente, pelo território dos Estados Unidos[78].

Em dezembro de 2005, a primeira página do jornal americano *The New York Times* trazia como manchete que George W. Bush, então presidente dos EUA, permitiu que agências do governo daquele Estado espionassem telefones sem autorização judicial. Era focada, a espionagem, apenas nas interceptações de chamadas telefônicas internacionais e tráfego de e-mails de cidadãos estadunidenses. O Governo dos EUA

[76] LYON, David. *As apostas de Snowden:* desafios para entendimento de vigilância hoje. Disponível em: <http://www.seer.ufrgs.br/index.php/redppc/article/view/52029/32055>. Acesso em: 08 jan. 2016.
[77] HARDING, Luke. *Os Arquivos de Snowden*. Trad. Bruno Correia e Alice Klesck. Rio de Janeiro: LeYa, 2014. p. 75-77.
[78] Ibidem. p. 76-77.

realizou varredura de *e-mails*, faxes, chamadas telefônicas, dados transacionais – coletados aos bilhões[79].

Snowden explicou que a agência NSA era capaz de transformar um celular em um microfone e dispositivo de rastreamento, e deu a entender que nada na internet tradicional seria seguro. Snowden solicitou, num primeiro momento, que seu interlocutor jornalista utilizasse para a comunicação entre eles apenas a rede TOR, disponível apenas na *deep web*, o que postergaria as denúncias contra si[80].

Edward Snowden descreveu, ainda, o que seria a Diretiva 20: um documento de diretriz política com alto grau de sigilo, de 18 páginas, datado de outubro de 2012, por meio do qual o chefe do executivo estadunidense, Barack Obama, teria pedido aos funcionários seniores da inteligência que elaborassem uma lista de potenciais alvos para ataques cibernéticos no exterior. Não se fala aqui de defesa, mas de ataque, no contexto do pugilato cibernético.

Outro risco está relacionado ao sentimento de coação pela consciência da vigilância. Um relatório estudado pelo jornalista Greenwald[81], conclui que um número considerável de autores parte do pressuposto de que suas comunicações estão sendo monitoradas, mudando comportamentos[82]. A consciência da vigilância pode contribuir, por si só, para a mudança de opiniões pessoais que são publicadas, verdadeiro risco à democracia pela sensação de coação.

No que tange aos riscos contra o Estado e sua economia, pode-se citar como exemplo o narrado por Greenwald sobre o programa canadense OLYMPIA[83], que se destina a vigiar as ações do Ministério das Minas e Energia brasileiro. Documentos deixaram claro que, além de terroristas (alvos relacionados à segurança nacional), a NSA praticou espionagem econômica e diplomática. Nesse aspecto, a NSA, segundo

---

[79] HARDING, Luke. *Os Arquivos de Snowden*. Trad. Bruno Correia e Alice Klesck. Rio de Janeiro: LeYa, 2014. p. 79-89.
[80] Ibidem. p. 68-90.
[81] Relatório *Efeitos Arrepiantes: vigilância da NSA leva escritores americanos à autocensura*, publicado pela fundação PEN American Center em novembro de 2013. (título traduzido do inglês)
[82] GREENWALD, Glenn. *Sem Lugar para se esconder*. Trad. Fernanda Abreu. Rio de Janeiro: Sextante, 2014. p. 190 -191
[83] SCHELL, Bernadette H. *Internet censorship*: a reference handbook. Oxford: ABC-CLIO, 2014. p. 14.

Glenn, se dedica a uma única missão maior: evitar que qualquer comunicação eletrônica, por mais ínfima, fuja do seu alcance sistemático[84].

Deve-se meditar sobre o risco à segurança nacional imposto pelo terrorismo, mas não se pode olvidar do risco destas informações pararem em qualquer lugar, o que poderia ser tão grave quanto os riscos do terrorismo, a depender das circunstâncias. Apenas para ilustrar essa preocupação, pode-se citar que os dados de contribuintes vazaram da Receita Federal do Brasil e chegaram a ser vendidos em mídias por "camelôs" na cidade de São Paulo, causando desde pequenos inconvenientes até grandes tragédias pessoais.

A fim de evitar episódios de ataque cibernético que alcancem também os dados de instituições norte americanas, em fevereiro de 2015, o presidente estadunidense Barack Obama, deslocou-se para a Califórnia com a finalidade de discutir segurança cibernética. O objetivo do chefe do executivo estadunidense era que as empresas de tecnologia compartilhassem mais informações com as autoridades em nome da segurança do país. Em contraponto, existe a intenção, por parte de algumas empresas e por parcela da população, de que a privacidade seja protegida, o que tem sido considerado um obstáculo para o governo dos EUA[85]. O presidente americano já havia, em janeiro de 2015, uma semana após ataques feitos pelo Estado Islâmico ao Pentágono, anunciado medidas para conter ataques virtuais[86].

Já foram citados na introdução os riscos decorrentes de projetos e programas de espionagem específicos, a exemplo do Projeto Echelon[87], quando se fez referência à filosofia da interceptação[88] evidenciada por Boatti e Tavarolli.

Impulsionada pelos atentados terroristas em Paris, a norma jurídica francesa relacionada à possibilidade de espionagem por parte do Estado foi aprovada pela

---

[84] GREENWALD, Glenn. *Sem Lugar para se esconder*. Trad. Fernanda Abreu. Rio de Janeiro: Sextante, 2014. p. 190 -191.

[85] SEVERIANO, Alan. *Obama faz vídeo para incentivar cadastramento no programa de saúde.* Jornal Hoje. Disponível em: <http://glo.bo/1F63APa> Acesso em: 13 fev. 2015.

[86] SOTO, Cesar. *O mundo contra os Hackers*. In: Revista ISTOÉ. ed. 21 Jan 2015, nº2355. São Paulo: Três, 2015. p. 65.

[87] LAWNER, Kevin J. *Post-Sept. 11th international surveillance activity*: a failure of intelligence: the echelon interception system & (and) the fundamental right to privacy in Europe. Disponível em: <http://heinonline.org/HOL/LandingPage?handle=hein.journals/pacinlwr14&div=22&id=&page=>. Acesso em: 07 fev. 2016.

[88] Para mais informações sobre a filosofia das interceptações: BOATTI, Giorgio. e TAVAROLI, Giuliano. *SPIE*: *I Servizi Segreti delle Multinazionali*: dossier, intercettazioni, guerre informatiche. Mondadori, Milano: 2008, p. 196 e ss.

Câmara daquele país em 2015. Tal norma oferece amplos poderes ao Estado francês para espionar[89]. Trata-se de uma regra comparável ao *Patriot Act* estadunidense. De acordo com o projeto de Lei aprovado, é possível interceptar de forma quase ilimitada comunicações e dados (inclusive em massa), aumentando a vigilância do Estado francês contra o terrorismo[90].

Ressalte-se que em nada a legislação brasileira impacta nas decisões de países estrangeiros em vigiar desmedidamente. A norma brasileira não é suficiente para proteger pessoas em território nacional de uma decisão política estrangeira como esta, que permite a coleta de informações, independentemente da presença física de agentes de outro Estado em solo brasileiro.

Os críticos dizem, dentre outros argumentos, que a referida lei francesa centraliza o poder de vigilância nas mãos de pouquíssimas pessoas. O atual presidente da Ordem dos Advogados de Paris, Pierre-Olivier Sur, argumenta que:

> Não podemos aceitar uma lei que, eminentemente, autoriza a criação de sistemas que não só localizam pessoas, veículos ou objetos em tempo real, mas que também capturam dados pessoais baseados no que os elaboradores da lei chamam, vagamente de importantes interesses de política externa, interesses industriais, científicos e econômicos da França, prevenção da violência coletiva ou prevenção do crime e do crime organizado.[91]

O fato é que a lei foi aprovada por relevante maioria de votos: 438 contra 86. Em poucas oportunidades durante os três primeiros anos de seu mandato, François Hollande, presidente francês, gozou de ampla maioria no parlamento francês como nesta votação[92].

Todavia, nem todos estão conscientes dos riscos contra a privacidade dos cidadãos, suas famílias e suas empresas.

---

[89] PORTAL O GLOBO. *Câmara francesa aprova lei de inteligência que libera espionagem ilimitada nas comunicações*: ed de 05/05/2015. Disponível em: <http://oglobo.globo.com/mundo/camara-francesa-aprova-lei-de-inteligencia-que-libera-espionagem-ilimitada-nas-comunicacoes-16062176>. Acesso em: 07 maio 2015.

[90] KERN, Soeren. *O Parlamento Francês Aprova Lei Abrangente de Espionagem de Dados*. 6 de Maio de 2015. Trad.: Joseph Skilnik. Disponível em: <http://pt.gatestoneinstitute.org/5715/franca-lei-espionagem>. Acesso em: 07 maio 2015.

[91] Ibidem

[92] RIBEIRO, Gustavo. *A França e o direito de espionar*. Disponível em: <http://jota.info/a-franca-e-o-direito-de-espionar>. Acesso em: 09 maio 2015.

## 1.2 Riscos individuais: ameaça de privação de serviços públicos e de direitos fundamentais

Direitos individuais podem ser ameaçados por pessoas comuns, Estados, empresas, grupos terroristas e outros criminosos. Quando se trata de crime, remete-se a bens jurídicos caros para a comunidade. As ameaças aos direitos individuais podem ter origens diversas, incluindo aí o ambiente cibernético. Menezes e Assunção[93] citam tentativas legais e jurisprudenciais de que sejam evitadas tais ameaças, como a Constituição da República em seu art. 5º , X, XII e LX; a Lei de Imprensa[94] (Lei nº 5.250, de 9 de fevereiro de 1967); a Lei da Política Nacional da Informática (Lei nº 7.232, de 29 de outubro de 1984); o novel Código Civil, ao tratar dos direitos da personalidade; o marco civil da Internet (Lei nº 12.965, de 23 de abril de 2014); REsp 1.335.153-RJ e REsp 1.334.097-RJ, Rel. Min. Luis Felipe Salomão, julgados em 28 de maio de 2013. A legislação nacional é, por vezes, redundante em proteger tais direitos.

Os riscos podem ser relativizados pela sociedade organizada, mas o engajamento social pode reduzi-los de forma relevante. Dentre os riscos individuais mais evidentes, pode-se citar o risco à privacidade, intimidade, negação de serviços públicos disponibilizados para servir diretamente ao cidadão, dentre os quais o risco de fraude em votações realizadas apenas por meios informáticos.

Não é por acaso que países desenvolvidos não têm adotado o voto eletrônico para eleger representantes. O uso de meios informáticos em eleições pode configurar risco para o indivíduo, para o Estado e para as instituições.

Glenn Greenwald, o jornalista que teve acesso aos dados de Snowden, declarou-se surpreso pelo tamanho e pela abrangência dos dados da vigilância secreta norte-americana, com sistemas implementados quase sem prestação de contas, transparência ou limite. Foram alvo de vigilância em massa e indiscriminada, inclusive países aliados

---

[93] MENEZES, Rafael da Silva; ASSUNÇÃO, Linara Oeiras. *Os contornos jurídicos da proteção à privacidade no marco civil da internet.* In: Governança das Redes e o Marco Civil da Internet: Liberdades, Privacidade e Democracia. Organizadores: Fabrício Bertini Pasquot Polido e Mônica Steffen Guise Rosina. Belo Horizonte: UFMG, 2015. p. 146-150

[94] O Supremo Tribunal Federal, por meio da ADPF 130, julgou a Lei de Imprensa incompatível com a Constituição Federal de 1988. O Ministro Carlos Ayres Britto, então relator, votou pela incompatibilidade total da Lei de Imprensa com a atual ordem constitucional. Na oportunidade o Ministro considerou a liberdade de imprensa irmã siamesa da democracia. Salientou ainda que a imprensa não pode sofrer antecipado controle nem mesmo por força do Direito-Lei; não havendo espaço constitucional para que o Estado adentre em matérias que são da essência da liberdade de imprensa.

dos Estados Unidos. O jornalista descreveu a vigilância de satélites, e relatou que, no período de um mês, uma única unidade da NSA havia coletado, em um único sistema, dados sobre mais de três bilhões de chamadas telefônicas realizadas por meio da internet, além de *e-mails*. Em apenas 30 dias, em todas as ferramentas, aquela unidade coletou 2,3 bilhões de dados de e-mails e chamadas somente do Brasil[95].

Segundo Greenwald, governos do mundo têm se esforçado para adestrar seus cidadãos a desdenhar da própria privacidade, convencendo pela tolerância às invasões ao universo privado. Os defensores da vigilância abordados pelo jornalista opinaram que a privacidade é para quem tem algo a esconder. Apesar disso, nenhum deles se dispôs a entregar a senha de seu *e-mail*. Da mesma forma, na oportunidade em que a presidente do Comitê de Inteligência do Senado estadunidense, Dianne Feinstein, discorreu que a coleta de dados da NSA não configurava vigilância, uma vez que não inclui o conteúdo de nenhuma comunicação, usuários da internet peticionaram para que ela respaldasse sua afirmação com atos, publicando uma vez por mês uma lista completa das pessoas com quem havia trocado *e-mails* e telefonemas, especificando a duração das chamadas e a sua localização física e de seus interlocutores. Obviamente, tais pedidos não foram atendidos[96]. Ao que parece, aqueles que mitigam a privacidade alheia não estão muito dispostos a abrir mão da própria privacidade.

Podem ser citados como motivações para que órgãos governamentais vigiem as pessoas por meio de redes informáticas, atenuando sobremaneira a privacidade: o agravamento das desigualdades sociais, o terrorismo, tensões entre Estados, espionagem sobre tecnologias, estudo de ambiente político, autodefesa, planejamento para ataques de toda forma (inclusive não bélicos), controle sobre qualquer forma de instabilidade, fortalecimento de poder, dentre outros.

Sabe-se que há situações em que pessoas se expõem voluntariamente por meio da internet, limitando sua privacidade em algum grau. Um exemplo disso é o caso do primeiro-ministro canadense, Stephen Harper: a imprensa canadense divulgou que Harper seguia Homer Simpson, personagem de desenho animado, no *Twitter*. Logo após a divulgação das contas que seguia, o primeiro-ministro deixou de seguir o

[95] GREENWALD, Glenn. *Sem Lugar para se esconder*. Trad. Fernanda Abreu. Rio de Janeiro: Sextante, 2014. p. 97-99.
[96] Ibidem. p. 183-185.

personagem[97]. Esta exposição é considerada voluntária, já que está disponível a qualquer um que acesse a rede, e só ocorre porque o próprio usuário decidiu tornar a informação pública. Quando alguém divulga qualquer informação na rede, sujeita-se a alguns riscos, dentre os quais o de ter a informação amplamente divulgada, inclusive fora da internet. Esses casos de auto exposição são considerados menos relevantes para este estudo, visto que aí a limitação à privacidade decorre de um ato voluntário do indivíduo que torna pública uma informação a seu respeito.

Em contraponto, alguns que utilizam a rede de computadores têm maior preocupação com privacidade. São pessoas que não querem ter suas contas de *e-mail* invadidas e seus documentos pessoais divulgados. A despeito de eventuais cuidados do usuário, as novas tecnologias tornam cada vez mais difícil a tarefa de manter dados pessoais em sigilo.

Os avanços tecnológicos cada vez mais se incorporam ao dia-a-dia das pessoas. Com a popularização de determinada tecnologia, as facilidades que ela possibilita se tornam parte da vida dos usuários. Os *smartphones* são ótimos exemplos disso, facilitando de forma evidente a vida de seus usuários. As pessoas, conhecendo ou ignorando os riscos, acabam a eles se sujeitando em troca das facilidades que proporcionam: um mesmo aparelho serve para fazer e receber ligações, enviar mensagens de texto, acessar redes sociais, tirar fotos, enviar e receber diversos tipos de arquivos, acessar *e-mails*, auxiliar no deslocamento por uma cidade desconhecida, fugir de congestionamentos, controlar a dieta ou as finanças, entreter-se com jogos, armazenar músicas, servir como calculadora etc.

Por essas e outras tantas funcionalidades, os *smartphones* se tornaram o grande símbolo de uma época em que os indivíduos sentem necessidade de estar conectados todo o tempo e de resolver diversos problemas usando um único dispositivo. Toda essa comodidade, porém, depende do uso de dados do usuário, que tem como característica marcante a conectividade plena.

É comum, atualmente, que pais presenteiem seus filhos com *smartphones* que possuem tecnologia de geolocalização. Por meio de *softwares*, os pais podem saber

[97]APF. *Primeiro-ministro canadense deixa de seguir Homer Simpson no Twitter.* Disponível em: <http://noticias.br.msn.com/primeiro-ministro-canadense-deixa-de-seguir-homer-simpson-no-twitter-1>, consultado em 26 jun.14.

exatamente a localização dos telefones de seus filhos. É provável que a intenção principal dos pais controladores ao escolher o presente seja a de vigiar seus filhos, sabendo quais locais eles frequentam. O intuito de vigiar pode ser proteger, mas, ainda assim, vigiar. Situação diferente é aquela em que o marido ciumento presenteia sua esposa com o mesmo moderno e funcional *smartphone*. Talvez ele também queira vigiar. O presente, a despeito de útil, certamente diminui a privacidade do usuário vigiado por meio da rede. Se o cônjuge souber a motivação do presente, quem sabe o rejeite. Não seria uma hipótese inesperada.

Entretanto, como já se argumentou, os pais controladores e os cônjuges ciumentos não são os únicos que se interessam pelos dados que podem ser transmitidos por *smartphones*: alguns governos (para que se fale somente deles) podem monitorar todos os dados registrados por um *smartphone*, o que inclui dados privados, como trocas de mensagens. Isso e muito mais pode ser captado a partir de um *smartphone*.

Ao mesmo tempo, este verdadeiro aparelho espião costuma facilitar o comércio, diversão, viagens e investimentos. São tantos os benefícios para os usuários que boa parcela destes assume os riscos de utilizá-lo para colher seus bons frutos.

Apenas como ilustração, quando se "crackeia" um *software* para que se possa utilizá-lo sem pagar por ele, assumem-se vulnerabilidades em sistemas informáticos que podem potencializar todo o mal que se contrapõe à privacidade própria. Se utilizar um produto registrado já pode representar alto risco de invasão à privacidade por meios informáticos, imagine-se o risco que pode vir de um software feito por um desconhecido que sabe informática o suficiente para "crackear" um programa. Isso ocorre porque os sistemas podem ser manipulados a fim de que seja possível a coleta de dados de interesse com o envio pela rede mundial de computadores.

Outro risco que se assemelha com o risco à privacidade é o risco da negação de serviços, com tendência a maior vulnerabilidade os públicos, consoante a essencialidade de cada serviço. A vulnerabilidade das redes de computadores pode impactar no dia-a-dia de muitos brasileiros, inclusive dos que não utilizam redes de computadores diretamente. De alguma forma, mesmo comunidades situadas nos mais distantes rincões do Brasil sofrem influência de máquinas ligadas em rede: se, no momento em que necessitam de um serviço, a rede não está em funcionamento adequado, podem ficar sem atendimento médico, sem energia elétrica, sem o apoio oportuno que poderia até

salvar vidas. Grande parte dos serviços públicos disponibilizados são controlados por redes de computadores, inclusive serviços críticos como geração de energia, tratamento e distribuição de água, serviços de transporte, dentre outros.

Um risco relevante está relacionado com as ameaças a direitos individuais por parte de grandes corporações de telecomunicações, como o Google. Para entendê-las, deve-se ter em mente que todo produto ou serviço oferecido "graciosamente" tem que ser financiado por alguém[98]. Outro ponto a ser destacado: normalmente, investimentos visam o lucro.

Ron Ploof[99] afirma que o Facebook tomou decisões de muita relevância no âmbito da privacidade[100], induzindo o pensamento de que teriam sido decisões tomadas por adolescentes com pouca maturidade. Segundo Sánchez-Ocaña, o Facebook tem acesso a determinados dados que o Google não pode escanear e nem obter[101].

Tal informação é de grande relevância, pois uma das vantagens competitivas do Google foi, por muito tempo, ser aquele que melhor conhecia os usuários, podendo prever, portanto, sua conduta. O Facebook, por sua vez, só pela análise do botão "curtir", pode analisar preferências dos usuários, oferecendo publicidade ainda mais direcionada[102]. Trata-se de concorrência ameaçadora.

Pela análise destes dados, percebe-se que uma das fontes de lucro destas corporações é o fato de que conhecem o usuário, e podem, com isso, prever o seu consumo potencial. Naturalmente, para melhor se conhecer o usuário, mais se abranda a privacidade. Uma vez que conhecem as preferências do usuário, as gigantes da internet podem direcionar melhor a publicidade específica para cada perfil. E, quanto mais direcionada a publicidade, mais elas lucram. Sugere-se proceder a seguinte experiência: acessar lojas virtuais a partir de um computador pessoal. Visite produtos específicos. Atente-se que a publicidade ofertada em outras buscas na internet será, muitas vezes, baseada nas últimas visitas em lojas virtuais.

---

[98] SÁNCHEZ-OCAÑA, Alejandro Suárez. *A Verdade por Trás do Google*. Trad. Sandra Martha Dolinsky. São Paulo: Planeta, 2013. p. 139.

[99] Especialista em criação de conteúdos na rede há 27 anos.

[100] A política de privacidade do Facebook inovou, aumentando significativamente o potencial dos resultados da análise de dados realizada pela corporação sobre seus usuários. Para mais detalhes, acessar: <https://www.facebook.com/about/privacy>.

[101] SÁNCHEZ-OCAÑA, Alejandro Suárez. op. cit. p. 140-141.

[102] Ibidem. p. 141.

Pode-se presumir que quem se dispõe a ter uma conta no Facebook abre mão de parte considerável de sua privacidade. Um usuário médio do Facebook expõe hábitos de consumo, hábitos familiares, preferências em geral (cidades, times de futebol, estilo musical, leituras, filmes etc). Por vezes, usuários das redes sociais disponibilizam voluntariamente informações sobre si e seus entes mais próximos que permitem que se chegue a várias conclusões sobre eles e sua rotina. Não raramente a disponibilização de informações pessoais vem acompanhada de fotos ilustrativas e dados de geolocalização que confirmam informações disponibilizadas.

Pedro J. Ramirez, diretor do periódico *El Mundo*, líder dentre os prestadores de informação na Espanha, contou sobre uma experiência própria: sua filha foi estudar no exterior. Na oportunidade em que foi recebido na Universidade, ele conversou com o responsável pelas admissões, e este lhe disse que, durante o processo de seleção, haviam se informado sobre o pai da então candidata por meio da versão inglesa da Wikipedia. Mostraram-lhe informações que, segundo o próprio Ramirez, eram corretas. Assépticas e superficiais, mas corretas. Houve apenas uma exceção, segundo o diretor: no tópico "vida pessoal", dizia que ele vivia uma relação como amante de Rauph Lauren. Pedro explicou que à saída de um evento, Rauph Lauren esperava-o de carro para um passeio na cidade, sob o olhar dos presentes. Em razão do que teria sido um engano, logo foi oferecido o endereço IP do autor daquele "vandalismo informativo". O endereço IP permitiu que se identificasse o autor das informações[103].

O detalhe é que o IP do autor foi ofertado por Larry Page, presidente do Google. É intrigante o fato de que o presidente do Google estava certo de conseguir o endereço eletrônico utilizado em um site alheio ao Google, a Wikipedia. Talvez este seja um indício digno de preocupação, quando se foca na privacidade[104]. Como se não bastasse, Sánchez-Ocaña afirma que o Google almeja o monopólio de acesso à informação, oferecendo-se para coletar mais e mais conteúdo.

Além das buscas em geral, outra ferramenta famosa do Google é o *street view*. Pode-se percorrer todo um bairro sem sair da frente do computador. O *street view* permite visitar virtualmente a frente de todas as casas de uma rua. Para uns, a ferramenta é considerada uma maravilha; para outros, uma ameaça. Inclusive uma

[103] SÁNCHEZ-OCAÑA, Alejandro Suárez. *A Verdade por Trás do Google*. Trad. Sandra Martha Dolinsky. São Paulo: Planeta, 2013. p. 154-158.
[104] Ibidem. p. 157-159.

relevante ameaça à privacidade. Mary Kalin-Casey, moradora de Nova Iorque, ressaltou a inquietude de ter visto pelo *street view* seu gato de estimação, um quadro de sua avó, dentre outros objetos de valor; tudo isso publicado na internet. São imagens colhidas sem prévia autorização por parte das pessoas que nela aparecem, e em situações que podem ter trágicas consequências, inclusive de imagens sujeitas a más interpretações. Quanto a isso, existe uma conhecida imagem de uma mulher urinando na rua, gente com roupa íntima, ruas de prostituição com movimento de pessoas etc.[105]

Em 2010, o Google anunciou que coletou "acidentalmente" dados pessoais, inclusive e-mails com senhas, por intermédio de redes wi-fi abertas (não protegidas por senha) que seus carros acessavam enquanto fotografavam as ruas. No ano seguinte, o Google foi sancionado pelo Estado francês por violar normas de respeito à privacidade. Segundo a Comissão Nacional de Informática e Liberdade (CNIL) francesa, os dados pessoais obtidos sem consentimento incluíam senhas, mensagens de amantes adúlteros, detalhes de operações bancárias *on-line*. Coletaram-se, da mesma forma, dados privados na Irlanda[106]. No Brasil, instrumentos jurídicos de controle efetivo para evitar a manipulação de dados na forma da Lei brasileira, não tem prosperado: o governo federal defendeu que grandes provedores de serviços de internet seriam obrigados a instalar estruturas de processamento de dados no Brasil, contudo a norma que obrigaria tal conduta não avançou no Congresso Nacional. Seria um artigo do Marco Civil da Internet[107]. Mesmo que tivesse sido aprovado, tecnicamente seria de difícil efetividade.

Ainda no que tange à esfera individual, o risco relacionado a novíssimas tecnologias – como a nanotecnologia – também merece destaque, ainda que não se trate de um risco unicamente individual. A nanotecnologia pode quebrar criptografias até então consideradas seguras, potencializando riscos[108]. Trata-se de um risco cibernético relacionado com a velocidade de processamento e que pode impactar de forma contundente no (des)respeito à lei. Essas tecnologias podem tornar vulneráveis chaves criptográficas utilizadas hoje em dia para proteção de dados utilizados comercialmente. Considere-se que todo procedimento bancário, *v.g.*, realizado pela internet, é baseado

---

[105] SÁNCHEZ-OCAÑA, Alejandro Suárez. *A Verdade por Trás do Google*. Trad. Sandra Martha Dolinsky. São Paulo: Planeta, 2013. p. 243.

[106] Ibidem. p. 250-251.

[107] BEZERRA, Arthur C.; WALTZ, Igor. *Privacidade, neutralidade e inimputabilidade da internet no Brasil*. Revista Eptic Online, p.161-175, maio/ago, 2014. v. 16, n. 2. p. 164.

[108] MARTINS, Elaine. *É hora de descobrir os segredos da computação quântica*. Disponível em: <http://www.tecmundo.com.br/computacao-quantica/2666-e-hora-de-descobrir-os-segredos-da-computacao-quantica.htm>. Acesso em: 13 fev. 2015.

em criptografia. Caso a criptografia de uma operação como essa esteja comprometida, muito vulnerável se torna a segurança dos indivíduos da sociedade em rede, até que apareça uma nova tecnologia que a substitua.

Tecnologias chamadas proprietárias, diferentemente de um *software* livre, podem conter o que é conhecido por "bomba lógica": dispositivos que funcionam independente da vontade e conhecimento do usuário, inseridos com o conhecimento do fabricante, mas que podem vulnerabilizar o usuário de alguma forma. A "bomba lógica" pode ser inserida em um aparelho informático ligado à internet para que este envie dados pessoais de tempos em tempos para determinado destinatário. Existem outros nomes pelos quais é conhecida em ambiente virtual, assim como existem outros dispositivos que colocam em risco a segurança do usuário sem o seu conhecimento.

Além dos programas que já vêm nos próprios equipamentos, há programas maliciosos que podem infectar dispositivos informáticos ao instalar softwares, sendo tão maior o risco quanto mais desconhecida for a procedência do que se insere num computador pessoal ou outro dispositivo ligado em rede. Sobre esse assunto, há um julgado do Supremo Tribunal Federal a ser analisado no tópico 3.2 do presente estudo.

Ademais, para Wu, protocolos abertos – como, por vezes oferecido por gigantes como Google e Apple – e suas vantagens de integração, facilitam a fusão de tecnologias de diferentes corporações e o controle de como a humanidade irá partilhar as informações que possuem. Tudo por meio de monopólios da informação, evitando a criação de concorrentes em razão do modelo oferecido[109]. As vantagens de integração facilitam a vigilância da tecnologia fundida por parte das grandes corporações; e os monopólios da forma como se difunde informação podem se mostrar, eventualmente, como mais um grande risco para a comunidade, até por fomentar a não regulação de alguns parâmetros adotados sob pena de inviabilizar, por normas, o trânsito de dados em determinada área jurisdicional. Na prática, em razão dos modelos adotados pela internet, a inviabilidade será apenas legal, como já evidenciado por meio de intervenções jurídicas de grandes companhias de mídia que não conseguem evitar o compartilhamento de mídias das quais são proprietárias. Seus atos apenas evitam parte de tais compartilhamentos não autorizados de, por exemplo, músicas ou filmes.

---

[109] WU, Tim. *Impérios da comunicação*: Do telefone à internet, da AT&T ao Google. Trad. Cláudio Carina. Rio de Janeiro: Zahar, 2012. p. 323-328.

O risco da cessão de dados pessoais para processamento externo com finalidade econômica também assombra. O Google trabalha com dados: financia pesquisas para conhecer os seres humanos de forma pessoal e tão profunda que pretendem, por exemplo, monitorar e combater doenças como o câncer por meio da nanotecnologia[110]. Trata-se de uma verdadeira maravilha da ciência, que pode aumentar a expectativa de vida, prevenir e auxiliar no tratamento de doenças.

Porém, lado-a-lado com as maravilhas da tecnologia, aparecem os riscos decorrentes do seu uso. Com o monitoramento, a entidade acaba coletando informações pessoais preciosas, como se fosse um laboratório ou centro médico. Tais dados nas mãos de quem vive de vender informações potencializa alguns riscos decorrentes do fato de informações personalíssimas serem compartilhadas com terceiros.

Note-se que as informações são coletadas eletronicamente e aparentemente processadas em computador, podendo, então, ser alvo de ataques cibernéticos na hipótese de os dispositivos estarem conectados na rede mundial de computadores.

Aliado ao risco apresentado, deve-se atentar para o fato de que empregadores podem desejar informações sobre quais funcionários devem contratar e quais devem demitir para maximizar os lucros. Em outras palavras, ainda que não se tenha intenção declarada, trata-se de uma hipótese altamente lucrativa explorar dados tão pessoais.

Existem grandes benesses e grandes riscos envolvidos. Ainda que alguém possa se utilizar deste tipo de dados de forma pouco ética, tal levantamento de dados, por outro lado, pode ser muito útil, auxiliando na prevenção de enfermidades e na transformação da sociedade em comunidade no caminho do bem comum.

Talvez um remédio contra a vigilância indesejada seja mais vigilância, vigiando quem nos vigia, relativizando, assim, os riscos. Natural que esta solução careça de regulamentação e de regulação. Tal assertiva foi inspirada numa afirmação do professor Carlos Ayres Britto em exposições por ele proferidas no grupo de pesquisa que coordena no UniCEUB durante a produção deste trabalho, ao lecionar que um remédio para o "excesso" de liberdade na imprensa é mais liberdade.

---

[110] OLHAR DIGITAL. *Google quer entrar no corpo das pessoas usando a nanotecnologia*. Disponível em: <http://olhardigital.uol.com.br/noticia/google-quer-entrar-no-corpo-das-pessoas-usando-nanotecnologia/44909>. Acesso em: 14 fev. 2015.

Os governos podem prestar um serviço de utilidade pública financiando a atenuação dos riscos cibernéticos por meio do investimento no uso da tecnologia disponível para este fim e do investimento em pessoal especializado.

Uma vez que a preocupação recai sobre pontos sensíveis de segurança, vigiar quem vigia a sociedade deve ser implementado de forma compensadora e sem ingerência política. O risco de se ampliar a vigilância na rede pode ser ampliado caso essas atividades sejam controladas por pessoas com cargos políticos. O ideal é que o serviço seja feito por técnicos especializados, a partir de decisões da sociedade. Em casos como este, nos quais pretende-se que não haja ingerência política direta sobre as atividades, a regulamentação de verba independente, com vistas à autossuficiência, é um fator de grande importância.

### 1.3 Riscos para empresas e empreendedores

Os riscos inerentes às sociedades empresárias no ciberespaço são riscos privados que refletem no Estado e no bem comum. Apenas para ilustrar, até mesmo instituições bancárias transnacionais como o HSBC[111] tem sido atacadas com êxito, gerando receio por parte dos seus dirigentes, acionistas e investidores. A geração de renda por meio do pagamento de tributos por parte de empresas, por si só, já justificaria o envolvimento da sociedade na defesa dessas empresas que geram empregos no país que as defendem. Se a defesa cibernética provida pelo Estado se desenvolve adequadamente, todos tendem a se beneficiar direta ou indiretamente.

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

[111] CRUISE, Sinead. *HSBC says internet banking services down after cyber attack*. Disponível em: <http://www.reuters.com/article/us-hsbc-cyber-idUSKCN0V71BO>. Acesso em: 07/02/2016.

como o Google, segundo Pozzobon e Pozobon[112], auxiliam com seus instrumentos a possibilidade de espionagem.

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

O secretário executivo da entidade que zela pela governança da internet no Brasil, o Comitê Gestor da Internet (CGI), ao explicar a pressão da sociedade global por uma gestão internacional da rede, comentou que os Estados Unidos podem desligar a internet de qualquer país a qualquer momento[113].

O secretário Glaser, da CGI.br, informou que os Estados Unidos, em parte pressionados pelo escândalo descrito por Edward Snowden, concordaram em abrir mão da tutela que exercem sobre a Corporação da Internet para Designação de Nomes e Números (ICANN), entidade que administra questões técnicas importantes para o funcionamento da rede, como a distribuição de domínios (endereços eletrônicos da internet)[114].

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

Ameaçar a segurança na internet pode implicar em ameaçar as próprias empresas que se utilizam da rede mundial, e naturalmente tal fato pode trazer reflexos para a sociedade em aspectos como economia e segurança. A má utilização ou a negação do

---

[112] POZZOBON, Tanise; POZOBON, Rejane de Oliveira. *O que o Google sabe sobre você?* Primeiras observações sobre direcionamento de informações. In: Revista do programa de pós-graduação da Universidade Federal Fluminense no 32. Rio de Janeiro, UFF, 2015. p. 8-19.

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

[114] Ibidem.

serviço da rede mundial de computadores pode causar prejuízos que transcendem o que se imagina corriqueiramente. O mau funcionamento da rede mundial de computadores pode ameaçar a economia num aspecto macro, pois, por meio de serviços gerenciados por computadores em rede, são operadas redes elétricas, redes logísticas e outras atividades estratégicas para uma comunidade. Tais riscos exemplificados podem ser controlados ou ao menos relativizados por meio de uma boa estrutura estatal de proteção cibernética.

Uma sociedade de economia mista como a Petrobrás deve ter como escopo o fomento tecnológico para que o país detenha tecnologias de interesse; geração de empregos de qualidade, geração de renda; transformação do seu conhecimento tecnológico em produtos que gerem recursos para a sociedade brasileira e para a companhia. Os tributos advindos da comercialização de produtos e serviços podem ser altamente relevantes para a coletividade.

Quando um projeto tecnológico é espionado, é possível que haja uma perda tecnológica estratégica para a empresa e para o Estado Brasileiro, principalmente ao se considerar, no exemplo, que a Petrobrás possui tecnologia de ponta e que ela pode ser a única detentora de determinadas tecnologias. A Petrobrás, na hipótese de vazamento de informações estratégicas ligadas à sua atuação comercial, tem muito a perder, e, juntamente com ela, a sociedade que a financia: perde na diminuição do número de postos de trabalho, na redução do valor arrecadado pelo recolhimento de tributos, na criação potencial de novos concorrentes estrangeiros, dentre outros.

A internet elimina o conceito de corporação unidimensional, impessoal e massificada, demandando profunda mudança na forma como o Direito deve encarar o relacionamento entre tais atores. O Direito deve atender à sociedade digital, e o fará por meio dos instrumentos do Estado[115]. Enquanto for possível, suportará este dever por meio das boas relações sociais. Em casos de necessidade, pelo Direito; e, quando não restar alternativa para manter a ordem legal, terá que utilizar de sua força, que, no caso de redes informáticas, depende dos técnicos que atuam com o que se chama de defesa cibernética. Por ser um bem jurídico tutelado tão ímpar e estratégico, e considerando que a ameaça a este bem jurídico pode se contrapor à segurança nacional, a maior parte dos países destina recursos consideráveis para que seja defendido pelos profissionais da

[115] PINHEIRO, Patrícia Peck. *Direito Digital*. 2. ed. São Paulo: Saraiva, 2007. p. 1-2.

guerra e, em segundo plano, pelos órgãos de segurança pública. Todos estes participam do que se chama de Defesa Cibernética.

O Direito deve equilibrar, também na internet, interesses comerciais, privacidade, interesses de Estado, visando a melhor servir à sociedade. O equilíbrio, se aceito pela sociedade, deve ser fomentado por meio de vigilância e punibilidade definidos pelo próprio Direito[116]. Empresas disputam consumidores na internet, por vezes mitigam a privacidade alheia, mas também merecem a proteção da sociedade e do Estado para que continuem a agregar valor por meio do trabalho. Por meio da *deep web*, segurança e riscos podem ser potencializados.

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

O risco relacionado ao alto valor da tecnologia e do conhecimento é relevante porque torna o empreendedor e a empresa alvos compensadores para ataques cibernéticos. A consciência da importância do valor da tecnologia e do conhecimento acaba por justificar investimentos estatais na atividade de defesa no ciberespaço.

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

A maior parte dos países em desenvolvimento tem tentado agregar valor à sua economia industrializando produtos localmente, mas grande parte não fez progressos significativos. Apenas alguns poucos avançaram em processos como *catching-up*[117]. O desenvolvimento tecnológico tem se mostrado fator fundamental para o

---

[116] PINHEIRO, Patrícia Peck. *Direito Digital*. 2. ed. São Paulo: Saraiva, 2007. p. 43.

[117] Procedimento a partir do qual um país tecnologicamente avançado em determinada tecnologia auxilia um Estado menos desenvolvido a alcançar o dito desenvolvimento, ganhando competitividade tecnológica e econômica decorrente da referida ajuda.

desenvolvimento econômico de sociedades empresárias. Em economias centrais, mais da metade do desenvolvimento econômico de longo prazo são originados em mudanças tecnológicas que alimentam a produtividade, melhorando o desenvolvimento de novos produtos, processos e novos ramos de atividades[118]. Tais atividades devem ser fomentadas e protegidas pela sociedade que delas se beneficia.

A aptidão tecnológica se refere à condição de fazer uso efetivo de conhecimento tecnológico quando se deseja assimilar, utilizar, adaptar ou mudar tecnologias em uso. Inclui a capacidade de assimilar conhecimento e, a partir deste, gerar novo conhecimento. Compreende a produção, o investimento, a inovação. O acúmulo de aptidões tecnológicas, ao longo do tempo, pode fomentar uma industrialização de mais alto nível, com o consequente desenvolvimento socioeconômico na hipótese de o fenômeno acontecer em regiões menos desenvolvidas[119]. Se as atividades de defesa cibernética fomentadas pelo Estado podem proteger tais valores que geram desenvolvimento sinérgico para toda a comunidade, o Estado deve, para seu próprio bem, fazê-lo.

A industrialização pode ser acelerada por meio da imitação, o que não implica necessariamente em falsificação ou clonagem de mercadorias importadas. A imitação pode ser uma atividade legal, que não envolve violação de patentes nem violação de propriedade intelectual[120]. Se a imitação é precedida de invasões cibernéticas alienígenas com foco em espionagem industrial, pode trazer grandes prejuízos para empresas, para a sociedade, para o ambiente acadêmico e o governo que foram vítimas de tal atividade. A depender do tamanho do prejuízo socioeconômico, pode até mesmo ameaçar a segurança nacional. Deve-se ter sempre em mente que, quando as empresas são ameaçadas, junto com elas é ameaçado o desenvolvimento social que geram, aí incluídos empregos e renda gerados e os impostos arrecadados que a sociedade espera receber delas. A proteção das sociedades empresárias contra-ataques cibernéticos pode até ser realizada por uma atividade privada, mas o Estado pode e deve adotar políticas públicas que protejam as empresas deste tipo de vulnerabilidade, pois, mesmo em uma visão egoística, estaria, em última análise, protegendo a si próprio. Este raciocínio é

---

[118] KIM, Linsu. *Da imitação à inovação*: a dinâmica do aprendizado tecnológico da Coréia. Campinas: Unicamp, 2005. p 13-16.
[119] Ibidem. p. 16-18.
[120] Idem. p. 27.

evidenciado, inclusive, pelo cumprimento da função social da sociedade empresária: a empresa favorece a sociedade, e esta deve tomar medidas para fomentá-la e preservá-la.

A capacitação tecnológica é algo complexo, influenciada por fatores como: ambiente de trabalho, nível de desenvolvimento tecnológico nacional, políticas públicas, educação formal, viés sociocultural e estrutura organizacional. As fontes do aprendizado tecnológico podem ser os esforços internos das sociedades empresárias, da comunidade nacional e da comunidade internacional[121]. Adicione-se aos fatores já elencados que influenciam a capacitação tecnológica a própria disponibilidade de uma rede de computadores livre, veloz, irrestrita e segura. Por meio de redes de computadores seguras as pesquisas tecnológicas podem refletir conhecimentos sinérgicos trocados entre pesquisadores, usuários em potencial da tecnologia desenvolvida ou aperfeiçoada, outros interessados. Frise-se, pois, que limitar o uso da internet não pode ser considerada uma solução razoável, pois tal tecnologia hoje fomenta o desenvolvimento em quase todos os ramos da economia, de uma forma ou de outra.

Das fontes apresentadas, a comunidade internacional constitui, por vezes, a mais relevante para sociedades empresárias em processo de *catching-up*, pois, quando mudanças tecnológicas são implementadas em países desenvolvidos, são criadas oportunidades favoráveis em países que tentam recuperar seu atraso tecnológico. Empresas que desenvolvem uma rede ampla e ativa com a comunidade internacional fortalecem sua própria capacidade tecnológica[122], no entanto carecem ainda mais de proteção, porque por vezes lidam também com patrimônio de terceiros estrangeiros. A distância induz ao uso de redes informáticas para o trânsito de informações, e o prejuízo potencial para o Estado e a sociedade pode ser agravado pela possibilidade de indenização a empresas estrangeiras por eventual vazamento de informações estratégicas, obrigando o Estado a perder divisas para pagamento de relevantes indenizações em hipóteses de pouca segurança no trânsito de informações. Mesmo em hipóteses de culpa concorrente, o prejuízo pode existir e deve ser evitado.

É vantajoso para a sociedade investir na sustentabilidade das sociedades empresárias. E a segurança cibernética é mais uma forma de investimento que favorece

---

[121] KIM, Linsu. *Da imitação à inovação*: a dinâmica do aprendizado tecnológico da Coréia. Campinas: Unicamp, 2005. p. 145.
[122] Ibidem. p 145-146.

a todos, inclusive as empresas. Quando se busca resguardar empresas, protege-se também a economia, pela consequente potencialização de segurança no trânsito de informações por redes informáticas.

Apenas para citar modelos de países centrais, hoje se cogita segurança cibernética por meio de parcerias público-privadas[123]. O referido modelo pode ser importado de países centrais e perfeitamente aplicado à realidade brasileira. Com um contrato bem construído, eventual parceria pode ser um ganho para o parceiro privado, para a sociedade e para o Estado que fomenta tal parceria.

[123] KESAN Jay P; HAYES Carol M. Mitigative counterstriking: self-defense and deterrence in cyberspace. In: *Harvard Journal of Law & Technology.* Volume 25, Number 2 Spring 2012. Disponível em: <http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech429.pdf>. Acesso em: 14 jan. 2016.

## 2 O PUGILATO CIBERNÉTICO E O DIREITO À PRIVACIDADE

A despeito de antiga, a dicotomia entre coletividade e individualidade continua a fazer parte de discussões em diversos ramos das ciências sociais. Quanto ao aspecto coletivo, Carlos Ayres Britto refere-se à comunidade como evolução da sociedade[124]. No contexto atual, questiona-se ser mais conveniente para uma comunidade democrática o direito à privacidade ou a segurança contra potenciais ameaças que as redes informáticas podem oferecer ou potencializar. Pretende-se que na polêmica não se olvide dos conceitos de centralidade individual e de coesão social, necessários à evolução democrática.

Neste debate, deve-se considerar que grandes riscos estão presentes em uma e outra opção, no entanto tais riscos podem ser controlados pela própria comunidade, para que permaneçam em níveis aceitáveis. Beck[125] aduz em sua obra que a resistência ao terrorismo pode abrir caminho para uma grande política contra um oponente comum: o terror.

Segundo pesquisa de 2015 patrocinada pela Anistia Internacional e conduzida pela YouGov[126], a população de treze países, incluindo Estados Unidos e Brasil, se opõem à monitoração feita por governos em seus cidadãos, e reprovam a espionagem estadunidense em outros países. É interessante notar ainda que a maioria é favorável a espionagem de estrangeiros em seus próprios países[127]. Por certo, nem todos conhecem a fundo o problema, no entanto a maioria sinaliza que não deseja ser monitorado por governos, reforçando a ideia de que uma eventual monitoração esteja, como regra, desvinculada de agentes do governo.

A Avast, empresa transnacional que trabalha com segurança da informação em redes de computadores, realizou uma pesquisa em 11 países e concluiu que a maioria das pessoas em países desenvolvidos prefere ter fotos próprias expostas na internet do que dados financeiros pessoais. A resposta se inverte em países como Rússia, Índia e

---

[124] BRITTO, Carlos Ayres. *O humanismo como categoria constitucional*. Rio de Janeiro: Ed. Forum, 2012.
[125] BECK, Ulrich. *Sobre el terrorismo y la guerra*. Barcelona: Paidós, 2003.
[126] Empresa transnacional que realiza consultoria e pesquisa.
[127] ANISTIA INTERNACIONAL. *Pesquisa inédita indica preocupação dos internautas brasileiros com vigilância e privacidade na internet.* Disponível em: <https://anistia.org.br/noticias/pesquisa-inedita-indica-preocupacao-dos-internautas-brasileiros-com-vigilancia-e-privacidade-na-internet/>. Acesso em 14 fev. 2016.

Brasil[128]. De uma forma ou de outra, percebe-se que há uma invasão crescente à privacidade de todos, indistintamente, seja dentro da legalidade ou como a relatada por Edward Snowden[129].

Vive-se numa era na qual nem todos têm consciência das possibilidades tecnológicas que mitigam a privacidade. Um desabafo na internet pode fazer com que sua vida passe a ser um "livro aberto". Muitas tecnologias permitem armazenar sites visitados ou assuntos pesquisados. Somado ao que se compartilha voluntariamente na rede mundial de computadores – utilizando-se computadores pessoais ou *smartphones*–, a observação da conduta na internet é uma ferramenta para analisar o usuário em detalhes: a hora em que se usa a rede, o que se está buscando, de onde realiza os acessos. Anúncios são direcionados de forma pessoal, em razão de interesses demonstrados na rede[130].

Uma vez que um aparelho informático, como um *smartphone* ou um computador pessoal, está conectado à rede mundial de computadores, termina a privacidade[131]. O terrorismo tem sido o maior pretexto desta realidade moderna – de invasão de privacidade – quando se trata de espionagem estatal realizada por países desenvolvidos. Não se deve olvidar que o terrorismo é fonte de riscos contra meios de controle úteis para a comunidade, e é o meio pelo qual se realizam muitos ataques potencialmente lesivos.

Neste ponto, convém tecer algumas considerações que facilitam a compreensão da relação do pugilato cibernético com o direito à privacidade. Em uma democracia, fazer valer os direitos fundamentais dos cidadãos, ainda que com uso proporcional da força, é desejável e necessário para a vida em comunidade. O Estado deve, pelo menos, estar pronto para empregar a força em favor dos cidadãos e do bem comum. No que tange ao ambiente virtual, a situação não é muito diferente. A disponibilidade de redes

---

[128] JORNALWEBDIGITAL. *Pesquisa Avast no Brasil e mais 10 países*: usuário prefere perder privacidade do que dados financeiros. Disponível em: <http://jornalwebdigital.blogspot.com.br/2015/12/pesquisa-avast-no-brasil-e-mais-10.html>, Acesso em: 14 jan. 2016. A pesquisa foi mencionada ainda em outros sítios como: <http://tecnologia.ig.com.br/2015-12-16/brasileiro-prefere-que-cibercriminoso-acesse-seus-dados-no-celular-do-que-a-mae.html>

[129] BAUMAN, Zygmunt. *Após Snowden*: Repensando o Impacto da Vigilância. Disponível em: <https://revistas.ufrj.br/index.php/eco_pos/article/view/2660/2225>. Acesso em: 14 jan. 2016.

[130] LEMOS, Ronaldo, et al. *Estudio I*: Privacidade na Internet. Globonews. Exibido em: 30 maio 2012.

[131] Ibidem.

de computadores e os direitos assegurados de forma efetiva pelo Estado criam condições para que sejam tuteladas economias, empregos, vidas.

A tutela eficiente de direitos em ambiente cibernético é mais eficaz quando o Estado se previne contra potenciais danos causados por meio de redes informatizadas. Isso se torna mais claro a partir da constatação de que o Direito nem sempre pode garantir que danos sejam evitados ou reparados. Não são raros os casos em que um juízo é incapaz de alcançar quem eventualmente agride um bem jurídico tutelado, ainda que o agressor seja determinado ou determinável: é quando o resultado de um processo judicial é o típico 'ganha, mas não leva'.

A razão para isso é que o conceito de jurisdição se baseia na soberania, que, por sua vez, diz respeito a um poder exercido, via de regra, em determinado território. Pode ser que um bem jurídico seja tutelado pela norma brasileira, mas não alcance o agressor em razão de este e seus bens se encontrarem em outro território, no qual o direito violado não seja tutelado.

Para que a ordem jurídica seja assegurada nas hipóteses em que eventual agente agressor, que se utiliza da internet, se encontra fora do alcance das forças públicas do Estado, é necessário um trabalho de prevenção técnica, aliado à repressão pela técnica rápida e eficaz.

Destarte se faz necessário o atendimento às necessidades técnicas típicas do pugilato cibernético, para que o Estado assegure a ordem jurídica em redes informatizadas. Acontece que tais necessidades técnicas, por englobarem atividades de vigilância, são relacionadas com mitigação da privacidade. Deve-se, assim, procurar um equilíbrio para que seja efetivo o respeito ao direito constitucional à privacidade em contraponto à defesa nacional, reforçando o Estado democrático de direito. Constatar-se-á, a seguir, que os resultados esperados do pugilato cibernético muitas vezes são potencializados pela limitação da conquista social ao direito à privacidade.

Agentes públicos especializados em defesa cibernética podem proteger a sociedade de grandes ameaças, o que tem repercussões não somente no ambiente virtual. As ameaças em potencial são muitas, e a melhor regulação deverá levar em conta todas elas. As normas que regulam como a defesa cibernética deve ser implementada pelo Estado devem ser objetivas no que for possível, oferecendo

segurança jurídica para a sociedade e para os profissionais que atuam na área. No entanto, como a prática efetiva nas redes informáticas normalmente está um passo à frente da norma, infere-se a necessidade de que as normas que regulam o tema sejam também principiológicas ou determináveis em alguns casos.

Evidencia-se uma mobilização transnacional contra o terrorismo materializada em acordos internacionais já percebidos por Ramírez[132]. Para o autor, um marco significativo em tal esforço foi o ataque contra as torres gêmeas acontecido em Nova Iorque em 2001. O autor destaca como instrumentos jurídicos contra o terror, além da Convenção de Genebra de 1937 (no tocante ao tema) e da Convenção Europeia sobre Repressão do Terrorismo de 1977; a Convenção Internacional para a Repressão dos Atentados Terroristas Cometidos com Bombas, de 1998; a Convenção Internacional para a Repressão do Financiamento do Terrorismo de 2000. Como prováveis consequências do marco em pauta, diversos debates em assembleias organizadas pela ONU e a Convenção Interamericana contra o Terrorismo, de 2002.

Tantos instrumentos jurídicos internacionais visando a um objetivo comum dos Estados tendem a facilitar a efetividade da defesa cibernética, visto que é uma grande aliada do combate ao terror. Mesmo por via transversa, todo este debate já acontecido em desfavor do terrorismo acolhe grande parte dos argumentos postos para que o pugilato cibernético tenha por consequência o melhor que os Estados podem ofertar para a comunidade. É chegada a hora de debater sobre os limites da atuação dos Estados nas redes informáticas tendo sempre em vista o objetivo final que é uma sociedade democrática, segura, ordeira, progressista.

O trabalho legislativo nacional da regulação desse setor deve ser realizado com muita cautela. Um remédio utilizado em doses excessivas pode fazer mal. Ademais, vendo apenas pelo prisma da segurança, potenciais ameaças devem ser monitoradas. O grande objetivo deve ser a qualidade de vida em sociedade, no caso em razão da necessidade de segurança.

A sociedade livre, justa e solidária proposta pela CR/88 depende de paz e estabilidade para ser consolidada. A preferência constitucional pela solução pacífica de

---

[132] RAMÍREZ, Sergio García. Considerações sobre terrorismo. In: OLLOQUI, José Juan de (Coord.). *Problemas jurídicos y políticos del terrorismo*. México: Universidad Nacional Autónoma de México, 2004. p. 67-123.

conflitos e o repúdio ao terrorismo acenam para que a defesa cibernética nacional se fortaleça ou a soberania nacional dependerá de favores de aliados quando a ameaça se utilizar como meios as redes informatizadas. A Lei nº 7.170, de 14 de dezembro de 1983, que define os crimes contra a segurança nacional, também ampara o entendimento ora exposto ao acatar o texto de seu artigo 20, que criminaliza com reclusão condutas terroristas. Evidentemente a conduta se subsumirá ao tipo penal em hipóteses em que o agente da conduta criminosa se utiliza de meios informáticos. A Lei nº 13.260, de 16 de março de 2016, regulamentando o inciso XLIII do art. 5º da Constituição da República, define o crime de terrorismo, abordando aspectos investigatórios e processuais inerentes ao tema, inclusive conceituando organização terrorista. Todo este arcabouço jurídico concorre para a sociedade livre, justa, solidária e para a atuação pelo Estado no pugilato cibernético em favor de sociedade.

O arcabouço legal ora apresentado concorre ainda para os objetivos postos pela Convenção Interamericana contra o Terrorismo, de 2002, patrocinado pela OEA (Organização dos Estados Americanos), e com franca adesão estadunidense, maior potência bélica das Américas, inclusive no campo cibernético. Soa falacioso o argumento de que o Estado e o povo brasileiros estariam a salvo de ameaças terroristas, mas ainda que tal argumento fosse razoável, não autorizaria o descuido com a prevenção de significativas ameaças às comunidades que usam meios informáticos em alguma fase de potencial conduta terrorista.

Destaca-se que as Forças Armadas têm sido empregadas em operações de garantia da lei e da ordem, atuando, assim, em algumas ocasiões, como órgãos de segurança pública. Para tal hipótese de emprego, deve também haver preparação adequada, mesmo em épocas de não crise e não guerra. Ainda que esta preparação exista, o foco das Forças Armadas deve ser, em regra, a Segurança Nacional, conforme preceito constitucional disposto no art. 142[133] no sentido de que as referidas forças destinam-se à defesa da Pátria, à garantia dos poderes constitucionais e, devidamente demandados, da lei e da ordem.

[133] Art. 142, CR/88. As Forças Armadas, constituídas pela Marinha, pelo Exército e pela Aeronáutica, são instituições nacionais permanentes e regulares, organizadas com base na hierarquia e na disciplina, sob a autoridade suprema do Presidente da República, e **destinam-se à defesa da Pátria, à garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem.** (grifos do autor)

Em hipóteses nas quais as Forças Armadas atuem também em favor da Segurança Pública[134], como eventualmente tem acontecido [135], o ideal é que seja utilizado o banco de dados das forças de segurança pública, a fim de se cumprir o previsto na Portaria Normativa nº 3.389/2012 do Ministério da Defesa, complementando os dados eventualmente levantados durante as operações de cooperação. Tal Portaria discorre sobre a Política Cibernética de Defesa, e promove uma atuação colaborativa da sociedade brasileira para com o Pugilato Cibernético, e ainda orienta as aludidas atividades para o atendimento das necessidades de Segurança Nacional. A proposta apresentada pelo *Livro Verde de Segurança Cibernética no Brasil*, do Gabinete de Segurança Institucional da Presidência da República, conforme já visto, também é considerado.

Exclui-se, portanto, das considerações da pesquisa, as controvérsias sobre a legitimidade da atuação das forças armadas na segurança pública. A garantia da segurança pública será, em regra, problema a ser resolvido pelas polícias, sem intervenção das Forças Armadas. Em casos de necessidade, realizando-se operações conjuntas, as Forças Armadas poderão se utilizar das informações disponibilizadas pelas polícias, que são consideradas, conforme texto constitucional, forças auxiliares empregadas como reserva das forças armadas em situações determinadas[136].

Atualmente, os ataques cibernéticos são ameaça constante a pessoas e instituições em todo o planeta. Como um evento danoso pode provir de qualquer lugar, a qualquer momento e contra qualquer pessoa, a segurança depende de prevenção e verdadeira prontidão. O poder constituído deve estar pronto para reagir a agressões perpetradas por meios cibernéticos, razão pela qual a preparação deve ser contínua: ela não termina, apenas se aperfeiçoa. A aptidão pode se dar por meio do aperfeiçoamento técnico de equipamentos e/ou pela capacitação dos profissionais da área e seus bancos

---

[134] DAMÉ, Luiza. *Dilma assina decreto de Garantia da Lei e da Ordem para o Rio*. Portal O Globo. Disponível em: <http://oglobo.globo.com/brasil/dilma-assina-decreto-de-garantia-da-lei-da-ordem-para-rio-12022760>. Acesso em: 26 jun. 2014.

**[135]** PORTAL G1. *Governo diz que já tem autorização para usar Exército nas ruas, na BA.* Disponível em: <http://g1.globo.com/bahia/noticia/2014/04/dilma-assina-decreto-de-garantia-da-lei-e-da-ordem-para-ba-diz-governo.html>. Acesso em: 30 jun. 2014.

[136] Art. 144, CR/88. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos: § 6º - As polícias militares e corpos de bombeiros militares, **forças auxiliares e reserva do Exército**, subordinam-se, juntamente com as polícias civis, aos Governadores dos Estados, do Distrito Federal e dos Territórios. (grifo nosso)

de dados. Deve-se sempre levar em consideração, por ocasião do planejamento e da preparação, a opção da sociedade no que se refere à intensidade de defesa, inversamente proporcional ao direito à privacidade.

Assim como a polícia necessita de bancos de dados e trabalhos estatísticos para otimizar a sua atuação, quem labora com defesa cibernética terá seu trabalho otimizado pelo uso da estatística e de bancos de dados, sem os quais a atividade é exercida sem foco. O trabalho de defesa certamente será repressivo, mas deve ser também – e com muito mais razão, nesse caso – preventivo, de forma a perseguir economicidade e eficiência, que são princípios da Administração Pública.

Quando há processamento eletrônico de dados para análise, os algoritmos utilizados podem ser previamente selecionados considerando os objetivos que a sociedade deseja alcançar por meio da preparação para o pugilato.

Tal preparação, como já retratado, possui íntima relação com privacidade. Destaque-se com alguns grifos o que a Magna Carta brasileira dispõe de forma categórica no art. 5º, X, CR/88 sobre o tema:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...]
> X - **são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação**. (grifo nosso)

Caracterizando o direito à vida previsto no *caput*, decorre que é preciso assegurar um nível de vida compatível com a dignidade humana (vida digna).[137] Certamente uma vida digna prescinde de graves ameaças, o que torna a segurança fundamental num contexto de possível risco social, como o que pode acontecer sem uma adequada segurança cibernética.

Sobre o inciso X supramencionado, pode-se asseverar que não se deve admitir, em regra, a obtenção e a disseminação não autorizada de informações pessoais. Revelar assuntos privados pode configurar uma exposição do indivíduo de forma prejudicial.

---

[137]CANOTILHO, J. J. Gomes, et al. *Comentários à Constituição do Brasil*. São Paulo: Saraiva/Almedina, 2013. p. 213.

Deve-se ainda preservar a inviolabilidade no sentido de que sejam impedidas buscas e apreensões estatais, realizadas na esfera privada, até o limite do que a comunidade considera razoável. Em regra, deve-se defender a privacidade do indivíduo e da família[138]. Porém, há que se destacar o exemplo contraditório dos Estados Unidos: o mesmo país, que positivou a proteção prevista na já citada quarta emenda da Constituição estadunidense, oferecia até pouco tempo a proteção do *Patriotic Act* para o combate ao terrorismo, ambos institutos já abordados neste trabalho, e aparentemente antagônicos.

A não renovação temporal do *Patriotic Act* pelo Congresso estadunidense em junho de 2015 pouco muda no panorama ora analisado. Em primeiro lugar, existe a hipótese de ser sucedido por uma norma de alcance compatível em breve, apesar do contexto eleitoral. O ato não foi renovado em razão de uma manobra política de se usar o regimento da casa de forma a não permitir a renovação, a qual não chegou a ser votada a tempo. Em segundo lugar, a falta de mobilização pela prorrogação do *Patriotic Act* deve-se ao fato de a espionagem continuar liberada quando não se tratar de cidadão estadunidense. Em outras palavras, a manutenção da estrutura já montada e descrita por Edward Snowden parece justificada para uma atuação sem o *Patriotic Act*.

Numa perspectiva do Direito europeu, o respeito à vida privada inclui a inviolabilidade das comunicações em geral, inclusive o respeito à inviolabilidade da correspondência. Contextualizado no assunto, está o que a literatura alemã retrata sobre o íntimo, o secreto, o privado; tudo num sistema de autodeterminação informacional, extraído a partir de um juízo concreto de ponderação do "direito geral da personalidade". Este é considerado por alguns como uma parte da teoria das esferas elevada ao nível dos direitos, e aflora a partir da efetivação de direitos mais concretos, como o direito às esferas íntima, secreta e privada, assegurando o respeito à inviolabilidade documental, de dados, de comunicações pessoais, e, em especial, à intimidade, núcleo mais sensível da esfera privada[139].

A mesma França, cujo código civil diferencia vida privada íntima de vida privada ordinária, com diferentes consequências jurídicas, desde 2015 ameaça o limite da proteção à privacidade com a já citada norma que oferta a legalidade da espionagem

[138] CANOTILHO, J. J. Gomes, et al. *Comentários à Constituição do Brasil*. São Paulo: Saraiva/Almedina, 2013. p. 276-277.
[139] Ibidem. p. 277.

ostensiva e em massa, também sob a justificativa de combate ao terrorismo. Essa parece ser uma tendência, principalmente quando analisada em face da atuação do Estado Islâmico[140].

No Brasil, os termos intimidade e vida privada são usados como sinônimos, em que pese alguns autores que estudam o assunto mais a fundo ressalvarem que a intimidade é mais restrita[141, 142]. A norma constitucional é categórica, mas existem outras carências – não menos importantes – da comunidade que devem ser supridas pelo Estado. Ou seja, os direitos possuem limites. Não há direito absoluto[143]. O direito à intimidade pode ceder em face da segurança pública, de outro direito ou diante de um bem coletivo, por exemplo. Se a redução do âmbito de incidência da proteção normativa se dá em abstrato apenas por meio de uma lei, o mesmo não se pode afirmar diante de um caso concreto[144].

A Lei nº 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos, visa a tutelar dados existentes em dispositivos informáticos. Tal inviolabilidade de dados armazenados decorre do mandamento constitucional previsto no art. 5º, X, CR/88 supramencionado.

Em meados de 2014, entrou em vigor no Brasil o Marco Civil da Internet. A Lei nº 12.965, de 23 de abril de 2014, a qual regula a internet no Brasil, privilegia a privacidade, a proteção aos dados pessoais, a responsabilização sobre condutas, conforme se conclui da análise do seu art. 3º[145]. Da leitura dos art. 8º[146] e 11[147] da

---

[140] Grupo terrorista jihadista considerado dos mais radicais, violentos e impiedosos da atualidade, segundo o portal TERRA.

[141] CANOTILHO, J. J. Gomes, et al. *Comentários à Constituição do Brasil*. São Paulo: Saraiva/Almedina, 2013. p. 277.

[142] No mesmo sentido, conforme já abordado na introdução, o Professor Carlos Ayres Britto entende que o Direito à Intimidade protege a pessoa sozinha, consigo mesma; enquanto o Direito à privacidade protege o indivíduo se relacionando com outros.

[143] Poder-se-ia afirmar que como regra, não há direito absoluto. Baseado em discussões acontecidas no plenário do STF, e a partir de entendimentos de doutrinadores como Kildare Gonçalves Carvalho, Ingo Wolfgang Sarlet, José Joaquim Gomes Canotilho afirma-se que a proibição à tortura, à escravidão, e ao tratamento desumano e degradante são considerados por respeitável doutrina como direitos fundamentais absolutos – entendimento baseado no direito à dignidade da pessoa humana, previsto no art. 1º, III da CR/88. Este também é o posicionamento do Ministro Carlos Ayres Britto, pois segundo ele seria impossível a relativização dos aludidos direitos.

[144] CANOTILHO, J. J. Gomes, *et al*. *Op Cit*. p. 282-283.

[145] Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - **proteção da privacidade**; III - **proteção dos dados pessoais**, na forma da lei; IV - preservação e garantia da neutralidade de rede; V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - **responsabilização dos agentes de acordo com suas atividades, nos termos da**

mesma norma depreende-se que o legislador, mais uma vez, privilegia o direito à privacidade. Coloca o exercício do referido direito como condição para o pleno exercício da prerrogativa de acesso à rede mundial de computadores, sendo nulas quaisquer cláusulas contratuais que violem tal garantia. Outrossim, são igualmente nulas cláusulas que desrespeitem o direito à inviolabilidade e ao sigilo das comunicações em rede. A proteção oferecida pela Lei quanto a coleta de dados pessoais observar a norma brasileira diz respeito, também, a serviços prestados do exterior, desde que pelo menos um dos terminais de computador envolvidos esteja localizado no Brasil e o empreendimento oferte serviço ao público brasileiro, ou ainda o grupo econômico possua estabelecimento no Brasil.

Depreende-se de tal entendimento que o legislador quer fazer valer a Lei brasileira quando há envolvidos localizados no Brasil quando o assunto é proteção de dados e à privacidade; no entanto tem consciência de que existem algumas limitações à vontade expressa no texto legal decorrentes da arquitetura da rede. Pouco poderá fazer o Estado brasileiro sem um aparato de segurança cibernética a sua disposição ou ajuda internacional, se, *v.g.*, a empresa ou grupo econômico não estiverem fisicamente no Brasil.

---

**lei**; VII - preservação da natureza participativa da rede; VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. [...] (grifo nosso)

[146] Art. 8º A **garantia do direito à privacidade** e à liberdade de expressão nas comunicações **é condição para o pleno exercício do direito de acesso à internet.**
Parágrafo único. **São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que: I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet**; ou II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil. (grifo nosso)

[147] Art. 11. 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, **deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.**
§ 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, **desde que pelo menos um dos terminais esteja localizado no Brasil.**
§ 2º O disposto no caput 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**.
§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, **bem como quanto ao respeito à privacidade e ao sigilo de comunicações**. [...] (grifo nosso)

Ao revés, se existe um aparato de defesa cibernética compatível com o objetivo a ser alcançado, o pugilato cibernético promovido pela comunidade pode, além de protegê-la em situações críticas, fazer valer a Lei nacional em território brasileiro.

Tal realidade decorre do fato de que em redes informáticas, o princípio da territorialidade é mitigado. Face a tal entendimento, pode não fazer sentido proteger, por meio da norma brasileira, dados que são devassados por usuários da rede ao redor do planeta. A premissa é simples: a internet não respeita fronteiras. A construção da proteção informática não pode ser realizada alhures ou apenas baseada em bonitas ideologias. Em que pese os esforços no sentido de debater normas internacionais para operações de informação, inclusive cogitando o uso de analogia em sua aplicação[148], a eficácia deste esforço parece distante da realidade em que hoje se vive.

A visão do que ocorre atualmente na comunidade deve ser pragmática, para que sejam reduzidos os danos sociais e para que ao menos as normas nacionais contribuam efetivamente com o bem da sociedade brasileira quando se cogita tratar de direito aplicado em redes de computadores. O ordenamento jurídico brasileiro protege convenientemente a privacidade em abstrato. A sociedade, porém, deve considerar a real ameaça à paz social não somente pelo terrorismo, ressaltando a ameaça da mitigação da privacidade. O indivíduo também deve se proteger do Estado que foi criado para protegê-lo, e que deve lhe possibilitar a participação democrática, liberdade e qualidade de vida, no caso brasileiro.

Eventos envolvendo esta temática que ocorrem em outras partes do mundo devem ser trazidos ao debate social, visto que não faz sentido que somente os agentes localizados em território brasileiro e no domínio virtual brasileiro se sujeitem a limitações que trazem inúmeros prejuízos, inclusive econômicos a empreendedores, inclusive.

A própria norma admite sua limitação de alcance, como no § 1º do art. 11 grifado *supra*. Entretanto, como já visto anteriormente, brasileiros comuns já são vigiados ao redor do mundo por nações e empreendimentos estrangeiros. De toda forma, parece inaceitável dar carta branca para os agentes políticos que conduzem

[148] HOLLIS. Duncan B. *Why States Need an International Law for Information Operations*. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1083889>. Acesso em: 10 fev. 2016.

investigações, sob pena de a estrutura – concebida para contribuir com a sociedade – causar danos a esta.

A despeito da clareza da norma constitucional, do Marco Civil da internet e de outras normas no quesito privacidade, em que pese as interpretações clássicas oferecida a estas normas, elas devem ser entendidas em seu contexto, de forma a contribuir com a própria sociedade, considerando os riscos que o cidadão médio tem assumido na prática.

Por certo, nem todas as pessoas aceitam mitigar sua privacidade em nome da segurança, o que pode ser demonstrado pelo crescente mercado dos aparelhos chineses Blackphones[149] (com sistema operacional PrivatOS), ou ainda a migração de usuários comuns de *smartphones* para telefones com *flips,* pensando na melhoria de sua privacidade. Ainda assim, hoje em dia, a maioria das pessoas age como se desconhecesse os riscos à sua privacidade ou os aceitasse.

Até que a sociedade se posicione de forma diversa, parece razoável realizar a leitura da norma que preserva a privacidade considerando a realidade da comunidade global em que vivemos racionalizando o custo-benefício. Una-se a tal realidade o fato de que Segurança Cibernética é o mais novo e maior problema exclusivo de segurança nacional do século XXI. Apesar disto, pelo menos até 2015, não se teve notícia de nenhum amplo debate nos Estados Unidos sobre o conceito de guerra cibernética; como também debates sobre as normas estadunidenses ou internacionais que poderiam se relacionar com o termo ora referido[150].

Muitos são os exemplos históricos a demonstrar que sociedades já tiveram que se defender de seu próprio governo, e serem defendidas pelos poderes constituídos. Sendo assim, parece ser um risco muito grande a radicalidade de permitir a devassa da privacidade pelas instituições, assim como o de não permiti-la em nenhuma medida. A variável de maior peso parece ser o nível democrática da sociedade.

O debate social é um meio adequado para conscientizar a coletividade dos riscos, para que a própria sociedade decida sobre seu futuro e assuma as consequências de tal decisão. Deixar essa decisão para os governos também pode ser uma ameaça para

---

[149] Mais informações em: https://blackphone.ch/

[150] MALAWER. Stuart S. *Cyber Warfare*: Law and Policy Proposals for U.S. and Global Governance. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1437002&download=yes>. Acesso em: 10 fev. 2016.

a comunidade, pois não se pode afirmar até quando um governo será fiel ao que o povo dele espera e qual uso fará de informações pessoais a que venha a ter acesso. Nesse âmbito, todos os riscos devem ser assumidos consciente e voluntariamente.

## 2.1 O direito à privacidade como uma conquista civilizatória

Sobrepesar o direito à privacidade com outros direitos e garantias é algo que deve ser feito considerando que a privacidade é um signo da evolução. O conceito de privacidade sofreu e sofre variações, por vezes de forma célere. O termo privacidade tem origem no latim *privates,* que significa separado do resto. Uma pessoa, separando-se do resto, pode se revelar. A privacidade é uma conquista civilizatória, fruto de expressivo esforço e coesão social na luta por direitos individuais. Olvidar tal conquista é abrir mão de uma vitória relevante dos antepassados. Ao fim e ao cabo, a privacidade é um signo de avanço das comunidades.

No Direito Romano, afirmava-se a supremacia do público sobre o privado. As mudanças na relação entre as esferas pública e privada foram muitas ao longo dos séculos, em especial no pós-Idade Média. Hoje em dia, o Direito Público deve legitimar-se frequentemente junto à sociedade, sobretudo no que tange a restrições a direitos e garantias individuais, no intuito de demonstrar a imprescindibilidade do interesse público face a determinada limitação individual.

Na introdução deste trabalho, informou-se que o termo privacidade está sendo usado em sentido amplo por ora. No entanto é conveniente discorrer de forma mais pormenorizada sobre o instituto neste momento.

Robert Alexy, em sua obra Teoria dos Direitos Fundamentais[151], menciona a teoria das esferas (*Sphärentheorie*). Talvez Heinrich Hubmann tenha sido, em sua obra *Das Persönlichkeitsrecht,* um dos primeiros a divulgar tais conceitos[152]. Henkel, de forma semelhante, classifica a personalidade humana em três esferas, em grau

[151] ALEXY, Robert. *Teoria dos direitos fundamentais*. Trad. Virgilio Afonso da Silva. 2 Ed. São Paulo: Malheiros Editores, 2008. p. 360 e ss.
[152] CORDEIRO, Antônio Menezes. *Tratado de Direito Civil Português*: Parte Geral – Pessoas. Lisboa: Almedina, 2004. v. 1, tomo III. p. 200.

decrescente de proteção[153]. Trata-se, em síntese, de classificações com utilidade semelhante.

Na figura das esferas concêntricas, a esfera mais interna caracteriza-se pelo território do mais íntimo: compreende os assuntos de natureza reservada, assuntos secretos, de interesse personalíssimo (*Geheimnisphäre*). Ao redor deste círculo, a segunda esfera privada inclui assuntos que o indivíduo oferece para conhecimento de pessoas de sua confiança, ficando de fora a comunidade em geral (*Privatsphäre*). O terceiro círculo – o mais amplo e, portanto, o menos íntimo – engloba tudo o que se leva ao conhecimento de terceiros, numa esfera de domínio social ou público.

Aspectos relacionados, por exemplo, à vida sentimental, estado de saúde, convicções políticas e religiosas são de foro íntimo, e estariam no círculo mais interno. Fatos partilhados com limitado número de pessoas diriam respeito a aspectos da vida privada. A considerar, assim como Tércio Sampaio[154], que a intimidade não repercute na esfera social, esta deixa de estar, sob qualquer pretexto, ao alcance do Estado fiscalizador. O Estado só pode proteger o cidadão naquilo que potencialmente repercute na esfera social.

Antes, privacidade era um conceito ligado à burguesia, individualista, próprio do liberalismo. O direito teve que se adequar ao desenvolvimento tecnológico. Para Doneda, podem-se unificar os valores expressos pelos termos intimidade e vida privada[155]. Todavia, esses dois conceitos ganharam novos contornos com o surgimento da internet, que revolucionou a comunicação em massa e facilitou sobremaneira a exposição da vida privada.

Os direitos à intimidade e à própria imagem integram a proteção constitucional à vida privada para Alexandre de Moraes. Tal proteção, para o autor, salvaguarda um espaço íntimo intransponível por intromissões ilícitas externas. Intimidade e vida privada são conceitos próximos, diferenciados pela menor amplitude da intimidade. A privacidade envolve os relacionamentos de um ser humano, inclusive relações

---

[153] SAMPAIO, José Adércio Leite. *Direito à intimidade e à vida privada*: uma visão jurídica da sexualidade da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998. p. 255.

[154] FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados*: o direito à privacidade e os limites à função fiscalizadora do Estado, Cadernos de Direito Constitucional e Ciência Política. São Paulo: Revista dos Tribunais, 1992. p. 77-90.

[155] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 111-112.

comerciais, laborais ou acadêmicas para o constitucionalista brasileiro. O doutrinador admite que a garantia não possui caráter absoluto, sendo oponível a condutas delituosas, citando como jurisprudência concorrente a seu entendimento o HC 79.285/RJ – Rel. Min. Moreira Alves. Sobre o sigilo de comunicação, o autor manifesta o direito ao sigilo de correspondência e de comunicação, mas ressalta que nenhuma liberdade individual é absoluta: admite ser possível, respeitados determinados parâmetros, a interceptação mesmo de correspondências e comunicações, sempre que as liberdades públicas estiverem sendo utilizadas como instrumento de salvaguarda de práticas ilícitas. Cita, por meio do direito comparado, que as constituições finlandesa, italiana, dinamarquesa também admitem limitações ao direito de privacidade, em regra, inviolável. Cita Vicente Greco Filho como voz discordante, pois este atribui o direito expresso no Art. 5º, X da CR/88, como absoluto, e opina Greco pela inconstitucionalidade do Art. 1º da Lei nº 9.296, de 24 de julho de 1996 (sobre a privacidade e o fluxo de comunicações em sistema de informática e telemática)[156].

Gilmar Mendes expressa que o direito à intimidade e à vida privada limita a liberdade dos meios de comunicação. Ressalta o consenso de que o direito à privacidade pretende manter o indivíduo livre da observação de outras pessoas, citando Alan West. Admite limites ao direito à privacidade em razão da vida em comunidade que acolhe interesses públicos. Tais interesses são maiores que a pretensão de "ser deixado só". A depender das circunstâncias no caso concreto a intromissão à privacidade pode ser considerada aceitável ou abusiva. O autor aborda ainda sobre o consentimento do indivíduo na restrição à privacidade. Admite que o consentimento, mesmo tácito, pode ser oferecido pelo indivíduo em desfavor de sua própria privacidade. Admite, o doutrinador, a tendência de se justificar a intrusão na vida privada em casos de relevância pública, mesmo em hipóteses em que a privacidade é documentada em meios de comunicação de massa. Ressalta que interesse público difere de interesse do público. O autor também admite que a privacidade não é um direito absoluto ao abordar o tema relacionado ao sigilo das comunicações[157]. Note-se o foco principal do debate na presente análise: a restrição ao direito à privacidade com fins a proteção da sociedade.

---

[156] MORAES, Alexandre de. Constituição do Brasil interpretada e legislação constitucional. 5. ed. São Paulo: Atlas, 2005. p. 224-250.

[157] MENDES, Gilmar Ferreira; BRANCO, Gustavo Gonet. *Curso de direito constitucional*. 9. ed. São Paulo: Saraiva, 2014. p. 280-295.

Este deve ser o norte do pugilato cibernético financiado pela comunidade. O pugilato cibernético que não protege a sociedade não parece justificar a privação da privacidade.

Canotilho, quando discorre sobre direitos fundamentais, ressalta que em caso de dúvidas de hermenêutica deve prevalecer a interpretação que restrinja menos o direito fundamental, admitindo portanto que não existem direitos absolutos[158].

Ferraz entende ser a privacidade um direito subjetivo fundamental, podendo ser, o titular, pessoa física ou jurídica, brasileiro ou não, residente ou em trânsito no país; e cujo objeto é a integridade moral do titular[159].

Silva remete ao fato de que o direito à intimidade e à vida privada é direito conexo ao da vida. Concluiu tal assertiva pelo fato de que o direito à vida está presente no *caput* do artigo, enquanto que o direito à privacidade mereceu um inciso, sendo manifestação do que está presente no *caput*[160]. Ora se a vida estiver ameaçada, de acordo com este entendimento, não há que se falar em privacidade quando o que se está em jogo é o direito à vida.

O autor ressalta que a Constituição protege contra a divulgação do privado e a investigação do privado, que seria a pesquisa de acontecimentos referentes à vida pessoal e familiar, dentre outras tutelas[161]. Neste ponto deve-se ressaltar que o pugilato cibernético, quando financiado pelo Estado, deve almejar uma pesquisa contra ameaças; o que pode em muito diferir investigar acontecimentos referentes à vida pessoal e familiar. No entanto se ao exercer o direito de estar só, o indivíduo pode ameaçar a vida, utilizando a interpretação de que a vida é o valor primeiro, expresso no *caput*, não há razão para que a privacidade seja protegida sob tais argumentos. Deve-se, no entanto, ressaltar, que a privacidade é uma relevante conquista que deve ser mantida sempre que tal direito não se torne uma ameaça para a comunidade.

Luís Roberto Barroso desvenda uma categoria jurídica desenvolvida nas últimas décadas: a dos interesses coletivos, como uma fronteira entre o público e o privado. As

---

[158] CANOTILHO, J. J. Gomes; MOREIRA, Vital. *Fundamentos da Constituição*. Coimbra: Coimbra Editora, 1991. p. 143.

[159] FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados*: o direito à privacidade e os limites à função fiscalizadora do Estado, Cadernos de Direito Constitucional e Ciência Política. São Paulo: Revista dos Tribunais, 1992. p.77.

[160] SILVA, José Afonso da. *Curso de direito constitucional positivo*. 37 ed. São Paulo: Malheiros. 2014. p. 208-212.

[161] Ibidem

relações comunitárias e os interesses coletivos comporiam a fronteira entre a vida exclusivamente privada e a vida pública; e com perspicácia infere que o público não se confunde com o estatal. O espaço público seria o da relação dos indivíduos com o Estado, com o poder político[162].

A distinção apresentada pelo autor pode dar suporte a princípios a serem respeitados pelo Estado quando dos atos de investigação necessários para a preservação da vida em seu sentido mais amplo. Em última análise, a segurança nacional é uma forma de preservar o Estado, no entanto mais que isso, a preservação da segurança do Estado pode proteger a vida de cada um de seus indivíduos. A invasão à privacidade será tão mais aceitável quanto mais perto da preservação da vida estiver. Invadir a privacidade para preservar o Estado, em última análise pode preservar seus cidadãos, mas não necessariamente. Se o Estado serve a seus cidadãos isto poderá ser verdade, mas se o Estado se serve de seus cidadãos em favor de minorias, a invasão à privacidade não poderá ser considerada legítima.

A partir da percepção dos autores aqui expressa, pode-se aduzir que o direito à privacidade no contexto do pugilato cibernético deve ser respeitado como expressão da conquista que representa. Desde os idos do direito romano que afirmava a supremacia do direito público sobre o privado, houve relevante evolução que não deve ser olvidada. A privacidade que não repercute na esfera social (intimidade) deve ser preservada do alcance do Estado fiscalizador. A divulgação da vida íntima também não interessa ao pugilato cibernético, pois a defesa cibernética está focada em proteger a sociedade de potenciais e significativas ameaças que possam advir do mau uso de redes informáticas. Obstar a intromissão de terceiros na vida privada e familiar é um direito que deve ser preservado. Esta deve ser a regra: a inviolabilidade do direito.

No entanto, considerando que nenhuma garantia possui caráter absoluto, pode-se ressalvar o direito nas oportunidades em que seu uso salvaguarda práticas ilícitas. Se de regra, a intimidade e a vida privada limitam o direito dos meios de comunicação, também deve-se limitar o Estado fiscalizador sempre que não houver indícios que justifiquem conduta diversa. Trata-se de um direito que a Constituição Federal aborda como conexo ao direito à vida, tamanha sua importância.

---

[162] BARROSO, Luís Roberto. *Curso de direito constitucional contemporâneo*: os conceitos fundamentais e a construção do novo modelo. 3. ed. São Paulo: Saraiva, 2011. p. 82-85.

Mesmo com o consentimento tácito de determinado agente, o Estado deve, de regra, preservar a privacidade em sentido lato do indivíduo. Trata-se de direito fundamental reconhecidamente válido para pessoa física e jurídica. Ademais não seria razoável permitir que nem mesmo o Estado investigue o privado por si só. O objetivo da investigação atinente ao pugilato cibernético deve ser norteado pela ameaça em potencial para a sociedade que pode advir de determinadas condutas extremamente nocivas. Devem ser tratados como casos excepcionais, e em razão de interesses coletivos. A invasão da privacidade, quando acontecer, deve ser justificada na preservação da vida a ser vivida com qualidade; e focada na segurança geral necessária para o progresso da comunidade. Tal entendimento encontra amparo, por analogia, no julgamento do HC 79.285/RJ relatado pelo Min. Moreira Alves.

### *2.1.1 A privacidade na era da internet*

Manuel Castells, ao tratar sobre o tema internet, escreveu que ela teve origem no Departamento de Defesa estadunidense, idealizada, pois, por quem entende de defesa nacional:

> [...] a internet originou-se de um esquema ousado, imaginado na década de 1960 pelos guerreiros tecnológicos da Agência de Projetos de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos (a mítica DARPA) para impedir a tomada ou destruição do sistema norte-americano de comunicações pelos soviéticos, em caso de guerra nuclear. De certa forma, foi o equivalente eletrônico das táticas maoístas de dispersão das forças de guerrilha, por um vasto território, para enfrentar o poder de um inimigo versátil e conhecedor do terreno. O resultado foi uma arquitetura de rede que, como queriam seus inventores, não pode ser controlada a partir de nenhum centro e é composta por milhares de redes de computadores autônomos com inúmeras maneiras de conexão [...][163]

A partir dessa constatação, Castells evidencia que a internet foi concebida numa arquitetura de rede que inicialmente não favorecia o controle e a vigilância devido à dispersão e multiplicidade de formas de conexão, inclusive conexões ponto-a-ponto (P2P). Esse autor ratifica tal possibilidade ao admitir o anonimato na rede por meio de

[163] CASTELLS, Manuel. *A sociedade em rede*. Trad: Roneide Venâncio Majer. 8. ed. rev. ampl. São Paulo: Paz e Terra, 2005. p 44. v. I.

sítios como Tumblr[164], no entanto, a depender da plataforma utilizada, isso não se verifica, como admite o próprio Castells quando narra que:

> o Facebook era criticado no movimento [de protesto contra a classe política] por ser uma plataforma com proprietários, o que chocava com a abertura valorizada pelo movimento. Da mesma forma, o novo software de reconhecimento facial do Facebook identifica imediatamente pessoas em fotografias, e isso era mal visto, dada a desconfiança de que o Facebook não protegeria a privacidade caso intimado por autoridades[165].

A segurança do Tumblr, *v.g.*, é relativa, não sendo nem tão segura quanto os mais conservadores desejariam, nem tão insegura quanto o que é oferecido, por exemplo, pela *deep web*[166].

Com a popularização da internet também como ferramenta de comunicação pessoal, chegou-se a imaginar que ela seria um terreno anárquico, sem controle e sem barreiras, no qual não poderia haver intervenção estatal. Rodotà evidencia em seu estudo que:

> regulamentações restritivas da coleta e da circulação de informações são possíveis em tempos razoavelmente tranquilos, ou mesmo realmente felizes. Quando, ao contrário, cresce a instabilidade social, aumenta também a necessidade de informações e da ligação entre os vários bancos de dados para enfrentar situações de emergência em matérias de ordem pública, no mercado de trabalho, e assim por diante.[167]

Tal constatação corrobora com a percepção de que o direito à privacidade não é oponível contra todos, principalmente em momentos de crise, instabilidade social e medo, em que é mais evidente a necessidade de segurança. Rodotà destaca também que o avanço da internet permite, pela possibilidade de cruzamento de dados, o controle, a vigilância e a classificação de dados[168].

Em face dessas possibilidades, algumas pessoas e governos têm mudado hábitos pela consciência do risco eletrônico: importante que se diga que tais atores são apenas

---

[164] CASTELLS, Manuel. *Redes de Indignação e Esperança*: Movimentos Sociais na era da Internet. Trad: Carlos Alberto Medeiros. São Paulo: Zahar, 2013. p. 132-134.
[165] Ibidem. p. 134.
[166] Mais informações sobre o assunto estão disponíveis em: <http://mundoestranho.abril.com.br/materia/o-que-e-a-deep-web>.
[167] RODOTÀ, Stefano. *A Vida na Sociedade da Vigilância*: A Privacidade Hoje, Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda; Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 92-95.
[168] Ibidem. p. 145-146.

alguns, e hoje não há a percepção de que sejam maioria. Agentes de inteligência de países europeus têm cogitado voltarem a usar as antigas máquinas de escrever (mecânicas). Pode-se citar um motivo ainda pouco conhecido do grande público sobre computador desconectado da rede. Dragos Ruiu, *hacker* canadense, descobriu um vírus em seu Macbook que nunca havia sido conectado à internet. Ele percebeu que o computador rodou uma atualização misteriosa que não era da Apple: mudava configurações, deletava e transmitia documentos. Pesquisadores do Instituto Fraunhofer, entidade alemã, provaram a possibilidade de espalhar vírus de computador fora das redes de computadores: bastava certa proximidade do alvo, independente de conexão à internet, comprovando a tese de Dragos. Detalhe: o vírus que atacou Dragos não é detectado por antivírus comerciais, e não infecta apenas os Macs[169].

Uma quantidade considerável de pessoas tem voltado a portar telefones cuja única função é falar. Outras tantas têm adquirido telefones cujos fabricantes investem pesado no *marketing* focado em informações criptografadas em seus produtos. Em breve serão comercializados para o público comum *smartphones* com criptografia da Rede Tor (*deep web*), o que, ao menos em tese, preservaria a privacidade dos usuários – como é o caso do Boss Phone[170].

Oportuno ainda falar da possibilidade de insegurança dos dados em nuvem já evidenciado em ataques publicados na imprensa mundial, como no caso da coleta de dados de usuários que possuíam conta relacionada ao videogame da Sony PS3[171].

Em que pese os esforços para que a privacidade seja mantida, a regra da internet parece ser a exposição. As pessoas querem o conforto proporcionado pela tecnologia e se sujeitam às suas consequências, com conhecimento de causa ou por ignorância. Sítios como o *Facebook* têm sido utilizados, até mesmo por governos como fonte de informações, atitudes que por vezes podem imprimir consequências em liberdades civis

---

[169] GARATTONI, Bruno; BADÔ, Fernando. *Vírus de computador se espalha pelo ar*. Disponível em: <http://super.abril.com.br/tecnologia/virus-computador-se-espalha-pelo-ar-787622.shtml>, consultado em: 09 ago. 2014.

[170] AGRELA, Lucas. *Boss é o primeiro smartphone com a criptografia da rede tor.* Disponível em: <http://info.abril.com.br/noticias/tecnologia-pessoal/2015/01/boss-e-o-primeiro-smartphone-com-a-criptografia-da-rede-tor.shtml>. Acesso em: 14 fev. 2015.

[171] Portal G1. *Entenda o ataque à rede on-line do PlayStation 3, a PSN*. Tecnologia e Games. Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/05/entenda-o-ataque-rede-line-do-playstation-3-psn.html>. Acesso em: 14 fev. 2015.

ou investigações criminais[172]. Em alguma medida limitam liberdades e podem proteger a sociedade ao mesmo tempo.

Os riscos assumidos vão muito além daqueles concernentes à exposição de dados nas nuvens, da exposição e publicação de dados pessoais em redes sociais, riscos de comporem um banco de dados público de pesquisadores com parte considerável de suas vidas publicadas para quem tiver interesse de conhecer. Considerem-se esses riscos como voluntários.

Há ainda os riscos dissimulados: aqueles em cuja divulgação não há interesse. Ainda assim, eles já são conhecidos e impactam na mitigação da privacidade. Como já foi colocado, tecnicamente é possível oferecer um produto ou serviço com vícios ocultos que podem ter por escopo o lucro ou a segurança da própria comunidade.

Existe a vigilância que visa ao lucro e a vigilância que protege: a tecnologia pode ser usada para bons e maus propósitos, construindo ou destruindo. A vigilância pode ser importante para a vida em comunidade. Um policiamento preventivo pressupõe vigilância, e, conforme se destacou anteriormente, a sociedade parece admitir a ameaça contra a privacidade para que sua segurança seja reforçada. Em contraposição a simplicidade proposta no presente parágrafo, pode vir o entendimento de que a divisão da vigilância que protege e da que visa ao lucro nem sempre é tão clara; e tal entendimento possui fundamento. Como se poderá constatar por meio da leitura do quarto capítulo do presente estudo, por vezes o Estado protetor se associa a empreendedores com ações nas bolsas de valores como forma de oferecer sinergia a seus projetos. Na análise oferecida adiante se poderá constatar que a internet, o iPhone, o GPS nasceram em projetos do Estado americano e encontraram fértil campo para desenvolvimento em empresas, inicialmente também americanas.

Decorre de tal constatação que a sociedade deve estar vigilante sobre os limites que pretende impor aos meios disponibilizados para que os objetivos comuns sejam atingidos. A Lei regulamentando e outras normas regulando segundo a vontade social podem funcionar como um sistema de freios e contrapesos que evitem que a vontade da

[172] SEMITSU. Junichi P. *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1782267>. Acesso em: 14 fev. 2016.

comunidade seja olvidada, sem que se abra mão da proteção que a sociedade manifesta o seu favor.

O argumento de que a vigilância visa à proteção da população pode angariar adeptos para medidas desse gênero. A autoridade pública agiria contra os maus e em favor dos que não estão fazendo nada errado; aqueles que não estão desempenhando atividade ilegal não teriam o que temer. O problema aparece na hipótese em que a autoridade utiliza os dados coletados para a consecução de outros objetivos, tais como mitigar dissidências políticas contra poderes constituídos. Discordar do poder constituído com argumentos razoáveis e inteligentes não consiste em ilegalidade: faz parte do processo de evolução de uma comunidade. Os instrumentos utilizados para proteger a população contra o terrorismo são os mesmos que podem ser utilizados para espionar quem faz oposição ao Estado. Este tipo de espionagem pode trazer consequências graves para o investigado. Tal risco não pode ser olvidado sob pena de o Estado deixar de ser democrático e eventualmente de deixar de buscar o bem comum.

### *2.1.2 A privacidade sob a perspectiva normativa*

O direito à privacidade diz respeito à tutela de informações pessoais, as quais devem ser de conhecimento único e exclusivo daquele que as detém ou produz. A privacidade pressupõe ausência de interferência de outros indivíduos ou do próprio Estado, se isto é constrangedor à pessoa (dignidade) ou se a exposição é contrária à sua vontade. A Constituição Federal de 1988 dispõe, conforme já visto, em seu Art 5º, X sobre o tema.

O Art. 5º da CR/88 trata, em seu inciso XII[173], sobre a inviolabilidade do sigilo de dados, a qual tem relação com o direito fundamental à privacidade previsto no inciso X supramencionado.

Em outras palavras, o que diz respeito ao indivíduo pode ser excluído do conhecimento de terceiros. Note-se que a ressalva constitucional ao sigilo é feita tão somente – e "em último caso" – na hipótese em que o sigilo pode limitar informação sobre um bem tutelado tão caro para a sociedade a ponto de possuir tutela penal. Uma

[173] XII - **é inviolável o sigilo** da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, **salvo**, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer **para fins de investigação criminal ou instrução processual penal**; (grifo nosso)

investigação preventiva contra crime tipificado por suposta conduta terrorista parece caber na interpretação constitucional.

O Art. 11 do Código Civil de 2002 (Lei nº 10.406, de 10 de janeiro de 2002) contém uma cláusula de proteção aos direitos da personalidade, com o escopo de salvaguardar um tratamento flexível e amplo a estes direitos[174], compatível com a ordem constitucional. O Art. 20 do mesmo código prevê o uso de imagem de terceiros sem o respectivo consentimento somente na hipótese da administração da justiça e ordem pública[175], enquanto o artigo seguinte prevê a inviolabilidade da vida privada[176].

Veículos de comunicação que se utilizam de modernas tecnologias de transmissão e difusão de dados e imagens materializam constante tensão entre a vida privada, a imagem e a liberdade de comunicação[177]. Por certo a pessoa comum não deve suportar a invasão à sua privacidade da mesma forma que uma pessoa pública. Destarte já se pode perceber que doutrina e jurisprudência sinalizam, em algumas circunstâncias, a mitigação da privacidade[178] baseando-se no artigo 220[179], da Constituição Federal de 1988.

---

[174] OLIVEIRA, James Eduardo. *Código Civil anotado e comentado*: doutrina e jurisprudência. Rio de Janeiro: Forense, 2009. p. 15.

[175] CAVALIERI FILHO, Sergio. *Programa de responsabilidade civil.* 8 ed. São Paulo: Atlas, 2008. p. 104.

[176] Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária. [...]
Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.
Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes.
Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

[177] BITTAR, Carlos Alberto. *Os direitos da personalidade*. 7. ed. Rio de Janeiro: Forense, 2008. p. 118.

[178] MORAES, Alexandre de. *Direitos Humanos Fundamentais*: Teoria Geral. Comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil. 9 ed. São Paulo: Atlas, 2011. p. 138.

[179] Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.
§ 1º - Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.
§ 2º - É vedada toda e qualquer censura de natureza política, ideológica e artística.
§ 3º - Compete à lei federal:
I - regular as diversões e espetáculos públicos, cabendo ao Poder Público informar sobre a natureza deles, as faixas etárias a que não se recomendem, locais e horários em que sua apresentação se mostre inadequada;

A Lei nº 9.296, de 24 de julho de 1996 regulamenta o inciso XII, parte final, do art. 5º da CR/88, e versa sobre interceptação de comunicações telefônicas, de informática e telemática. No referido diploma legal, em seu art. 10º, são criminalizadas certas condutas, *in verbis*: "Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei."

Por sua vez, a Lei nº 12.527, de 18 de novembro de 2011, em seu art. 32, IV, responsabiliza o agente público no trato de informação sigilosa ou pessoal: "Art. 32. Constituem condutas ilícitas que ensejam responsabilidade do agente público ou militar: [...] IV - divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido à informação sigilosa ou informação pessoal."

A legislação ora mencionada, assim como a Lei nº 12.737, de 30 de novembro de 2012 – a qual dispõe sobre a tipificação criminal de delitos informáticos –, acaba influenciando o debate sobre a mitigação da privacidade em favor de investigações que visam a resguardar a segurança nacional. Isso ocorre porque, em grande parte, a ação preventiva de investigação e vigilância acontece ao redor do mundo por meio de mídias eletrônicas, em especial quando do trânsito de dados por redes de computadores.

Da análise dos instrumentos normativos supracitados, nota-se que a privacidade parece essencial no cenário interno, onde ela tem *status* de direito fundamental. Internacionalmente a privacidade também é objeto de discussões e tratados. A Declaração Universal dos Direitos do Homem de 1948 prevê o respeito à privacidade, e protege as pessoas contra o próprio Estado de forma evidente, em conformidade com seu artigo 12[180].

---

II - estabelecer os meios legais que garantam à pessoa e à família a possibilidade de se defenderem de programas ou programações de rádio e televisão que contrariem o disposto no art. 221, bem como da propaganda de produtos, práticas e serviços que possam ser nocivos à saúde e ao meio ambiente.
§ 4º - A propaganda comercial de tabaco, bebidas alcoólicas, agrotóxicos, medicamentos e terapias estará sujeita a restrições legais, nos termos do inciso II do parágrafo anterior, e conterá, sempre que necessário, advertência sobre os malefícios decorrentes de seu uso.
§ 5º - Os meios de comunicação social não podem, direta ou indiretamente, ser objeto de monopólio ou oligopólio.
§ 6º - A publicação de veículo impresso de comunicação independe de licença de autoridade.

[180] Art. 12. Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei, contra tais interferências ou ataques.

Note-se que as intromissões negadas são as arbitrárias. Ademais percebe-se o viés de conquista civilizatória ao se mencionar a proteção, mesmo que contrarie o Estado, em favor da honra, reputação, família, domicilio, correspondência. A eventual agressão a tal conquista deve ser algo muito estudado, responsável, razoável e proporcional aos objetivos de bem comum que a comunidade almeja no sentido de sua própria sobrevivência.

Em 1992, promulgava-se e entrava em vigor no Brasil o Pacto Internacional sobre os Direitos Civis e Políticos, de 1966. Em seu artigo 17, o referido diploma internacional declara que:

> 1. Ninguém será objeto de intervenções arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de atentados ilegais à sua honra e à sua reputação.
> 2. Toda e qualquer pessoa tem direito à proteção da lei contra tais intervenções ou tais atentados.

O Pacto Internacional sobre os Direitos Civis e Políticos, de 1966 segue tutelando os mesmos bens jurídicos já previstos na Declaração Universal dos Direitos do Homem, ratificando a importância da conquista neles retratados. A privacidade não pode ser um direito de segunda categoria. Mitigá-la deve ser justificado apenas e tão somente em favor da preservação de outros direitos essenciais para a vida comunidade.

No mesmo sentido, o Comitê dos Direitos Humanos, em seu Comentário Geral nº 16[181], adotado na 32.ª sessão, de 1988, discorre sobre a sua interpretação do artigo *supra*citado opinando que a vigilância eletrônica deve ser evitada e a privacidade deve

[181] Mesmo em relação a interferências que estejam em conformidade com o Pacto, a legislação relevante deve **especificar em pormenor as circunstâncias precisas em que tais interferências são permitidas**.
A decisão da admissão de uma tal interferência é tomada exclusivamente pela autoridade designada nos termos da lei e analisada caso a caso. O cumprimento do art. 17 exige que se garantam, 'de jure' e 'de facto', a integridade e a confidencialidade da correspondência.
**Deve proibir-se a vigilância, seja eletrônica ou de outra forma, as interceções telefônicas, telegráficas ou através de outras formas de comunicação, as escutas telefônicas e a gravação de conversas**. As buscas domiciliárias devem restringir-se a buscas de provas necessárias e não devem permitir-se se constituírem uma perseguição. A recolha e conservação de informações pessoais em computadores, bases de dados e outros dispositivos, seja por autoridades públicas ou por particulares ou organismos, devem ser reguladas por lei. **Os Estados têm de adotar medidas eficazes para garantirem que as informações sobre a vida privada de uma pessoa não cheguem às mãos de pessoas que não estejam autorizadas por lei para as receberem, processarem e usarem e que nunca sejam usadas para fins incompatíveis com o Pacto.** Cada indivíduo deve também poder saber quais as autoridades públicas, pessoas singulares ou entidades privadas que controlam ou que podem vir a controlar os seus ficheiros. Se os ficheiros contiverem dados pessoais incorretos ou se tiverem sido recolhidos ou processados de forma contrária à lei, cada indivíduo deve ter o direito de pedir a sua retificação ou eliminação[181]. (grifo nosso)

ser garantida, como deve ser garantido que sua violação se dará somente por pessoas autorizadas e na forma da Lei.

Também para fazer cumprir tais opções legislativas em ambiente cibernético, o pugilato na rede financiado pela sociedade pode se mostrar uma útil ferramenta. Garantir que informações privadas não sejam manipuladas por quem não está autorizado para tal é objetivo com o qual a defesa cibernética pode contribuir; no entanto, é esperado em tal situação, que pessoas autorizadas a manipular dados que trafegam na rede de computadores tenham que fazê-lo para que o ambiente esteja mais seguro. Por vezes, a referida vigilância pode ser realizada sem que haja, como regra, intervenção humana, mas realizada eletronicamente.

As Diretrizes da Organização para a Cooperação e Desenvolvimento Econômicos (OCDE) para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, adotadas em 23 de setembro de 1980, oferecem princípios referentes à coleta e gerenciamento de dados pessoais, quais sejam: princípio de limitação da coleta, princípio da qualidade dos dados, princípio de definição da finalidade, princípio de limitação de utilização, princípio do *back-up* de segurança, princípio de abertura, princípio de participação do indivíduo, princípio de responsabilização[182].

[182] OCDE. *Síntese Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais*. Disponível em: <http://www.oecd.org/sti/ieconomy/15590254.pdf>. Acesso em: 15 fev. 2015. Os princípios estão assim descritos: "7.**Princípio de limitação da coleta**: a coleta de dados pessoais deveria ser limitada e qualquer desses dados deveria ser obtido através de meios legais e justos e, caso houver, informando e pedindo o consentimento do sujeito dos dados. 8.**Princípio de qualidade dos dados**: os dados pessoais deveriam ser relacionados com as finalidades de sua utilização e, na medida necessária, devem ser exatos, completos e permanecer atualizados. 9.**Princípio de definição da finalidade**: os propósitos da coleta de dados pessoais devem ser indicadas no momento da coleta de dados ao mais tardar e o uso subsequente limitado à realização destes objetivos ou de outros que não sejam incompatíveis e que sejam especificados cada vez que mudar o propósito. 10.**Princípio de limitação de utilização**: dados pessoais não deveriam ser divulgados, comunicados ou utilizados com finalidades outras das que foram especificadas de acordo com o Parágrafo 9, salvo : 1. com o consentimento do sujeito dos dados; ou 2. por força de lei. 11.**Princípio do *back-up* de segurança**: back-up de segurança regulares deveriam proteger os dados pessoais contra riscos tais como perda, ou acesso, destruição, uso, modificação ou divulgação desautorizados de dados. 12.**Princípio de abertura**: deveria haver uma política geral de abertura a respeito do desenvolvimento, da prática e da política referentes a dados pessoais. Deveriam estar prontamente disponíveis meios de estabelecer a existência e natureza de dados pessoais, as finalidades principais de seu uso, bem como a identidade e residência habitual do controlador de dados. 13.**Princípio de participação do indivíduo**: um indivíduo deveria ter o direito de: 1. obter do controlador de dados, ou por outro meio, a confirmação de que este possui ou não dados referentes a ele; 2. de que lhe sejam comunicados dados relacionados a ele [...]; 3. obter explicações caso for rejeitado um pedido feito conforme o disposto nos subparágrafos 1 e 2, e ter meios de contestar tal recusa; e 4. contestar dados relacionados a ele e, se a contestação for recebida, pedir que os dados sejam apagados, retificados, completados ou modificados. 14. **Princípio de responsabilização**: o

Respeitando os princípios elencados em tais diretrizes, a obtenção de dados por meios legais e justos estaria inserida no princípio de limitação da coleta; o princípio da qualidade dos dados relaciona que os dados privados devem ser utilizados, apenas e tão somente, na medida da necessidade e para a finalidade determinada. O princípio da definição da finalidade, destarte, oferece suporte para o princípio da qualidade dos dados, pois os propósitos das coletas de dados privados devem ser indicados, respeitados, e sempre que os propósitos forem modificados, tal fato deve ser especificado. Os dados coletados devem ser utilizados apenas e tão somente para a finalidade determinada já explicitada, salvo com consentimento do sujeito dos dados ou por força legal – trata-se do princípio de limitação de utilização.

Por sua vez, o princípio do *back-up* de segurança deveria proteger dados pessoais contra riscos, no entanto o *back-up* de segurança rotineiro pode acarretar na facilitação do acesso indevido a dados pessoais. Para que uma conduta realizada evite riscos e não se redunde no seu aumento ao sujeito dos dados, deve-se realizar um juízo de conveniência e oportunidade a fim de que os bens jurídicos tutelados pelo princípio não sejam prejudicados. O princípio da abertura fomenta políticas públicas voltadas a manipulação dos dados pessoais. Possui grande relação com o princípio de participação do indivíduo, pois se trata de um ponto que também depende de regulação. Por fim, pelo princípio de responsabilização, a sociedade poderá dispor de meios mais eficazes para que a forma e efeitos da coleta e processamento de dados privados aconteçam exatamente da forma que a sociedade espera.

O documento supracitado de 1980, que deveria representar um consenso entre Estados sobre o tema, prevê a cooperação entre os países visando a facilitar a troca de informações. Por certo, estas diretrizes não são seguidas por países mais desenvolvidos, conforme indícios apresentados pelo jornalista Glenn Greenwald[183] quando se refere a Edward Snowden e à NSA, ou ainda pelo sítio do wikileaks[184]. A motivação parece lógica: a coleta limitada e a limitação temporal para guarda de informações dificultaria a análise de dados.

---

controlador de dados terá de prestar contas pela observância das medidas que dão efeito aos princípios acima indicados." (grifo nosso)

[183] GREENWALD, Glenn. *Sem Lugar para se Esconder*. Trad. Fernanda Abreu. Rio de Janeiro. Sextante, 2014.

[184] wikileaks.org, consultado em 26.06.14.

O princípio da abertura, caso fosse seguido, acarretaria em evidente comprometimento de eventuais investigações. Em outras palavras, o consenso conseguido por meio da OCDE parece não condizer com a realidade fática ante a necessidade de que o terrorismo seja combatido. Em outras palavras, a escolha nacional deve, ao mesmo tempo, sustentar coerência e analisar a realidade que não pode ser mudada, para que a escolha nacional não signifique fonte prejuízo social.

Privilegiar a privacidade, ignorando o que acontece em outros países centrais, pode desaguar na dicotomia do legal e do fático, pois o processamento de dados privados por meios cibernéticos continuará ocorrendo a despeito da norma legal brasileira, ainda que digam respeito a dados coletados exclusivamente no Brasil.

Por outro modo, pode-se dizer que mesmo que o ordenamento jurídico brasileiro aparentemente coloque o direito à privacidade como garantia absoluta – uma vez que a CR/88 fala de inviolabilidade da intimidade e da vida privada –, realidades como o terrorismo tendem a mitigar consideravelmente aquilo que fora concebido durante a constituinte de 1988, suscitando uma reinterpretação das normas. Para tanto, faz-se necessário o aval da própria sociedade, que precisa de segurança e estabilidade para fruir de melhor qualidade de vida. Tal constatação tende a se refletir na jurisprudência.

### *2.1.3 A privacidade sob a óptica jurisprudencial*

A fim de selecionar os julgados mais relevantes para a presente pesquisa, realizou-se pesquisa documental no sítio LEXML (rede de informação legislativa e jurídica). Esta ferramenta constitui-se de um portal de informações jurídicas de destaque no Brasil. As palavras chave utilizadas foram “privacidade”, “privacidade caráter absoluto”, “privacidade dados”, “quebra sigilo”, “sigilo de dados”.

A partir do retorno das pesquisas, foram eleitos julgados que sintetizassem o entendimento dos tribunais sobre os pontos de interesse, tendo-se chegado aos julgados *infra*.

Em acórdão proferido em 2006 por ocasião do RE 418416 / SC[185], o Supremo Tribunal Federal (STF) posicionou-se no sentido de que a norma protetiva

[185] EMENTA: (...) II. Quebra de sigilo bancário: prejudicadas as alegações referentes ao decreto que a determinou, dado que a sentença e o acórdão não se referiram a qualquer prova resultante da quebra do sigilo bancário, tanto mais que, dado o deferimento parcial de mandado de segurança, houve a devolução da documentação respectiva. (...) IV - Proteção constitucional ao sigilo das comunicações

constitucional que trata da tutela à privacidade diz respeito à comunicação de dados, mas não aos dados em si, mesmo quando armazenados. Mitigou-se, pois, a proteção que poderia ter abrangido a interpretação da norma, sinalizando com a possibilidade de proteção menos abrangente da privacidade.

Por sua vez, o Tribunal Regional Federal (TRF) 1ª Região, 3ª Turma, no HC nº 2007.01.00.003265-4/DF[186], também tratou da privacidade de dados em seu julgado. Concluiu que o conhecimento de dados cadastrais, aí incluso o endereço eletrônico, quando de tais dados não se pode concluir sobre o modo de viver ou status da pessoa, não atinge a intimidade ou vida privada. Outras decisões como a Apelação nº 2003.71.00.028192-4/RS, TRF 4ª Região, 7ª Turma, seguiram o mesmo sentido, e o

---

de dados - art. 5º, XVII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial e a conseqüente ofensa da garantia da inviolabilidade do domicílio da empresa - este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação do art. 5º. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve "quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial". 4. **A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador.** (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270). V - Prescrição pela pena concretizada: declaração, de ofício, da prescrição da pretensão punitiva do fato quanto ao delito de frustração de direito assegurado por lei trabalhista (C. Penal, arts. 203; 107, IV; 109, VI; 110, § 2º e 114, II; e Súmula 497 do Supremo Tribunal). (grifo nosso)

[186] HABEAS CORPUS. TRANCAMENTO AÇÃO PENAL. IMPOSSIBILIDADE. DADOS CADASTRAIS DE E-MAIL. REQUISIÇÃO AUTORIDADE POLICIAL. ORDEM JUDICIAL. DESNECESSIDADE. INEXISTÊNCIA DE OFENSA AO DIREITO FUNDAMENTAL À PRIVACIDADE.
I. O resguardo do sigilo de dados, genericamente considerado, possui, como garantia que é, função instrumental, no sentido de viabilizar a efetiva realização de direitos individuais relativos à incolumidade da intimidade e da vida privada. Isso significa dizer que a garantia, conceitualmente, por si só, não tem qualquer sentido satisfatório, sendo antes uma projeção do direito cuja tutela instrumentaliza (STF, MS 23452 / RJ - RIO DE JANEIRO, Rel. Min. Celso de Melo). Nesse contexto, o campo de manifestação da garantia informa-se exatamente pela latitude da necessidade de tutela do direito, a entendermos, conseguintemente, que não se cogitando de ameaça ou efetiva lesão ao direito à intimidade e vida privada, igualmente não se pode cogitar em garantia de sigilo de dados.
**II. O conhecimento de dados meramente cadastrais, inclusive de e-mail, quando disso não se extrapola para a dimensão de informações sobre o status ou modus vivendi da pessoa, não atinge a intimidade ou a vida privada de alguém, não estando submetido à cláusula de reserva de jurisdição. Licitude da prova produzida nesses termos.**
III. Para o recebimento da denúncia é suficiente que ela conduza indicação do delito com as suas circunstâncias e demonstração dos indícios de autoria (e a não ocorrência das demais hipóteses do art. 43 do CPP), permitindo o exercício amplo da defesa.
IV. Sendo facultado ao réu, na fase de inquérito, o conhecimento dos atos de investigação não há que se falar em desatendimento ao princípio da ampla defesa.
V. Meras irregularidades do inquérito não contaminam a ação penal.
VI. Ordem que se denega. (grifo nosso)

entendimento majoritário é de que não acarreta violação de privacidade a requisição de dados, mesmo cadastrais.

Na jurisprudência brasileira, pode-se perceber uma confusão entre os conceitos de intimidade e vida privada, o que converge com a proposição de Danilo Doneda, que cita em sua obra:

> Recurso Especial nº 306570/SP, rel. Min. Eliana Calmon (D.J. 18/02/2002, p. 340): "O contribuinte ou o titular da conta bancária tem direito à privacidade em relação aos seus dados pessoais (...)"; [e] o Recurso Especial nº 58101/SP, rel. Min. César Asfor Rocha (D.J. 09/03/1998, p. 326): "É certo que não se pode cometer o delírio de, em nome do direito à privacidade, estabelecer-se uma redoma protetora em torno de uma pessoa para torná-la imune de qualquer veiculação atinente a sua imagem"[187]

Sobre essa confusão conceitual, há que considerar que vida privada é conceito que muda no tempo e no espaço. Trata-se de direito que pode se impor contra outra pessoa ou mesmo contra o próprio Estado. A Carta de 1824 associava o conceito de vida privada à inviolabilidade do domicílio, ainda que de forma implícita, sendo tal conceito reforçado na carta de 1891. Até a Constituição da República de 1988, as demais foram seguindo com a mesma concepção[188].

Independentemente da confusão anotada *supra*, o que se evidencia na jurisprudência é que a privacidade não é tomada como um direito prioritário em muitos casos, menos ainda absoluto. Segundo Müller, nenhum direito fundamental pode ser garantido de forma ilimitada[189]. Nesse sentido, uma quantidade considerável de julgados sobre privacidade tem reforçado a tese de que não se trata de um direito absoluto.

O Acórdão nº 388011 do Processo nº 20090020120351RCL[190]. Tribunal de Justiça do Distrito Federal e dos Territórios. 1ª Turma Criminal, traz uma afirmação de

---

[187] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 112.

[188] NASCIMENTO, Aline Tiduco Hossaka Molette. *Direito à vida privada e à intimidade do portador do HIV e sua proteção no ambiente de trabalho*. Curitiba: UFPR, 2009. Disponível em: <http://dspace.c3sl.ufpr.br/dspace/handle/1884/31089?show=full>. Acesso em: 26 jun. 2014.

[189] MÜLLER, Friedrich. In: ALEXY, Robert. *Teoría de los Derechos Fundamentales*. Madrid: CEPC, 2001. p. 310.

[190] EMENTA: RECLAMAÇÃO - MINISTÉRIO PÚBLICO - **INTERCEPTAÇÃO TELEFÔNICA - DIREITO À INTIMIDADE E À PRIVACIDADE - CARÁTER RELATIVO** – INTERESSE PÚBLICO - INVESTIGAÇÕES POLICIAIS - ELUCIDAÇÃO DE ESTELIONATO -

grande interesse para as discussões sobre a extensão do direito à privacidade, afirmando categoricamente que os direitos à privacidade e à intimidade não são absolutos, visto que devem considerar o interesse da sociedade. O referido julgado ainda remete ao princípio da proporcionalidade. Fica então a questão se seria proporcional mitigar a privacidade em favor do combate ao terrorismo. Por certo, o combate ao terrorismo é de interesse social, mas o preço a pagar por ele não é questão pacífica.

O habeas corpus do Superior Tribunal de Justiça (STJ) HC 8317 / PA – STJ, 6ª Turma[191], também trata de privacidade, desta vez no que tange a dados bancários. O Acórdão admite que o sigilo bancário que decorre do direito à privacidade (em sentido lato) tem sido mitigado por doutrina e jurisprudência em hipóteses de inquérito policial e quando se tratar de processo penal.

Na sequência, destaca-se o acórdão proferido no REsp 595600 / SC – STJ[192], 4ª Turma, que tratou da auto exposição livre e consciente de pessoas em rede de computadores, por vezes tornando públicos detalhes íntimos. Se alguém expõe a imagem voluntariamente em ambiente público, não poderá reivindicar privacidade diante da exposição voluntária. Esta decisão possui importância especial pois para as

---

PROPORCIONALIDADE. I. **O DIREITO À INTIMIDADE E À PRIVACIDADE NÃO POSSUEM CARÁTER ABSOLUTO. CEDE ESPAÇO AO INTERESSE DA SOCIEDADE.** II. O JUIZ DEVE ESTAR ATENTO ÀS CIRCUNSTÂNCIAS ESPECÍFICAS DE CADA CASO. PAUTADO NA PROPORCIONALIDADE, DEVE JUSTIFICAR A ADMISSIBILIDADE OU NÃO DA INTERCEPTAÇÃO TELEFÔNICA. III. RECLAMAÇÃO PROVIDA. (grifo nosso)

[191] EMENTA: HABEAS CORPUS. QUEBRA DE SIGILO BANCÁRIO. ADMISSIBILIDADE. 1 - A idoneidade do habeas corpus como meio de afastar constrangimento decorrente da violação do **sigilo bancário, desdobramento do direito à intimidade e à privacidade, que, por sua vez compreende-se no campo mais amplo do direito à liberdade, consoante autorizada doutrina, vem sendo admitida pela jurisprudência quando se tratar de processo penal ou inquérito policial.** 2 - Ordem concedida dada a carência de fundamentação do despacho impositivo da violação do sigilo bancário sem indicar elementos mínimos de prova quanto à autoria do delito. Decisão Vistos, relatados e discutidos estes autos, acordam os Ministros da Sexta Turma do Superior Tribunal de Justiça, na conformidade dos votos e das notas taquigráficas a seguir, por unanimidade, conceder a ordem de habeas corpus para declarar a insubsistência da decisão autorizativa da quebra do sigilo bancário do paciente. Votaram com o Ministro-Relator os Ministros Hamilton Carvalhido, Vicente Leal, William Patterson e Fontes de Alencar. (grifo nosso)

[192] EMENTA: DIREITO CIVIL. DIREITO DE IMAGEM. TOPLESS PRATICADO EM CENÁRIO PÚBLICO. Não se pode cometer o delírio de, em nome do direito de privacidade, estabelecer-se uma redoma protetora em torno de uma pessoa para torná-la imune de qualquer veiculação atinente a sua imagem. **Se a demandante expõe sua imagem em cenário público, não é ilícita ou indevida sua reprodução pela imprensa, uma vez que a proteção à privacidade encontra limite na própria exposição realizada.** Recurso especial não conhecido. Decisão Vistos, relatados e discutidos os autos em que são partes as acima indicadas, acordam os Srs. Ministros da Quarta Turma do Superior Tribunal de Justiça, na conformidade dos votos e das notas taquigráficas a seguir, por unanimidade, não conhecer do recurso, nos termos do voto do Sr. Ministro Relator. Votaram com o Relator os Srs. Ministros Fernando Gonçalves, Aldir Passarinho Junior e Barros Monteiro. Ausente, justificadamente, o Sr. Ministro Sálvio de Figueiredo Teixeira. (grifo nosso)

coletas de dados necessários para a defesa cibernética eficaz, também importam dados voluntariamente tornados públicos.

Na hipótese abordada pelo julgado em estudo, é difícil pleitear a tutela jurisdicional pela privacidade tendo em vista os riscos a que o indivíduo se submeteu voluntariamente.

Também o Superior Tribunal Militar (STM) confirmou o entendimento de que a quebra de sigilo bancário de pessoa investigada por crime não se confunde com invasão de privacidade, como se pode verificar no MS - 1997.01.000360-6 / RJ – STM[193], Plenário. No julgado, o STM conclui o mesmo que o STJ no HC 8317 / PA – STJ, 6ª Turma, já abordado no que se relaciona com sigilo bancário de investigado.

Ao julgar o HC 76203 / SP[194], a 2ª Turma do STF discutiu a contaminação do processo penal devido a possível ilegalidade decorrente de violação do direito à privacidade. Concluiu que por conta de apreensão de entorpecentes, já é possível a escuta telefônica, mesmo que dela não seja deflagrada ação penal. De tal entendimento se pode aduzir que com muito mais razão se pode mitigar a privacidade face a uma ameaça potencial à segurança nacional, principalmente com robusta justificativa.

Em outra oportunidade, a 2ª Turma do STF reitera a relatividade do direito à privacidade. O RE 219780 / PE[195] mostra-se bastante proveitoso para o debate, uma vez que são citados alguns dos pontos onde a privacidade deve ceder. Para a referida turma, a privacidade cede diante do interesse público e interesse social, desde que observado o

---

[193] EMENTA: MANDADO DE SEGURANÇA. Quebra de sigilo bancário. Aplicação da Lei nº 4.595/64, Art. 38. Representação do Encarregado do IPM. **A quebra do sigilo bancário de pessoas sob investigação não se confunde com invasão de privacidade protegida pela Constituição.** Embora medida excepcional, pode o Juiz determiná-la, em atendimento à Representação do Encarregado do IPM assumida pelo RMPM. O Mandado de Segurança é mesmo o instrumento processual próprio para a Defesa atacar a decisão que pretende seja revogada. Mandado de Segurança indeferido, por falta de amparo legal. Decisão por maioria. (grifo nosso)

[194] EMENTA: HABEAS CORPUS. PROCESSO PENAL. ESCUTA TELEFÔNICA. OUTROS MEIOS DE PROVA. LICITUDE. Escuta telefônica que não deflagra ação penal, não é causa de contaminação do processo. **Não há violação ao direito à privacidade quando ocorre apreensão de droga e prisão em flagrante de traficante.** Interpretação restritiva do princípio da árvore dos frutos proibidos. Habeas corpus indeferido. (grifo nosso)

[195] EMENTA: CONSTITUCIONAL. SIGILO BANCÁRIO: QUEBRA. ADMINISTRADORA DE CARTÕES DE CRÉDITO. CF, art. 5º, X. I. – Se é certo que o **sigilo bancário, que é espécie de direito à privacidade, que a Constituição protege art. 5º, X, não é um direito absoluto, que deve ceder diante do interesse público, do interesse social e do interesse da Justiça, certo é, também, que ele há de ceder na forma e com observância de procedimento estabelecido em lei e com respeito ao princípio da razoabilidade.** No caso, a questão foi posta, pela recorrente, sob o ponto de vista puramente constitucional, certo, entretanto, que a disposição constitucional é garantidora do direito, estando as exceções na norma infraconstitucional. II. - R.E. não conhecido. (grifo nosso)

princípio da razoabilidade. Note-se que o pugilato cibernético financiado pelo Estado pretende tutelar exatamente o interesse público e o interesse social em última análise, afinal, o Estado em uma democracia deve servir a comunidade.

Finamente, no HC 89083 / MS[196], a 1ª Turma do STF afirma que, em que pese a regra da preservação da privacidade, é possível o acesso a dados, inclusive sigilosos, para instrução criminal. Seria interessante refletir sobre as possibilidades desse entendimento face à ameaça potencial de ataque terrorista, e ainda considerando que a privacidade no Brasil, ao que parece, tem sido violada por agências de inteligência internacionais, conforme informações já citadas quando se abordou Edward Snowden e o sítio wikileaks.

Percebe-se, pois, que a interpretação jurisprudencial tem mitigado a privacidade em razão da realidade social, e quase sempre tal interpretação tem sido entendida e aceita pela comunidade em razão do foco ser o bem comum. Com vistas à preservação dos valores mais caros à democracia, a sociedade aparentemente tem recebido a mitigação da privacidade como medida necessária para preservar outros direitos e valores. Mesmo que esta seja a decisão presente da sociedade, é preciso cautela, pois o risco, como já demonstrado, também pode ter origem na vigilância em prol da segurança. Equilibrar as conquistas sociais é muito importante, até para que nenhuma delas se perca. A privacidade e a vida em comunidade para cooperação mútua são conquistas a serem preservadas. O grande critério de ponderação entre privacidade e segurança é a razoabilidade, a proporcionalidade e os objetivos a serem alcançados pela sociedade.

O Supremo, como os demais tribunais tem envidado esforços para que o interesse social prepondere sobre o interesse individual, sem que, no entanto, o direito à privacidade seja tratado como um direito secundário. Trata-se de uma conquista civilizatória. O melhor critério para ponderação entre a privacidade e a segurança

---

[196] EMENTA: COMPETÊNCIA PENAL - PRERROGATIVA DE FORO - EXTENSÃO - CO-RÉUS - IMPROPRIEDADE. A competência do Superior Tribunal de Justiça está delimitada na Constituição Federal, não sofrendo alteração considerados institutos processuais comuns - a conexão e a continência. Precedentes do Plenário: Habeas Corpus nº 91.273-7/RJ, acórdão divulgado no Diário da Justiça Eletrônico de 31 de janeiro de 2008, Habeas Corpus nº 89.056-3/MS, acórdão veiculado no Diário da Justiça Eletrônico de 2 de outubro de 2008, ambos de minha relatoria, e Inquérito nº 1.720-5/RJ, acórdão publicado no Diário da Justiça de 14 de dezembro de 2001, relatado pelo ministro Sepúlveda Pertence. SIGILO DE DADOS - QUEBRA - INDÍCIOS. **Embora a regra seja a privacidade, mostra-se possível o acesso a dados sigilosos, para o efeito de inquérito ou persecução criminais e por ordem judicial**, ante indícios de prática criminosa. (grifo nosso)

cibernética baseia-se na necessidade que uma comunidade tem de se desenvolver e prosperar; haja vista as decisões mencionadas, que tem privilegiado o interesse social e o interesse público.

### *2.1.4 Estudo de caso: ADI 3059 MC / RS*

Um julgado relacionado à utilização de *software* livre que merece destaque especial neste trabalho é a Ação Direta de Inconstitucionalidade (ADI) 3059 do Rio Grande do Sul, cujo relator foi o Ministro Carlos Ayres Britto. Far-se-á uma breve análise do julgado, relacionando a decisão com aspectos de interesse para o pugilato cibernético.

A ementa[197] da medida cautelar referente a ADI discorre sobre a utilização de *softwares* livres ou sem restrições proprietárias. O Rio Grande do Sul instituiu, no âmbito da Administração Pública sul-rio-grandense, por meio de Lei estadual a preferência na utilização desta modalidade de *software*. O referido ato normativo impugnado por uma agremiação partidária, do ponto de vista da técnica de defesa cibernética, favorece a defesa cibernética do estado.

O acórdão de 2004 deferiu o pedido cautelar, sustando os efeitos da Lei n° 11.871, de 19 de dezembro de 2002[198], do Estado do Rio Grande do Sul. A Lei, em seus

---

[197] Medida cautelar em ação direta de inconstitucionalidade. Legitimidade de agremiação partidária com representação no congresso nacional para deflagrar o processo de controle de constitucionalidade em tese. Inteligência do art. 103, inciso VIII, da Magna Lei. Requisito da pertinência temática antecipadamente satisfeito pelo requerente. Impugnação da Lei n° 11.871/02, do estado do Rio Grande do Sul, que instituiu, no âmbito da Administração Pública sul-rio-grandense, a preferencial utilização de *softwares* livres ou sem restrições proprietárias. Plausibilidade jurídica da tese do autor que aponta invasão da competência legiferante reservada à União para produzir normas gerais em tema de licitação, bem como usurpação competencial violadora do pétreo princípio constitucional da separação dos poderes. Reconhece-se, ainda, que o ato normativo impugnado estreita, contra a natureza dos produtos que lhes servem de objeto normativo (bens informáticos), o âmbito de competição dos interessados em se vincular contratualmente ao Estado-administração. Medida cautelar deferida.

[198] Art. 1º. A administração pública direta, indireta, autárquica e fundacional do Estado Rio Grande do Sul, assim como os, órgãos autônomos e empresas sob o controle do Estado utilizarão preferencialmente em seus sistemas e equipamentos de informática programas abertos, livres de restrições proprietárias quanto a sua cessão, alteração e distribuição.
§ 1º - Entende-se por programa aberto aquele cuja licença de propriedade industrial ou intelectual não restrinja sob nenhum aspecto a sua cessão, distribuição, utilização ou alteração de suas características originais, assegurando ao usuário acesso irrestrito e sem custos adicionais ao seu código fonte, permitindo a alteração parcial ou total do programa para seu aperfeiçoamento ou adequação.
§ 2º - Para fins de caracterização do programa aberto, o código fonte deve ser o recurso preferencial utilizado pelo programador para modificar o programa, não sendo permitido ofuscar sua acessibilidade, nem tampouco introduzir qualquer forma intermediária como saída de um pré-processador ou tradutor.

artigos 1º a 4º, discorre que a administração sul-rio-grandense indireta, direta, fundacional e autárquica, assim como os órgãos autônomos, sociedades empresárias sob o controle do Rio Grande do Sul deveriam utilizar, preferencialmente, os referidos softwares, independente de regulamentação da Lei promulgada.

Entretanto, o mérito da ação, julgada em 2015, antes relatado pelo então Min. Carlos Ayres Britto[199], tendo como novo relator do acórdão o Ministro Luiz Fux, foi julgado improcedente[200]. O argumento de usurpação da competência da União pelo

---

§ 3º - Quando da aquisição de *softwares* proprietários será dada preferência para aqueles que operem em ambiente multiplataforma, permitindo sua execução sem restrições em sistemas operacionais baseados em *softwares* livre.
§ 4º - A implantação da preferência prevista nesta Lei será feita de forma paulatina, baseada em estudos técnicos e de forma a não gerar perda de qualidade nos serviços prestados pelo Estado.
Art. 2º - As licenças de programas abertos a serem utilizados pelo Estado deverão, expressamente, permitir modificações e trabalhos derivados, assim como a livre distribuição destes nos mesmos termos da licença do programa original.
Parágrafo Único - Não poderão ser utilizados programas cujas licenças:
I - impliquem em qualquer forma de discriminação a pessoas ou grupos;
II - sejam especificadas para determinado produto impossibilitando que programas derivados deste tenham a mesma garantia de utilização/ alteração e distribuição; e
III - restrinjam outros programas distribuídos conjuntamente.
Art. 3º - Será permitida a contratação e utilização de programas de computador com restrições proprietárias ou cujas licenças não estejam de acordo com esta Lei, nos seguintes casos:
I - quando o *software* analisado atender a contento o objetivo licitado ou contratado, com reconhecidas vantagens sobre os demais *softwares* concorrentes, caracterizando um melhor investimento para o setor público ; II - quando a utilização de programa livre e/ou código fonte aberto causar incompatibilidade operacional com outros programas utilizados pela administração direta, indireta, autárquica e fundacional do Estado, ou órgãos autônomos e empresas sob o controle do mesmo.
Art. 4º - O Estado regulamentará as condições, prazos e formas em que se fará a transição, se necessária dos atuais sistemas e programas de computador para aqueles previstos no art. 1º, quando significar redução de custos a curto e médio prazo, e orientará as licitações e contratações, realizadas a qualquer titulo, de programas de computador.
Parágrafo único - A falta de regulamentação não impedirá a licitação ou contratação de programas de computador na forma disposta na lei.

[199] O Relator do caso mudou em decorrência da aposentadoria do Min. Carlos Ayres Britto que se deu em 16 novembro de 2012.

[200] Ação Direta de Inconstitucionalidade. Direito Administrativo e Constitucional. Lei nº 11.871/02, do estado do Rio Grande do Sul, que institui, no âmbito da administração pública regional, preferência abstrata pela aquisição de softwares livres ou sem restrições proprietárias. Exercício regular de competência legislativa pelo estado-membro. Inexistência de usurpação de competência legiferante reservada à união para produzir normas gerais em tema de licitação. Legislação compatível com os princípios constitucionais da separação dos poderes, da impessoalidade, da eficiência e da economicidade. Pedido julgado improcedente.
1. A competência legislativa do Estado-membro para dispor sobre licitações e contratos administrativos respalda a fixação por lei de preferência para a aquisição de *softwares* livres pela Administração Pública regional, sem que se configure usurpação da competência legislativa da União para fixar normas gerais sobre o tema (CRFB, art. 22, XXVII).
2. A matéria atinente às licitações e aos contratos administrativos não foi expressamente incluída no rol submetido à iniciativa legislativa exclusiva do Chefe do Poder Executivo (CRFB, art. 61, §1º, II), sendo, portanto, plenamente suscetível de regramento por lei oriunda de projeto iniciado por qualquer dos membros do Poder Legislativo.
3. A Lei nº 11.871/2002 do Estado do Rio Grande do Sul não engessou a Administração Pública regional, revelando-se compatível com o princípio da Separação dos Poderes (CRFB, art. 2º), uma vez

estado do Rio Grande do Sul foi afastado, ademais a norma promulgada seria compatível com os princípios constitucionais da separação de poderes, impessoalidade, eficiência e economicidade.

A decisão foi ratificada nos seguintes termos: "O Tribunal, por unanimidade, julgou improcedente o pedido formulado na ação. Não votou o Ministro Roberto Barroso, sucessor do Ministro Ayres Britto (Relator). Redigirá o acórdão o Ministro Luiz Fux (art. 38, IV, b, RISTF)".

Em seu voto, o então Relator Fux infere considerações[201] que vão ao encontro com cuidados desejáveis no que diz respeito à segurança cibernética. Ao fim e ao cabo, o software com o código aberto evidencia a presença de códigos maliciosos, facilitando a proteção cibernética dos terminais que os utilizam. Em outras palavras, se houver algo como uma bomba lógica, tal código malicioso pode ser identificado e o código-fonte pode ser aperfeiçoado, a fim de que funcione exatamente como se deseja. Ademais, a possibilidade de acesso ao código fonte permite o estudo e aprimoramento da tecnologia nele inserida, inclusive tecnologia de segurança. Tal característica fomenta, inclusive, o desenvolvimento tecnológico nacional, tanto no meio acadêmico quanto nos demais vetores interessados em estudar o *software* "por dentro", como as indústrias de aplicativos nacionais. Na hipótese de não haver acesso ao código-fonte de determinado aplicativo, não se pode ter certeza de seu conteúdo na íntegra, carecendo de confiança em quem o fez. Se o código-fonte disponibilizado for um código comentado[202], melhor

---

que a regra de precedência abstrata em favor dos *softwares* livres pode ser afastada sempre que presentes razões tecnicamente justificadas.
4. A Lei nº 11.871/2002 do Estado do Rio Grande do Sul não exclui do universo de possíveis contratantes pelo Poder Público nenhum sujeito, sendo certo que todo fabricante de programas de computador poderá participar do certame, independentemente do seu produto, bastando que esteja disposto a celebrar licenciamento amplo desejado pela Administração.
5. Os postulados constitucionais da eficiência e da economicidade (CRFB, arts. 37, caput e 70, caput) justificam a iniciativa do legislador estadual em estabelecer a preferência em favor de *softwares* livres a serem adquiridos pela Administração Pública.
6. Pedido de declaração de inconstitucionalidade julgado improcedente.

[201] "Vê-se, pois, que a diferença entre *software* "livre" e software "proprietário" não está em nenhuma qualidade intrínseca de qualquer das duas tipologias de programa, porém no que toca à licença de uso. O *software* é "livre", quando o detentor do respectivo direito autoral repassa ao usuário o código-fonte do programa, permitindo que este seja livremente estudado, adaptado, alterado, distribuído, etc. E não foi outra a definição de *software* livre que adotou a Lei nº 11.871/2002, do Estado do Rio Grande do Sul. [...]"

[202] O código-fonte comentado é aquele que possui comentários dos programadores sobre os comandos, o que facilita sua compreensão por pessoal especializado. Os conceitos utilizados neste tópico são os mesmos adotados pelo julgado em análise, que sempre que possível adota os conceitos da norma brasileira.

será para aqueles que desejam maior transparência e entendimento dos comandos do programa.

Seguindo em seus argumentos, o relator, no item 21 do relatório trata de disponibilização do código-fonte do programa e de concorrência de pequenas empresas. No item 22, fala de patentes tecnológicas, as quais alguns Estados não detêm por não possuírem pleno desenvolvimento de determinadas tecnologias de interesse; em seguida, é citado o incremento das oportunidades de emprego para a população e as oportunidades oferecidas para pequenas e médias empresas. No item 23, discorre que a utilização de *software* livre pode se mostrar como uma política de incentivo ao desenvolvimento científico e tecnológico regional que se compatibiliza com a Política Nacional de Informática de que trata a Lei nº 7.232, de 29 de outubro de 1984, e também compatível com a política pública expressa no inciso II do art. 3° da Constituição da República. Os itens 24 e 26 ratificam o uso e manipulação dos códigos-fonte dos *softwares* livres como uma forma de aquisição do conhecimento[203].

---

[203] "21. Amadurecida a reflexão desde o julgamento da medida cautelar, hoje estou convencido de que a resposta é negativa. Isto porque todos os que hajam desenvolvido um *software* e que tenham interesse em contratar com a Administração Pública podem se adequar à preferência legal. Basta que disponibilizem o código-fonte do programa. Podem concorrer desde as conhecidas multinacionais estrangeiras até as pequenas empresas brasileiras, sem que a preferência por um *software* "livre" seja obstáculo a nenhuma delas. Quando a Administração Pública instaura um processo licitatório para a aquisição de um programa de computador, pretende, na verdade, adquirir a licença de uso de um *software*, quase sempre acompanhada do suporte técnico para o efetivo funcionamento do programa nos sistemas e computadores da Administração. Ora, estabelecer preferência pelo *software* "livre" nada mais é do que escolher o tipo de licenciamento que melhor atenda às necessidades públicas (lembre-se: a diferença entre o *software* "livre" e o *software* "proprietário" não está no programa em si, mas no tipo de licença de uso). E o fato é que a Constituição Federal permite à Administração Pública ditar as especificações técnicas do produto a ser adquirido, nos termos da parte final do inciso XXI do art. 37 da CF [...]
22. [...] Como realçou o Advogado-Geral da União, "a migração dos sistemas de informação do setor público para *softwares* livres aumenta a demanda desses programas, gerando, no âmbito dos Estados, especialmente daqueles em desenvolvimento e que não detêm patentes tecnológicas, um incremento das oportunidades de emprego para a população. Como já anotado, notabiliza-se que pequenas e médias empresas passam a concorrer em igualdade de condições com as grandes multinacionais, detentoras dos registros de programas proprietários". Acresço: num mercado sabidamente concentracionário de poder em poucas empresas multinacionais, a utilização preferencial do *software* livre acaba por abrir com mais generosidade o leque de opções à Administração Pública e assim ampliar o próprio âmbito dos competidores.[...]
23. O que subjaz à lei impugnada é, em rigor, uma política de incentivo ao desenvolvimento científico e tecnológico regional. Política em tudo compatível com o objetivo fundamental que se lê no inciso II do art. 3° da Constituição. Política pública regional que afina com a "Política Nacional de Informática" de que trata a Lei n° 7.232/84. Iniciativa, enfim, viabilizadora da "autonomia tecnológica do País" (art. 219 da CF). [...]
24. Daqui se segue que o estabelecimento de preferência pela utilização de programas abertos de computador nos órgãos e entidades da Administração Pública consiste em saudável e natural política pública em tema de natureza administrativa. Nessa medida, não se confunde com indevida limitação da discricionariedade do administrador. [...]

Em síntese, pode-se afirmar que no que tange às observações constantes do relatório, nota-se a pertinência das considerações feitas e a compatibilidade com a natureza técnica do assunto. Os códigos-fonte disponibilizados nos *softwares* livres – que podem inclusive vir com comentários de programadores que facilitam a compreensão dos comandos – fomentam o pleno desenvolvimento das tecnologias envolvidas, incrementam as oportunidades de empregos de maior qualidade para a população, oferecem oportunidades extras para pequenos e médios empreendedores, o que pode gerar um volume maior de impostos recolhidos em favor da comunidade. Materializa, pois, uma política pública expressa em Leis e na Constituição.

O acerto da decisão do STF pode ser ratificado pela oportunidade de se gerar fomento ao desenvolvimento de novas tecnologias, emprego e renda. A decisão proferida fomenta ainda a segurança, aspecto principal deste trabalho, favorecendo a atuação do Estado no pugilato cibernético, tanto pela utilização de *softwares* mais seguros por serem conhecidos "por dentro", como pelo fomento à especialização de talentos humanos que podem auxiliar no combate às ilegalidades no mundo virtual.

## 2.2 Os limites entre o direito à privacidade e o pugilato cibernético

Os limites entre o direito à privacidade e a vigilância típica do pugilato cibernético devem ser buscados tendo como parâmetros a necessidade da sociedade por segurança e a realidade vivida na internet. A medida da necessidade pode ser um guia, mas se deve considerar até que ponto a privacidade já é mitigada em relação aos demais atores e o que se pode fazer a respeito.

Em nome da estabilidade das relações sociais, devem ser seguidas regras jurídicas também no mundo virtual. A segurança jurídica pode melhorar a qualidade de vida e corroborar com o progresso do Estado. Tendo em vista a dificuldade de fazer valer a jurisdição no mundo virtual, em algumas situações, a melhor forma de assegurar o cumprimento das normas pode ser a defesa técnica – no caso, a defesa cibernética –

---

26. Sucede que, aprofundando a análise da medida cautelar, tenho que existe, sim, um atributo do *software* "livre" que justifica a preferência estabelecia em lei: a aquisição do conhecimento. Quando a Administração Pública visa a adquirir um programa de computador, a proposta mais vantajosa será, quase sempre, aquela que lhe permita não somente usar o *software*, como também conhecer e dominar sua tecnologia. Isto tanto para viabilizar futuras adaptações e aperfeiçoamentos quanto para avaliar a real segurança das informações públicas. Tendo em vista essas específicas necessidades do Poder Público, pode-se afirmar, então, que o *software* "livre" é, a princípio, mais vantajoso, devendo, portanto, ter preferência em relação ao *software* "proprietário".

dos bens tutelados pelo Direito. O pugilato cibernético bem conduzido pode ser uma solução quando o que está em jogo é a segurança nacional. Segundo João Gabriel Álvares, "a defesa cibernética [...] se mostra como importante instrumento que, em última análise, pode garantir o *status quo* e a paz social de um Estado Democrático de Direito como o Brasil, no ciberespaço"[204].

Podem ser elencadas como medidas protetivas da privacidade o uso de um sistema operacional como o *Tails*, recomendado hoje quando se quer proteger dados contra a atuação de agências de inteligência[205]; ou o sistema operacional Ubuntu, considerado o mais seguro pelo governo britânico[206]. Utilizá-los pode diminuir consideravelmente o ataque à privacidade numa rede informática. No entanto, note-se que este tipo de proteção é individual. O que o Estado pode fazer em favor de cidadãos diz respeito à difusão da informação sobre esta espécie de proteção.

Ataques cibernéticos têm sido comuns no Brasil. A média de ataques em 2014 foi de cerca de 1000 por dia, sendo que mais da metade com origem dentro do próprio país; sendo cerca de 35% com origem no exterior[207]. A estatística ora apresentada faz concluir que se tem como resolver sem sair do território brasileiro grande parte dos ataques cibernéticos, no entanto para identificar os autores das ameaças, é necessária atuação de pessoal especializado.

Apesar de ser possível dificultar, individualmente, o acesso a dados privados, o Estado pode tutelar os Direitos e Garantias individuais garantidos na Magna Carta de 1988 por meio da já abordada difusão de informações de segurança, de leis, de preparação cognitiva de profissionais para atuar na defesa cibernética e de um aparato tecnológico que imponha a vontade manifestada pela sociedade.

---

[204] ÁLVARES, João Gabriel. Territorialidade e guerra cibernética: novo paradigma fronteiriço. In: *Segurança e Defesa Cibernética*: da fronteira física aos muros virtuais. Recife: UFPE, 2014.

[205] DAILYTASK. *Tails: O sistema operacional mais protegido contra a NSA*. Disponível em: <http://dailytask.com.br/slide/tails-o-sistema-operacional-mais-protegido-contra-a-nsa/>. Acesso em: 09 ago. 2014.

[206] CANALTECH. *Governo britânico considera Ubuntu o sistema operacional mais seguro*. Disponível em: <http://canaltech.com.br/noticia/linux/Governo-britanico-considera-Ubuntu-o-sistema-operacional-mais-seguro/>. Acesso em: 09 ago. 2014.

[207] OLIVEIRA, Eduardo Levi Chaves Barbosa de; SANTOS, Saulo Alex Santana; ROCHA, Fábio Gomes. Software livre na auditoria e segurança da informação: desenvolvimento de sistema operacional para perícia, auditoria, teste e gestão de segurança da informação. In: *Anais 2014 da 16a Semana de pesquisa da Universidade Tiradentes*: ciência e tecnologia para um Brasil sem fronteiras. Disponível em: <https://eventos.set.edu.br/index.php/sempesq/article/view/334>. Acesso em: 14 jan. 2016.

É certo que o pugilato cibernético entre Estados impacta na privacidade dos investigados. Há que considerar, porém, que as normas nacionais podem contribuir ou limitar a eficiência dos resultados apresentados pelo pugilato cibernético em favor da sociedade e do Estado.

O Art. 3º da Lei nº 12.965, de 23 de abril de 2014 – o Marco Civil da Internet – assegura em seu inciso II a proteção à privacidade na rede. A referida Lei é muito clara ao privilegiar a privacidade, mas a despeito do mandamento legal, lesões a este direito fundamental acontecem. Se a lesão à privacidade acontece a partir de uma agência de inteligência estrangeira, por exemplo, a norma nacional não alcançará, em regra, o agente que causou o dano. A única solução efetiva será a técnica, pois a diplomacia dificilmente conseguirá fazer valer a norma nacional em um Estado estrangeiro. Se a lesão à privacidade foi praticada por uma empresa transnacional, provavelmente ela o fará a partir de um país cujas normas sejam permissivas ou omissas em relação a tal atitude. A solução possível virá, mais uma vez, da capacidade técnica de impor o mandamento legal em território nacional. Também nestas hipóteses, resultados eficazes podem depender de mais vigilância. O Brasil faz parte de um pequeno número de Estados que regulamentou o uso da internet de forma específica[208].

O Estado estrangeiro ou suas empresas continuarão fazendo tudo o que sua norma nacional prevê, ainda que viole normas brasileiras e implique na mitigação da privacidade no Brasil. Certo é que aberrações podem ser colocadas como exemplo a ser combatido pela comunidade internacional, tais como a espionagem dos e-mails da Presidente da República do Brasil e da Chanceler alemã realizadas pela NSA[209].

Se a única solução que protege a soberania brasileira em seu próprio território é técnica, faz sentido que o Estado brasileiro a implemente. Para que se tenha uma ideia da relevância do tema para o Estado, havia, no orçamento da União de 2012, a previsão de investimento na ordem de R$ 111,0 milhões, destinados para a implantação do sistema de defesa cibernética, a fim de implementar no Exército Brasileiro a capacidade operacional de pronta resposta de defesa em áreas sensíveis nos campos civil, industrial

---

[208] BEZERRA, Arthur C.; WALTZ, Igor. *Privacidade, neutralidade e inimputabilidade da internet no Brasil*. Revista Eptic Online Vol.16 n.2 p.161-175 mai-ago 2014. Disponível em: <http://www.academia.edu/download/34909678/2276-6228-1-PB.pdf>. Acesso em: 08 jan. 2016.

[209] SNOWDEN, Edward. *Milênio*: Sonia Bridi entrevista Edward Snowden. Disponível em: <http://globotv.globo.com/globo-news/milenio/v/milenio-sonia-bridi-entrevista-edward-snowden/3389933/>. Acesso em: 08 jun. 2014.

e militar[210]. Observe-se que tal destinação orçamentária ocorreu antes das denúncias de Edward Snowden de que uma das maiores empresas do Brasil à época – a Petrobrás – estava sendo espionada[211].

Por meio do pugilato cibernético o Estado pode se proteger e aos seus cidadãos de ameaças sem agredir outras soberanias, preservando a ordem jurídica constitucional e a paz social. Se o aparato do Estado não for suficientemente seguro, poderá, ao menos, dificultar a atuação indesejada.

Crimes e ilícitos cibernéticos podem ferir profundamente uma sociedade, pois podem ameaçar serviços públicos essenciais – como distribuição de energia elétrica e de água, centrais telefônicas, serviços hospitalares –, instituições bancárias, bolsas de valores, privacidade de cidadãos comuns e de autoridades etc. Uma vez que crimes e ilícitos cibernéticos impõe um risco para a sociedade, conforme foi tratado no primeiro capítulo, um governo não pode ser considerado suficientemente confiável para manipular dados pessoais sobre a vida privada, visto que pode utilizar estas informações a seu favor, e não em favor da coletividade, da comunidade. Cresce a importância de que estes dados sejam manipulados por instituições com ingerência política relativizada ou mesmo sem ingerência política, mas com fluxo de recursos contínuos, independente de governo.

É desejável um controle externo apolítico da atividade cibernética desempenhada pelo Estado, realizado por pessoal com qualificação técnica compatível, mediante remuneração, e que não dependam desta atividade, para que isso não seja uma profissão, mas uma função temporária exercida em decorrência de mérito técnico. Não se convém relevar, durante a seleção dos recursos humanos, que eles poderão manipular dados estratégicos e de inteligência. Este cuidado auxilia na preservação da privacidade como conquista civilizatória dentro do possível.

Por certo, países centrais possuem centros de inteligência, e deles dependem para assegurar interesses típicos de Estado (interesses sociais), mitigando riscos contra sua população e suas instituições. Alguns agentes públicos, no entanto, mesmo em

---

[210] MENEZES, Dyelle. *Ação para defesa cibernética recebeu apenas 31% do previsto ano passado*. Disponível em: <http://www.contasabertas.com.br/website/arquivos/530/>. Acesso em: 08 jun.14.

[211] PORTAL G1. *Petrobras foi espionada pelos EUA, apontam documentos da NSA*. Fantástico. Edição do dia 08/09/2013. Disponível em: <http://g1.globo.com/fantastico/noticia/2013/09/petrobras-foi-espionada-pelos-eua-apontam-documentos-da-nsa.html>. Acesso em 07 fev. 2015.

países centrais, aparentemente sentem-se tentados a utilizar esta forma única de prover segurança como forma de ataques e agressões muitas vezes injustas contra os cidadãos indistintamente. Por exporem essa realidade, sítios como *wikileaks* e pessoas como Edward Snowden têm sofrido consequências aparentemente desarrazoadas, ou ao menos polêmicas.

Frise-se que na internet, como já se pôde constatar, a maior parte dos dados trafega sem qualquer tecnologia de segurança da informação[212]. Quando se olha uma praça pública, é possível ver casais passeando, crianças brincando ao sol, pessoas ouvindo música, alguém lanchando ou lendo um livro. Quando se observam dados trafegando sem segurança na internet, em tese, é possível ver se aqueles casais assistem vídeos pornográficos, se há indícios de infidelidade, o que compram e de quais lojas, qual o número do cartão de crédito que usam, para onde pretendem viajar nas férias, com quem trocam mensagens, quais arquivos deixam na nuvem, a que horas e de quais localizações acessam a rede etc.

Considere-se ainda os tantos que disponibilizam voluntariamente dados pessoais na internet. É de se perguntar quantos destes realmente entendem a quantidade de dados que se pode levantar a partir do que é voluntariamente oferecido a empresas com negócios na rede, como proprietárias das redes sociais e outros sítios que coletam informações como os servidores gratuitos de e-mail normalmente fazem.

O Google, em razão dos termos de privacidade[213] a que sujeita seus usuários, está em "rota de colisão" com a União Europeia. O Tribunal de Justiça da União Europeia reconheceu o direito dos cidadãos de serem "esquecidos", desde que peticionem. Hoje, qualquer pessoa na Europa pode pedir ao Google para que retire de suas ferramentas de busca sites desatualizados ou com informações prejudiciais a respeito de quem peticiona[214]. Porém, as informações continuarão existindo nos servidores da empresa.

---

[212] HARRIS, Shon. *CISSP*. Sixth Edition. USA: Mc Graw Hill, 2013. p. 21-155

[213] FUCHS, Christian. *Web 2.0, Prosumption, and Surveillance. In: Surveillance & Society*. vol. 8, no 3., 2011, Queen's University, Canada. Disponível em: <http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/4165/4167>. Acesso em: 06 fev. 2016.

[214] WATERS, Richard. *Google acata decisão da União Europeia sobre privacidade*. Disponível em: <http://www1.folha.uol.com.br/mundo/2014/05/1462454-google-acata-decisao-da-uniao-europeia-sobre-privacidade.shtml>. Acesso em: 06 set. 2014.

Nota-se facilmente que o Estado tem do que proteger os cidadãos menos precavidos. A defesa do Estado pode atuar, inclusive, em defesa da privacidade em relação aos outros atores da rede, no entanto, sem recursos estatais voltados para a defesa técnica das redes de computadores. A privacidade defendida no Marco Civil da internet será uma norma de aplicação limitada. Uma das causas da aludida relativização passa pelo lucro proporcionado às empresas por meio da análise de dados pessoais.

Um ponto interessante ao debate é se seria razoável e proporcional diferentes posturas de investigação quando se toma como referencial cidadãos ou não cidadãos; ou aliados e não aliados. A solução estadunidense, de acordo com declarações publicadas na imprensa, trata de maneira diferente os aliados e os não aliados[215]. Parece haver a mesma sorte de tratamento diferenciado entre cidadãos e não cidadãos.

Alguns órgãos de outros Estados já materializaram pedidos ao legislativo de seus países que tratavam da obtenção de dados que trafegam em rede. Um dos exemplos aconteceu com um projeto de lei estadunidense (Projeto de Lei 266 do Senado) não aprovado, o qual propunha:

> É o julgamento do Congresso [estadunidense] que fornecedores de serviços de comunicações eletrônicas e fabricantes de equipamentos de serviços de comunicações eletrônicas devem assegurar que sistemas de comunicações permitam ao Governo obter o conteúdo integral de voz, dados e outras comunicações quando apropriadamente autorizado pela lei.

Destarte, tal norma obrigaria que estes fornecedores de comunicações eletrônicas implementassem em seus sistemas formas de o governo norte-americano acessarem as informações que lhes interessasse sempre que permitido pela lei: o sistema teria que conter tal dispositivo[216].

Em 1992, também nos Estados Unidos, houve uma proposta recusada pelo Congresso à época e reapresentada em 1994, a qual requeria que todos os fabricantes de

---

[215] PORTAL G1. *EUA vão interromper espionagem de líderes aliados, promete Obama*. Disponível em: <http://g1.globo.com/mundo/noticia/2014/01/obama-anuncia-reducao-do-poder-da-agencia-de-espionagem-dos-eua.html>. Acesso em: 09 ago.14.

[216] ZIMMERMANN, Phil. *Por que você precisa do PGP?* Disponível em: <http://www.pgpi.org/doc/whypgp/br/>. Acesso em: 09 ago. 2014.

equipamentos de comunicações embutissem portas especiais que possibilitassem grampo remoto pelo FBI[217].

Questione-se se seria impossível que algum país exportador equipasse seus produtos vendidos com dispositivos semelhantes. Se tal hipótese fosse considerada possível, apenas um corpo técnico especializado poderia tentar identificá-los.

O governo estadunidense estaria encorajando empresas dos EUA como a AT&T (maior empreendimento de telefonia estadunidense) a utilizar em seus dispositivos um sistema com certo algoritmo que permitiria que o governo acessasse informação criptografada sempre que fosse permitido por norma legal[218]. Como consequência, a China proibiu a compra de aparelhos da empresa americana Apple com dinheiro público, supostamente pelo receio de espionagem implementada por meio destes dispositivos[219].

Para que não se imagine que ferramentas de invasão à privacidade são fomentadas somente em um país, cita-se que a China[220] seria empregadora de mais de dois milhões de pessoas com a atribuição de controlar a conduta de seus cidadãos na internet[221]. Naquele país, há quem afirme que existe um controle de históricos de acesso, correios eletrônicos e outras informações pessoais. O oposicionista do regime chinês Wang Xiamong foi preso por dez anos em razão de uma sentença que o condenou com base em dados sigilosos e pessoais fornecidos pelo Yahoo. Ainda na China, Shi Tao foi condenado em circunstâncias semelhantes[222]. Conclui-se, portanto, que alguns países podem até fazer bom uso das informações disponibilizadas, mas é muito elevado o risco de se permitir coletas de dados pessoais amplas e irrestritas em qualquer regime, especialmente em Estados com instituições democráticas débeis.

---

[217] ZIMMERMANN, Phil. *Por que você precisa do PGP?* Disponível em: <http://www.pgpi.org/doc/whypgp/br/>. Acesso em: 09 ago. 2014.

[218] Ibidem.

[219] YANG, Steven; CHEN, Lulu Yilun. *Governo da China não quer mais os MacBooks e iPads da Apple.* Disponível em: <http://exame.abril.com.br/tecnologia/noticias/governo-da-china-nao-quer-mais-os-macbooks-e-ipads-da-apple/>. Acesso em: 09 ago. 2014.

[220] THE US-CHINA ECONOMIC AND SECURITY REVIEW COMISSION. *Capability of the people's Republico f China to conduct cyber warfare and computer network exploitation.* McLean: Northrop Grumman Co., 2009.

[221] AGENCIA LUSA. *China emprega 2 milhões de pessoas para controlar a internet.* Disponível em: <http://memoria.ebc.com.br/agenciabrasil/noticia/2013-10-05/china-emprega-2-milhoes-de-pessoas-para-controlar-internet/>. Acesso em: 09 ago. 2014.

[222] TERRA TECNOLOGIA. *Saiba como funciona o controle da internet na China.* Disponível em: <http://tecnologia.terra.com.br/saiba-como-funciona-o-controle-da-internet-na-china,57182d8e6545b310VgnCLD200000bbcceb0aRCRD.html/>. Acesso em: 09 ago. 2014.

A tecnologia é aliada de quem a detém. E o domínio tecnológico faz diferença no resultado do pugilato cibernético. Questione-se se para haver ameaça é realmente necessária a conexão em uma rede. Alemães (Estado e população) e russos tem corrido às compras da velha máquina de escrever mecânica pelo receio de espionagem em computadores. Interessante que se diga que a motivação de a população alemã em procurar máquinas de escrever é o receio da espionagem estatal, provavelmente como reflexo de recordações da Alemanha nazista e da atuação da polícia secreta da Alemanha oriental.

Os supostos casos de espionagem atribuídos à NSA fizeram com que alemães ficassem em prontidão. O temor se estende para outros ramos da indústria de "conectáveis": empresas de tecnologia americana têm perdido mercado na Alemanha. Atribui-se a perda de mercado ao receio de espionagem. Uma exceção: aumentaram as vendas de celulares com tecnologia que criptografa (embaralha) as conexões, produzidos por uma empresa sediada em Washington. O Governo Alemão cancelou um contrato que tinha com a gigante de comunicação estadunidense Verizon. A chanceler alemã, Angela Merkel, teria sugerido a "criação de uma 'internet europeia', com a suposta finalidade de não depender de servidores americanos, pois seria implementada apenas por empresas europeias"[223]. Contudo, essa possibilidade pode solucionar em parte o problema dos governos de países europeus, mas não o dos seus cidadãos e seu direito à privacidade.

Nesse contexto, ressalta-se que só deve ser permitido ao Estado atentar contra a privacidade em situações determinadas ou ao menos determináveis, limitadas pela utilização de princípios como proporcionalidade, razoabilidade e dignidade da pessoa humana. O especialista no pugilato cibernético precisa saber bem os limites de sua atuação. Hipóteses que possam gerar dúvida quanto à conduta tomada pelo profissional devem partir do pressuposto que esse está atuando de boa-fé e em prol da comunidade. Ao profissional, visando ao bom exercício de sua profissão, deve ser oferecida tal segurança jurídica, pois, havendo dúvida, a tendência é que o agente público faça menos do que lhe é permitido quando sobrevier a dúvida se ele pode ou não realizar determinada tarefa.

---

[223] REDAÇÃO ÉPOCA. *Medo de espionagem aumenta venda de máquinas de escrever na Alemanha*. Disponível em: <http://epoca.globo.com/vida/noticia/2014/07/medo-bespionagemb-aumenta-venda-de-maquinas-de-escrever-na-alemanha.html/>. Acesso em: 09 ago. 2014.

O agente público, que escolhe ter por profissão servir à sociedade, deve exercer sua profissão dentro da legalidade, e a legalidade a que está sujeito é estrita: ao contrário da sociedade como um todo, em que se pode fazer tudo o que a norma não proíbe, o agente público só pode agir de determinado modo se houver norma permissiva para que assim proceda. É muito importante considerar esta realidade no debate sobre o pugilato cibernético.

Observa-se que as circunstâncias do mundo contemporâneo têm imposto mitigações ao conceito de privacidade. Os Estados[224], quando trabalham com políticas públicas, em particular, no combate ao terrorismo, argumentam pela necessidade de novas dinâmicas no que tange à privacidade. Em síntese, eles defendem que investigar e prevenir atos terroristas é algo intimamente ligado aos poderes estatais de vigilância. Como consequência, a legislação de países centrais, como Estados Unidos e França, tem se adaptado a esta "nova" demanda. Outro ponto a ser considerado é o fato de que os atos terroristas não são restritos a fronteiras nacionais, o que leva a crer que os Estados que possuem condições favoráveis já estão realizando esta espécie de vigilância além de seus territórios.

Em contraponto à mitigação da privacidade de usuários em favor do bem comum, há uma tendência de controle governamental da rede mundial de computadores que objetivam impor restrições no acesso a dados com a finalidade de todo tipo de controle; restringindo acesso a serviços globais, bloqueando fluxo de dados internacionais, dificultando o acesso a direitos sociais, econômicos ou civis a partir de dados de localização. Tais atitudes, que quase sempre partem de governos, tem mitigado a capacidade de pessoas físicas e jurídicas de se beneficiar do acesso ao conhecimento e do acesso a mercados internacionais, reforçando o controle sobre a informação local disponibilizada[225], com evidente prejuízo para a sociedade pela limitação ao acesso de dados, bens e serviços oferecidos por endereços eletrônicos estrangeiros que não estão sujeitos às mesmas restrições. Pode-se exemplificar pela censura que determinados países fazem com relação a alguns sites de internet e pela não aceitação de troca de dados imposta por determinados sites que restringem acesso a depender da origem do

[224] THE US-CHINA ECONOMIC AND SECURITY REVIEW COMISSION. *Capability of the people's Republic of China to conduct cyber warfare and computer network exploitation.* McLean: Northrop Grumman Co., 2009.

[225] CHANDER, Anupam; LE, Uyen P. *Breaking the Web:* Data Localization vs. the Global Internet. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858>. Acesso em: 09 fev. 2016.

usuário. O fato fica evidente quando se nega, por exemplo, o acesso a um aplicativo a depender da origem ou destino provável do acesso.

## 3 O DESAFIO JURÍDICO DE LIDAR COM O PUGILATO CIBERNÉTICO

Os bens jurídicos mais caros para determinada sociedade costumam ser tutelados de forma peculiar, merecendo, pois, a tutela do Direito Penal. Por exemplo, as comunidades que realmente enxergam o terrorismo como algo repugnante, costumam criminalizar as condutas típicas relacionadas ao terrorismo. Nesse raciocínio, ao se tratar da dificuldade de se impor a Lei em ambiente cibernético hostil, far-se-á uma abordagem inicial tratando de crimes cibernéticos, identificando-se problemas relacionados com o princípio da territorialidade e sua aplicabilidade em ambiente cibernético.

Relacionada a crimes cibernéticos, a Lei nº 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos, visa a tutelar dados existentes em dispositivos informáticos. Tal inviolabilidade de dados armazenados decorre do mandamento constitucional previsto no art. 5º, X, CR/88, manifestação do Direito à privacidade e intimidade.

A sociedade necessita de instrumentos de controle para fazer valer o que positivou nas normas. A norma materializa o que se pode entender por gestão de riscos sociais. Se determinada conduta oferece grande risco social, ela provavelmente será criminalizada, o revés acontecerá com uma conduta que pouco ou nenhum risco oferece para a sociedade.

Logo, em princípio, condutas que reconhecidamente desembocam em significativos riscos sociais são criminalizadas ou de alguma forma desestimuladas. Neste ponto cabe uma observação: diferentes povos cultuam diferentes valores; logo, criminalizam diferentes condutas. Assim sendo, não se pode contar necessariamente com o apoio de outros Estados quando determinada conduta fere bens caros particularmente a uma sociedade de referência. Pode ser que, em outras culturas, aquele bem jurídico não seja tão relevante a ponto de se conseguir apoio para tutelá-lo.

Em outras palavras: nem sempre a sociedade, por meio do Estado, consegue impor os interesses sociais em razão de princípios jurídicos consagrados. De forma geral, os Estados criminalizam o atentado contra a vida, em razão do valor destacado do bem jurídico em jogo. Assim sendo, pode-se supor que, sempre que uma conduta é criminalizada, é sinal de que é especialmente danosa para a sociedade. Vale ressaltar

que, por meio da defesa cibernética, um Estado pode defender outro Estado de ameaças no ciberespaço: ataques feitos por terroristas, por grupo de pessoas sem objetivo definido ou por um indivíduo altamente especializado em redes de computadores com intenção de causar dano a outrem. Em outras palavras: a inteligência de um país pode auxiliar outros Estados, por meio da cooperação internacional motivada pelo conhecimento de interesses comuns.

É desejável que a sociedade coíba condutas criminosas da forma mais contundente possível, desde que respeitados os princípios da proporcionalidade, da razoabilidade e da dignidade da pessoa humana, a legitimarem a ação dos agentes estatais.

No contraponto da defesa está a necessidade de vigilância, tanto maior quanto mais eficiente se pretenda a segurança. E vigilância cibernética é sinônimo de relativizar a privacidade. Neste ponto do debate, convém que sejam recapitulados os conceitos de territorialidade e extraterritorialidade já explorados nos capítulos anteriores.

Pela análise do tema já retratada neste trabalho, pode-se perceber que, se Estados preveem hipóteses de aplicação de sua própria norma penal em territórios onde não possuem soberania, tal postura pode causar conflitos entre normas de diferentes nacionalidades. O Código Penal brasileiro pode prever que sua norma alcance um agente localizado fora de seu território. Esta hipótese pode acontecer – e acontece - em casos de crimes informáticos, também conhecidos como crimes cibernéticos. Porém, esse alcance depende da anuência do outro país.

Como o Estado nem sempre pode atingir o agente de uma conduta considerada criminosa para fazer valer a Lei Penal brasileira em território estrangeiro, é fundamental a supremacia técnica ou, pelo menos, a preponderância técnica. Alternativamente se pode pedir intervenção de algum aliado que possua superioridade no ciberespaço para combater alguma ameaça, mas verifica-se nessa hipótese uma potencial perda de soberania, pela falta de capacidade de se defender. Por vezes, os agentes que praticam atos por meio de redes de computadores com reflexos em bens tutelados pela norma constitucional não são alcançáveis por eventual decisão jurisdicional brasileira em razão de estarem fora do território ou do alcance da jurisdição nacional. Eventualmente a conduta considerada criminosa no Brasil pode ser até mesmo desejável onde foi praticada, dada as diferenças existentes entre as culturas.

Eis uma importante razão para que o Estado se mova no sentido de conquistar supremacia técnica quando se fala de pugilato cibernético: pode ser uma das poucas formas de fazer valer a Lei dentro da jurisdição brasileira, por vezes a única forma eficaz de tutelar de fato os bens jurídicos que a Lei nacional pretende tutelar.

A realidade ora apresentada é sabida e se faz presente mesmo em países centrais. Por vezes, a primeira dificuldade é a identificação do autor de determinada conduta indesejável praticada por meio de rede de computadores[226].

### 3.1 Contexto normativo global

Para que se possa entender o contexto normativo global de forma sistêmica, é imprescindível tecer comentários acerca da regulação, cumulativamente com os instrumentos legais já abordados.

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

Se pode parecer estranho tratar de direito econômico ao abordar este tema, convém lembrar que potencialmente o pugilato cibernético tem um enorme impacto econômico, inclusive em ambiente empresarial.

Castells destaca que a ascensão do Estado Regulador, que se deu principalmente a partir dos anos 1980[227], contribuiu para o declínio dos meios clássicos de regulação do próprio Estado. Dessarte é notada uma crise do embasamento clássico do Estado industrial democrático sobre os conceitos de soberania e representatividade democrática, fazendo com que o Estado se torne cada vez mais frágil no contexto global e menos representativo internamente. A fragilidade notada por Castells é reforçada em

[226] EZEKIEL, Alan W. *Hackers, spies, and stolen secrets: protecting law firms from data theft*. In: Harvard Journal of Law & Technology Volume 26, Number 2 Spring 2013. Disponível em: <http://jolt.law.harvard.edu/articles/pdf/v26/26HarvJLTech649.pdf>. Acesso em: 14 jan. 2016.

[227] ROSSI, G. *Pubblico e Privatto nell'Economia di Fini Secolo*. Le Trasformazioni del Diritto Amministrativo. Milano: Giuffrè Editore, 1995. p.230-242.

Estados não centrais, como é o caso do Brasil, em razão das consistentes demandas sociais combinadas com a limitação dos recursos disponíveis para o Estado administrador notadamente perdulário: "gasta muito, e ao fazê-lo privilegia uns poucos, em detrimento da maioria, pois não investe nos serviços públicos essenciais dos quais esta [maioria] carece"[228].

O Estado Regulador aparece, atualmente, com uma forma redesenhada de intervencionismo estatal, voltando-se para um novo sentido oferecido ao comando e controle, talvez mais sutil, porém não necessariamente menos efetivo[229]. Para Chevallier, o Estado Regulador se torna um Estado estrategista que harmoniza interesses, viabilizando a prestação dos serviços de forma conveniente[230].

Considere-se ainda, conforme afirma Aguillar numa análise sistêmica de seus ensinamentos, o fato de que uma regulação exitosa em Estados centrais pode não ser um modelo importável por Estados periféricos sem modificação: ele sugere que se adapte a regulação às circunstâncias, à realidade fática do local onde ela será implementada e efetivada. Face a diferentes realidades sociais, diferentes circunstâncias influenciam na implementação de uma regulação adequada[231].

A regulação das tecnologias da informação e comunicação (TICs) contemporâneas, em especial a comunicação realizada por meio de redes de computadores, esbarra na peculiaridade de que o serviço tornou-se essencial para a vida em sociedade. Ademais, as TICs são de difícil controle por parte de qualquer Estado, face às peculiaridades que podem tornar ineficazes quaisquer tentativas de regulação legal: como visto, a internet não respeita o conceito clássico de territorialidade, primordial para a soberania de um Estado. Em outras palavras, a internet tem mitigado a soberania de todos os Estados.

A conclusão parcial a que se chega é que possivelmente será ineficaz qualquer tentativa de regulação jurídica da internet que não seja ratificada por outros atores internacionais. Nessa hipótese, a supremacia técnica no setor cibernético é uma

---

[228] MACHADO, H. B. *Curso de Direito Tributário*. São Paulo: Malheiros Editores, 2008. p. 26.
[229] COLSON, J.; IDOUX, P. In: Ferreira, R.S.P. (Org.) *A (In)adequação dos Mecanismos Regulatórios Setoriais aos Institutos Jurídicos de Índole Constitucional do Mercado e da Universalização de Serviços Públicos*. Brasília: Universidade de Brasília, 2009. p. 33.
[230] CHEVALLIER, J. In: Ferreira, R.S.P. (Org.) *A (In)adequação dos Mecanismos Regulatórios Setoriais aos Institutos Jurídicos de Índole Constitucional do Mercado e da Universalização de Serviços Públicos*. Brasília: Universidade de Brasília, 2009. p. 42.
[231] AGUILLAR, F. H. *Controle social de serviços públicos.* São Paulo: Max Limonad, 1999.

alternativa para manter tutelados os bens jurídicos que o Estado brasileiro pretende proteger.

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

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

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

A quarta razão que justificaria a regulação do setor é a escassez de recursos. Os autores exemplificam com o fato de o espectro eletromagnético ser limitado:

> [...] logo nem todas as emissoras podem instalar-se livremente sob pena de haver interferência na programação e consequente prejuízo para a comunicação de massa.(...) No caso da imprensa, a defesa de uma regulação técnica similar à da radiodifusão é pouco frequente, principalmente porque inexistem elementos que possam ser definidos consensualmente como "escassos".[232]

[232] ARANHA, M.I.; WIMMER, M.; PIERANTI, O.P. *Direito regulatório*. Brasília: Universidade de Brasília, 2009.

No caso da radiodifusão, a regulação técnica se justificaria com relativa tranquilidade sob o argumento de que o espectro eletromagnético comporta um número limitado de transmissores em razão da largura de banda no padrão técnico adotado pelo Estado. Todavia, quando se fala de internet, este argumento é mitigado: mesmo quando se imagina uma limitação quantitativa de nomes de domínio ou de endereços IP, aparece uma solução técnica implementável para que a quantidade possível aumente substancialmente. Um exemplo na telefonia é o acréscimo de um número no telefone que possibilita uma quantidade maior de assinantes. Esta técnica foi utilizada recentemente na telefonia celular dos estados da região sudeste do Brasil, multiplicando a disponibilidade de linhas telefônicas[233]. Mesmo uma transmissão analógica de radiodifusão utiliza uma largura de banda consideravelmente maior que uma transmissão em quaisquer dos padrões de transmissão digital contemporâneos. Em outras palavras: pela inovação tecnológica, é possível uma quantidade maior de transmissões que no passado utilizando-se como referência uma mesma faixa de frequência.

O século XX pode ser considerado o período em que se consolidaram conquistas atinentes a garantias constitucionais de direitos fundamentais. É entendido como o "[...] século de apresentação do Estado como um componente essencial na definição do conteúdo dos direitos fundamentais mediante enraizamento do conceito de serviço público e da ampliação concreta do rol de direitos dos cidadãos"[234]. Desde então, os direitos fundamentais devem ser assegurados pelo Estado regulador, por meio do "[...] exercício do poder de polícia, atividades de fomento e prestações positivas tradicionais de índole concreta e normativa"[235].

Quando se fala em regulação em um ambiente globalizado, deve-se considerar a necessidade de um ordenamento jurídico adaptado, consoante as relações internacionais, sendo desejável um acordo global, o que facilitaria a interação entre os Estados[236] e reforçaria o poder de controle. Um acordo global diminuiria o risco de beligerância

---

[233] ANATEL. *Nono Dígito*. Brasília, 2012. Disponível em: <http://www.anatel.gov.br/Portal/exibirPortalNivelDois.do?codItemCanal=1746&nomeVisao=Cidad%E3o&nomeCanal=Nono%20D%EDgito&nomeItemCanal=Nono%20D%EDgito>. Acesso em: 19 fev. 2014.

[234] WIMMER, M.; Pieranti, O.P. e Aranha, M.I. (2009) *O paradoxo da internet regulada*: a desregulação dos serviços de valor adicionado no Brasil, Revista de Economía Política de las Tecnologías de la Información y Comunicación.Vol. XI, n. 3, Sep.- Dic./2009. p. 3.

[235] Ibidem.

[236] SUNDFELD, C. A.; Vieira, O. V. *Direito global*. São Paulo: Max Limonad, 1999. p. 157-168.

entre atores internacionais e, de forma concomitante, potencializaria o regramento por normas internas.

Atualmente, a comunidade internacional tem atuado cada vez mais de forma colaborativa. Para que se tenha uma ideia das possibilidades de acordo e cooperação internacional, a Interpol está hoje presente em 190 países do mundo[237]. Dependendo do bem jurídico a ser tutelado pela regulação internacional, a possibilidade de que as regras sejam cumpridas por Estados e cidadãos aumenta significativamente. Para bens jurídicos tão caros a uma sociedade a ponto de serem tutelados pela Lei Penal, a possibilidade de acordo tende a aumentar, afinal os Estados buscam envidar esforços com fins a preservação de direitos que são caros à sua sociedade. O fato de ser uma matéria de interesse de vários países possibilita uma regulação potencialmente mais eficiente.

Quando se fala de regulação do pugilato cibernético, percebe-se, de um lado, a necessidade de o Estado prover a própria segurança, por meio de agentes públicos; e, de outro, tutelar direitos fundamentais constitucionalmente assegurados. A relação existe na medida em que a proteção do Estado será tão mais efetiva quanto maiores forem as informações disponíveis sobre as ameaças em potencial. Em tese, a criação deste banco de dados pode levantar-se contra a privacidade dos atores envolvidos, visto que um potencial dano precisa ser conhecido para ser melhor combatido. Em regra, o operador de defesa cibernética tem necessidade de norma autorizativa de sua conduta, e este fato tem sido um problema para essa espécie de atividade no Brasil. A interpretação sistêmica das fontes do Direito sobre o tema pode se mostrar polêmica no contexto brasileiro.

Com relação à efetiva ação de um dos países com maior ascendência no setor cibernético, o ex-líder do programa de segurança digital dos EUA, Howard Schmidt, especialista em segurança na internet e ex-coordenador de cibersegurança do governo Barack Obama, ensina que "[...] faz parte da responsabilidade de toda nação proteger os seus cidadãos contra a coleta de dados por sistemas de inteligência"[238]. Schmidt sugere atenção às normas internacionais, estabelecendo limites do aceitável.

---

[237] INTERPOL. *A Global Presence.* Disponível em: <http://www.interpol.int/Member-countries/World>. Acesso em: 19 nov. 2013.

[238] AGUILHAR, L. *A espionagem ultrapassou limites.* São Paulo, Disponível em: <http://blogs.estadao.com.br/link/a-espionagem-ultrapassou-limites/>. Acesso em 18 nov. 2013.

Declarou que se preocupa com a militarização da internet, uma vez que 27 Estados criaram organizações militares especializadas em explorar vulnerabilidades das redes de computadores e criar formas de destruir a infraestrutura de oponentes em potencial. Sinaliza com a necessidade de que sejam criadas normas para o ciberespaço. Sugere o modelo multissetorial para a regulação, adotado por órgãos como a ICANN. Adverte que os usuários comuns não imaginam os riscos que a Internet pode oferecer[239].

Sérgio Pagliusi, por sua vez, afirma que, em uma escala de 0 a 10, o Brasil estaria com nota entre 3 e 4 no quesito segurança da informação. Segundo ele, "[...] estamos começando a acordar para o problema. Nessa história de espionagem corporativa, temos muita lição a fazer. Falta consciência institucional e um longo aprendizado. A sociedade como um todo caiu em si e viu que é uma coisa que nos afeta"[240]. Tal assertiva leva a inferir que o pugilato cibernético influi na vida de toda a sociedade. A ameaça é tão real que a espionagem já cancela projetos de computação em nuvem[241]. Acerca da possibilidade de tecnologia brasileira eficaz para a necessária segurança, Rafael Moreira, conselheiro do Comitê Gestor da Internet (CGI), afirma que "[...] há uma massa de conhecimento dentro das universidades e em empresas inovadoras que podem contribuir propondo medidas para que possamos mudar isso [falta de segurança] no longo prazo"[242]. Portanto, o Brasil tem potencial para atuar com o pugilato cibernético, carecendo de aprimorar e integrar seus recursos.

Para Pinheiro[243], quando não existe um contrato entre partes com interesses antagônicos, a precariedade na definição de normas será um fator para potencializar a imprevisibilidade de eventual decisão judicial na relação entre elas, com a consequente insegurança jurídica inerente às circunstâncias apresentadas. Reforça ainda que um sistema justo seria aquele no qual a probabilidade da vitória do certo tende a cem por cento.

---

[239] AGUILHAR, L. *A espionagem ultrapassou limites.* São Paulo, Disponível em: <http://blogs.estadao.com.br/link/a-espionagem-ultrapassou-limites/>. Acesso em 18 nov. 2013

[240] GROSSMANN, L.O. *Espionagem dos EUA já cancela projetos de computação em nuvem*. Disponível em: <http://convergenciadigital.uol.com.br/ cgi/cgilua.exe/sys/start.htm?infoid=34377#.UoqGqxrrzQs>. Acesso em: 18 nov. 2013.

[241] Ibidem.

[242] AGÊNCIA BRASIL. *Especialistas ouvidos por CPI alertam para baixa segurança da informação.* Brasília, 2013. Disponível em: <http://www.correiobraziliense.com.br/app/noticia /politica/2013/10/22/interna_politica,394706/especialistas-ouvidos-por-cpi-alertam-para-baixa seguranca-da-informacao.shtml>. Acesso em: 18 nov. 2013.

[243] PINHEIRO, Patrícia Peck. *Direito Digital*. 2. ed. São Paulo: Saraiva, 2007. p. 1-2.

### *3.1.1 A Defesa Cibernética no Ministério da Defesa brasileiro*

No Brasil, a defesa cibernética – tratada como atividade estatal – é relativamente recente. Porém, antes de adentrar nos pormenores das atividades do que a partir de agora chamaremos de pugilato cibernético, pretende-se diferenciar a referida atividade do que se conhece por guerra eletrônica. Esta última é "[...] o conjunto de atividades que visam desenvolver e assegurar a capacidade de emprego eficiente das emissões eletromagnéticas próprias, ao mesmo tempo em que buscam impedir, dificultar ou tirar proveito das emissões inimigas"[244]. Desta definição conclui-se que a guerra eletrônica se relaciona com a propagação de radiofrequência no espectro eletromagnético.

Há poucos anos foi noticiado que, por meio de um equipamento móvel de escuta específico para telefonia celular francês e de escutas ambientais, foram realizadas escutas telefônicas e ambientais de comunicações de ministros do Supremo Tribunal Federal (STF)[245]. De acordo com os conceitos apresentados *supra*, casos como estas supostas escutas demonstram possibilidades de atuação da guerra eletrônica, já que se coletaram dados sem o uso de rede de computadores.

Como já foi descrito, o pugilato cibernético relaciona-se com o uso de computadores em rede. A este tema estaria ligado, *v.g.*, o fato afirmado pela empresa estadunidense de segurança eletrônica FireEye de que a China teria *hackeado* computadores de chanceleres europeus que iriam participar dias depois da reunião de setembro de 2013 do G20, o que foi negado e condenado pelo governo chinês[246].

A END determina que, no setor cibernético, deve ser constituída uma organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar. Espera-se que a preparação para a guerra cibernética auxilie no aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à defesa nacional contra-ataques cibernéticos.

A Portaria 3028/12 do Ministério da Defesa (MD), em seu art. 1º, atribui a responsabilidade pela coordenação e integração das atividades de Defesa Cibernética ao

---

[244] BRASIL. Ministério da Defesa. *C 34-1*: O Emprego da Guerra Eletrônica. Brasília: EGGCF, 2008.
[245] BONIN, R. O Livro Bomba. *Revista Veja*. Ed. 2351. São Paulo: Editora Abril, 2013. p.74-80.
[246] FOLHA DE SÃO PAULO. *China é acusada de hackear reunião do G20*. Disponível em: <http://www1.folha.uol.com.br/fsp/mundo/143297-china-e-acusada-de-hackear-reuniao-do-g20.shtml>. Acesso em: 12 dez.13.

Exército Brasileiro (EB) no âmbito das Forças Armadas do Brasil. Assim sendo, o maior centro de doutrina do MD está no Exército. Hoje, a organização encarregada de desenvolver a capacitação cibernética no âmbito do Ministério da Defesa é o Centro de Defesa Cibernética (CDCiber). Subordinado ao Departamento de Ciência e Tecnologia do Exército Brasileiro, esse centro tem recebido investimentos do Governo Federal com escopo na capacitação de pessoal que possa fazer frente a um possível ataque cibernético.

Para o CDCiber, a guerra cibernética em sentido estrito diz respeito a um nível de decisão operacional ou tático. Em nível estratégico, denomina-se Defesa Cibernética. No nível de decisão político, convencionou-se chamar de Segurança Cibernética. Esta é a terminologia adotada pelo MD. Neste trabalho, convencionou-se adotar a expressão pugilato cibernético qualquer que seja o nível de decisão. Conceitos de segurança cibernética, inteligência cibernética e pesquisa cibernética estão relacionados ao tema.

O MD, em 2012, editou a Política Cibernética de Defesa (MD31-P-02) por meio da Portaria Normativa nº 3389/MD. Fruto das diretrizes traçadas, foram implementados produtos como o antivírus nacional e o Simulador de Operações Cibernéticas, *software* que utiliza a doutrina brasileira para treinar os "guerreiros cibernéticos" formados no Exército. A capacitação de recursos humanos em guerra cibernética é feita, no âmbito do Exército, no Centro de Instrução de Guerra Eletrônica (CIGE), instituição de ensino superior que capacita também especialistas em guerra eletrônica.

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

A estrutura ora apresentada oferece sinergia para a defesa nacional, pois facilita a atuação conjunta de diversas áreas numa operação militar terrestre. Este contexto sugere que se pode realizar uma análise sistêmica dos vetores ora apresentados quando se tem a segurança no trânsito das informações com o objetivo a ser perseguido.

O CDCiber tem participado de grandes eventos realizados no Brasil, como a Rio +20, a Jornada Mundial da Juventude, a Copa das Confederações e a Copa do Mundo 2014, possuindo uma central de monitoração cibernética. A intenção é de que participe também das Olimpíadas do Rio de Janeiro em 2016.

A doutrina de guerra cibernética ainda é incipiente se comparada à doutrina de guerra eletrônica (GE). Logo, como possuem pontos em comum, vale uma análise de alguns conceitos de GE para que se comece a entender analogamente a guerra cibernética.

A GE está presente nas Forças Armadas brasileiras desde os anos 80 e já possui doutrina consolidada no Brasil. Está em curso, em razão de um acordo de compensação do Exército Brasileiro, o desenvolvimento em parceria de *hardwares* de sensores eletromagnéticos brasileiros, desenvolvidos com tecnologia alemã e brasileira. Trata-se de conhecimento industrial bastante restrito e importante para potencializar os esforços de segurança.

A doutrina de guerra eletrônica, no contexto internacional, destaca como sua principal atividade a inteligência do sinal (nível estratégico). Trata-se de uma atividade que busca formas de se preparar para a guerra, a partir da coleta constante de informações em tempo de paz. A atividade de inteligência do sinal busca apoiar o combate pelo conhecimento do potencial oponente e das vulnerabilidades próprias. No nível tático, busca-se obter dados a partir da aquisição de sinais eletromagnéticos. A finalidade de interceptar, identificar emissões determinadas e localizar o emissor de rádio frequência é o reconhecimento imediato da ameaça[247].

Existem outros ramos de atividades não menos importantes, porém praticadas somente em casos específicos. São executadas normalmente no nível tático, ou, numa linguagem mais simples, em efetivo combate. Uma delas visa a impedir ou reduzir o emprego eficiente do espectro eletromagnético pelo oponente: o que for possível e mais conveniente e/ou oportuno. Outra visa a assegurar a utilização eficiente do espectro eletromagnético, a despeito das tentativas do oponente em dificultar ou impedir as nossas transmissões e de obter dados a partir da aquisição de sinais eletromagnéticos[248].

---

[247] BRASIL. Ministério da Defesa. *C 34-1*: O Emprego da Guerra Eletrônica. Brasília: EGGCF, 2008.
[248] Ibidem.

Analogamente, pode-se estimar a importância, num contexto de pugilato cibernético, de saber o que se passa consigo e com o potencial oponente para que realmente se perceba a utilidade do emprego da defesa cibernética. Além disso, deve-se utilizar toda a informação obtida com o propósito de impedir ou dificultar o uso regular de uma rede de computadores quando necessário, e, ao mesmo tempo, assegurar que a própria rede de computadores funcione adequadamente.

Ainda que a doutrina militar brasileira não privilegie o ataque – mas a reação ao ataque –, é inquestionável que o preparo para operações de ataque ou de defesa é necessário. Com isso, pode-se concluir que uma boa preparação no campo do pugilato cibernético deve buscar conhecimento das próprias vulnerabilidades e assegurar a segurança no uso das redes de computadores próprias. Ademais, deve-se ter capacidade para interceptação e ataque. Partindo dessas premissas, o Brasil tem privilegiado técnicas de autodefesa e a defesa ativa, conforme declaração do General José Carlos dos Santos, então chefe do CDCiber[249].

No entendimento de Davi Ottenheimer, é desejável que, em caso de ataques cibernéticos, realizem-se contra-ataques visando à prevenção contra novos ataques, de forma comissiva, reforçando o conceito de defesa ativa[250].

Para que haja preparação adequada para o pugilato cibernético, é necessária uma constante busca de dados por meio da rede: tanto as vulnerabilidades próprias quando as de oponentes em potencial. Funciona como um agente de segurança na rua, que cumpre sua função mais adequadamente se souber quem está à sua volta, no ambiente onde se propõe a manter a ordem.

A busca de dados ora referida deve acontecer não só por meios eletrônicos, mas por todos os meios disponíveis. Dados como os disponibilizados pelo delator do suposto sistema governamental estadunidense de espionagem Edward Snowden[251] devem ser

---

[249] MOTTA, S. *CDCIBER:* na guerra cibernética, Brasil adota estratégia do contra-ataque. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/1632/cdciber---na-guerra-cibernetica--brasil-adota-estrategia-do-contra-ataque>. Acesso em: 16 fev.14.

[250] CONGRESSO INTERNACIONAL SOFTWARE LIVRE E GOVERNO ELETRÔNICO (V Congresso). *A favor de uma defesa ativa contra-ataques cibernéticos*: Belém do Pará. Disponível em: <https://gestao.consegi.serpro.gov.br/cobertura/noticias/a-favor-de-uma-defesa-ativa-contra-ataques-ciberneticos>. Acesso em: 16 fev. 2014.

[251] REDAÇÃO G1. *Entenda o caso de Edward Snowden, que revelou espiongem dos EUA*. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 16 fev. 2014.

confirmados ou ao menos ter sua probabilidade de veracidade escalonada para compor mais um subsídio nas análises de dados voltada para a defesa cibernética.

Sem considerar aspectos políticos, a oitiva de pessoas com acesso a informações de espionagem estatais dispostas a falar sobre o assunto é sempre um complemento desejável para confirmar ou não dados coletados eletronicamente, mas tais declarações devem ser sempre analisadas com cautela, a fim de evitar a manipulação por meio de dados falsos.

O modelo de guerra cibernética ainda é incipiente[252], mas está se desenvolvendo em razão do aporte de recursos que possibilita, inclusive a formação de uma doutrina própria, que considere as peculiaridades do Estado brasileiro. Muito se tem avançado no Ministério da Defesa quando se trata do assunto como por exemplo com a criação da Escola Nacional de Guerra Cibernética[253] cujo projeto tem sido elaborado pela Universidade de Brasília, no entanto, é possível ainda fomentar novas parcerias tanto com nações amigas quanto com a iniciativa privada. Tais parcerias podem trazer ganho não só para todos os envolvidos, potencializando de forma sinérgica a doutrina da guerra cibernética e as tecnologias envolvidas. A partir da construção de uma doutrina aperfeiçoada, cabe apresentá-la à sociedade para que, ratificando seu uso, se possam fazer adequações legislativas necessárias, se for o caso. Também no desenvolvimento e manutenção da doutrina de guerra cibernética, há grande espaço para o clássico modelo da tríplice hélice de desenvolvimento: Estado, academia e indústrias unidos no aperfeiçoamento da tecnologia de interesse em um modelo onde todos ganham.

Outro ponto positivo da escola de cibernética é o fato de estar ligada umbilicalmente com quem vai realizar operações cibernéticas em favor da sociedade. Pode-se, ainda, ampliar muito o uso da tecnologia para, como sugere o presente trabalho, utilizar a defesa cibernética em prol de todas as estruturas que ajudam a sociedade: defender diretamente quem gera emprego e renda na sociedade brasileira, independente de já existirem investimentos privados com o mesmo objetivo.

---

[252] SENADO FEDERAL. *Inimigos invisíveis*: a guerra cibernética. Disponível em: <http://www.senado.gov.br/noticias/Jornal/emdiscussao/defesa-nacional/razoes-para-a-implementaao-da-estrategia-nacional-de-defesa/inimigos-invisiveis-a-guerra-cibernetica.aspx>. Acesso em: 06 fev. 2016.

[253] MATSURA, Sérgio. *Brasil terá Escola Nacional de Defesa Cibernética.* Disponível em: <http://oglobo.globo.com/sociedade/tecnologia/brasil-tera-escola-nacional-de-defesa-cibernetica-15914957>. Acesso em: 06 fev. 2016.

### *3.1.2 O pugilato cibernético e o Direito Digital*

Algo que não se pode esquecer quando se reporta ao pugilato cibernético são alguns dos conceitos recorrentes no Direito Digital. O Direito busca tutelar bens jurídicos com a finalidade de tornar possível o bom convívio social. A sociedade da era da informação adveio de um longo processo que pode ter seu início vinculado à própria Revolução Industrial[254].

Pinheiro entende que o Direito Digital consiste na evolução do próprio Direito, abrangendo princípios e institutos vigentes e introduzindo novos institutos e elementos para o pensamento jurídico[255]. A velocidade das transformações tecnológicas tem sido uma barreira à legislação quando se trata de Direito Digital[256]. Da Revolução Industrial até os dias de hoje, a sociedade passou a atribuir cada vez mais valor aos bens imateriais, que de tão valorosos têm sido tutelados até mesmo pelo Direito Penal em diversos países, dentre eles, o Brasil. Cada vez mais tutelam-se bens imateriais, tais como a imagem, a integridade, a dignidade, a privacidade etc. A valorização desses bens pode ser inferida de disposições constitucionais e penais no Brasil, acompanhando uma tendência global. Grande parte destes bens imateriais possui vínculo com redes de computadores, em especial, com a internet[257].

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

Na medida em que sistemas críticos passam a depender das informações trafegadas em rede de computadores, aparece uma nova arma de combate: a manipulação das informações que trafegam em rede. O pugilato cibernético vem ganhando importância em razão da gama de ameaças que podem ser, por meio dele, combatidas.

Debates atinentes a iniciativas legislativas, como o Marco Civil da Internet, influenciam a regulação do pugilato cibernético no Brasil. Essa Lei em pauta valoriza a

---

[254] CRESPO, M.X.F. *Crimes digitais*. São Paulo: Saraiva, 2011. p.32.
[255] PINHEIRO, Patrícia Peck. *Direito Digital*. 2. ed. São Paulo: Saraiva, 2007. p. 29.
[256] Ibidem. p. 31.
[257] Idem. p. 32-37.

privacidade, a neutralidade da rede e define como imputar condutas indesejáveis a indivíduos. São temas que devem ser valorizados quando da apreciação dos limites de atuação do pugilato cibernético praticado pelos agentes públicos, enquanto instrumento do Estado. Porém, o Marco Civil possui aspectos muito polêmicos e grandes divergências a serem pacificadas com o tempo. Como sugere o Marco Civil da Internet, atenção especial merece a privacidade, como aqui já se tratou.

Quando se aborda o pugilato cibernético no âmbito governamental, deve-se ter em conta que essas são atividades planejadas e executadas pelo Poder Executivo. De acordo com a teoria apresentada por North[258], o judiciário teria um papel coercitivo numa relação entre outros dois agentes com interesses diversos: o Estado e o detentor de informação que deseja protegê-la.

De acordo com o que propôs North sobre a condução do pugilato cibernético pelo Executivo, o termo guerra cibernética evidencia – até mesmo pelo seu nome – que quem tem melhores condições de conduzir as operações cibernéticas são profissionais da guerra pois, ao menos em tese, podem tratar os dados adequadamente para que os objetivos da sociedade sejam alcançados.

Durante as manifestações populares ocorridas no Brasil em junho de 2013 contra atos de governo, vários protestos foram organizados por meio de redes sociais. Nessa ocasião, o Exército monitorou a rede com uma técnica semelhante à utilizada pela NSA. Isto se deu por meio de um *software* que filtra as informações disponibilizadas nas redes sociais. Desta forma, o Exército poderia identificar aqueles que assumiram o comando dos protestos. As informações foram repassadas para a Polícia Federal e para a Secretaria de Segurança Pública dos estados nos quais ocorreram tais manifestações[259].

Naquela ocasião, um grupo de cinquenta militares ficou responsável pela identificação dos líderes das manifestações, pontos de potencial conflito e organização de atos de vandalismo. Agentes e delegados da Polícia Federal atuaram em conjunto com o Exército. Segundo o General José Carlos, que estava na chefia do CDCiber, a atividade foi desempenhada dentro da legalidade, visto que o acompanhamento é necessário por envolver questões ligadas a Segurança Nacional, o que legitimaria e

---

[258] SASSINE. V. *Exército monitorou líderes de atos pelas redes sociais*. Disponível em: <http://oglobo.globo.com/pais/exercito-monitorou-lideres-de-atos-pelas-redes-sociais-9063915>. Acesso em: 08 dez. 2013.

[259] Ibidem.

justificaria, segundo ele, esta ação. O *software* utilizado para a realização desta operação é de fabricação nacional, desenvolvido pela Dígitro, sociedade empresária sediada em Florianópolis, SC, a qual comercializaria a solução para órgãos de segurança pública em geral.

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

> É uma técnica de filtragem que a própria espionagem deve utilizar racionalmente. Os americanos monitoram 2,3 bilhões de e-mails e telefonemas. Se não houver essa técnica, não é possível gerar inteligência sobre isso. O próprio embaixador americano (no Brasil), Thomas Shannon, indica que essa é a técnica utilizada pela NSA. É um processo semelhante. A grande diferença é que nós nos baseamos só em informações de domínio público.[260]

Fadi Chehardé, representante do ICANN que reside nos Estados Unidos, apresentou à presidente brasileira Dilma Rousseff a intenção de reunir no Brasil representantes de setores da sociedade com o escopo de redigir uma carta de princípios que o órgão pretende que seja a base para regulação do ambiente virtual. Além de garantir a liberdade de expressão na internet, a corporação pretende evitar o *great firewall*, uma espécie de censura governamental na internet. Sobre a recente espionagem realizada pela Agência Nacional de Segurança dos Estados Unidos contra outros países, ele opina que espiões são necessários, mas que deve-se deixar claro o que os países podem e o que não podem fazer na internet. A entidade teme que a espionagem afete a confiança dos usuários comuns de guardar dados "na nuvem"[261].

O direito à privacidade assegurado pela CR/88 engloba a tutela a informações pessoais do indivíduo, as quais são protegidas do uso de outros – inclusive do próprio Estado. A Lei nº 9.296, de 24 de julho de 1996, em seu artigo 10, dispõe que constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática sem autorização judicial ou com objetivos não autorizados em Lei. A Lei nº 12.527, de 18 de novembro de 2011, em seu art. 32, IV, dispõe que constitui ilícito divulgar ou

---

[260] SASSINE. V. *Exército monitorou líderes de atos pelas redes sociais*. Disponível em: <http://oglobo.globo.com/pais/exercito-monitorou-lideres-de-atos-pelas-redes-sociais-9063915>. Acesso em: 08 dez. 2013.

[261] VILICIC, F. Por uma Web Sem Censura. *Revista Veja*. ed. 2351. São Paulo: Abril, 2013. p. 114-115.

permitir a divulgação, acessar ou permitir acesso indevido a informação sigilosa ou informação pessoal. A Lei nº 12.737, de 30 de novembro de 2012, introduziu no Código Penal (art. 154-A) a seguinte tipificação criminosa: devassar dispositivo informático alheio, conectado ou não na rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo.

Por outro lado, as Forças Armadas possuem uma atribuição constitucional de defender a pátria, garantindo a lei e a ordem sempre que chamadas a tal atribuição (art. 142, CR/88). Sendo assim, é conveniente, sob pretexto de que às pessoas seja oferecida segurança na internet, derrubar "serviços, sites e redes ligadas ao crime virtual"[262] – como está previsto no Centro de Combate a Crimes Cibernéticos da Microsoft. Acontece que, para que este objetivo seja alcançado, é necessária uma investigação prévia, a partir da monitoração da rede mundial de computadores. Pode-se questionar até que ponto uma investigação como essa, anunciada por uma empresa privada na imprensa mundial, pode ferir a privacidade dos usuários da rede.

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

Numa análise sumária do que já foi apresentado, as Forças Armadas brasileiras têm adotado a política de monitoração das informações públicas disponibilizadas nas redes de computadores, ao menos quando se fala de segurança em grandes eventos. Na hipótese de a sociedade necessitar de mais segurança, seria desejável uma lei que autorizasse expressamente atuação mais livre dos órgãos públicos competentes, para que os gestores públicos possam desenvolver a atividade que lhes foi confiada de maneira mais consciente, maximizando a segurança e respeitando a privacidade nos limites estabelecidos. No cenário atual, em face da incipiência de julgados sobre o tema e a escassez de doutrinadores que o abordam, falta a gestores e agentes públicos segurança jurídica no desempenho da atividade. Isso decorre também da pouca

[262] REDAÇÃO INFO. *Microsoft abre centro para combater crimes cibernéticos*. Disponível em: <http://info.abril.com.br/noticias/internet/2013/11/microsoft-abre-centro-para-combater-crimes-ciberneticos.shtml>. Acesso em: 08 dez. 2013.

regulação do setor, uma vez que a conduta dos agentes públicos se funda no princípio da legalidade estrita. Se a pouca regulação é uma opção política de regular condutas, é questionável se essa seria a melhor decisão para a atividade em pauta.

Bill Clinton, ex-presidente dos Estados Unidos, diz que, em seu país, o governo pode monitorar ligações e *e-mails*, desde que em busca de padrões. O conteúdo é violado nas hipóteses em que se percebem conexões regulares com suspeitos de terrorismo. Decorre que, mesmo nestes casos, o governo necessita de requerimento a tribunal para acessar a comunicação. Apesar destas medidas de precaução, admite que bons técnicos são capazes de quebrar qualquer segurança na rede, citando exemplos públicos de quem já realizou este tipo de conduta. Ele opina, ainda, que o governo norte-americano não deveria levantar informações econômicas de aliados sob pretexto de segurança[263]. A par desta exceção, o ex-presidente afirma que, para a realidade americana, seria razoável levantar algumas informações não econômicas de aliados, informações – inclusive econômicas – de não aliados e informações consideradas sensíveis no combate ao terrorismo. De fato, poder levantar e armazenar informações facilita a atuação do Estado em contexto de pugilato cibernético.

### 3.2 O pugilato cibernético entre a centralidade individual e a coesão social

A defesa cibernética patrocinada pela sociedade pretende, além de sua própria defesa, tutelar a instituição do Estado e todos que concorrem de alguma forma para o bem da sociedade. Assim sendo, como visto, a defesa cibernética é concebida para proteger a sociedade de ataques cibernéticos de eventuais oponentes, incluindo-se hipóteses de *cyberterrorismo*.

Por outro lado, a defesa eficiente depende de vigilância, com os reflexos já tratados quando se abordou o direito à privacidade. Há de haver um equilíbrio entre as necessidades sociais, o qual deve ser norteado pela própria comunidade, debatendo e enfrentando o problema em sua plenitude. O ideal é que a decisão seja materializada em forma de Lei.

---

[263] DÓRIA, P.; RODRIGUES L. *Segurança não justifica espionagem econômica*. Disponível em <http://oglobo.globo.com/pais/exercito-monitorou-lideres-de-atos-pelas-redes-sociais-9063915>. Acesso em: 09 dez. 2013.

Como visto, ataques cibernéticos podem vulnerabilizar a sociedade como um todo, visto que as redes informáticas permeiam muitas formas de relacionamento e de controle humanos.

Pode auxiliar o debate trabalhar com a ideia de centralidade individual e coesão social[264]. Quando a sociedade está unida, está coesa, está no ponto ômega de sua evolução, ela atinge um patamar de coesão social: esse seria, no plano macro, o objetivo a alcançar. E, no plano micro, o objetivo seria a centralidade individual: quando o indivíduo não está na periferia de seu ser, mas no centro de si mesmo, alcançando a plenitude, na busca da felicidade.

Pode-se supor que uma comunidade é mais feliz quanto mais próxima do patamar da coesão. Todas as vezes que a sociedade alcança o patamar da coesão, ela está em um estado de conquista, de realização coletiva. Em suma: a centralidade está para o indivíduo assim como a coesão está para a sociedade. Todo indivíduo almeja a centralidade individual: sua autoestima está no ponto, não está esgarçada; e a essa ideia de centralidade individual corresponde a de coesão social no plano coletivo.

Do entendimento expresso *supra* se percebe que o interesse individual e o bem-estar da sociedade são institutos conciliáveis. Pode haver uma otimização do individual e do social. A solução do equilíbrio entre centralidade individual e coesão social passa por instituições que fomentam valor a um e outro, tais como sociedades empresárias: permitem conhecimento e realização pessoal e coletiva. Sociedades com empresas bem desenvolvidas costumam oferecer conhecimento e qualidade de vida onde estão inseridas, merecendo, em regra, proteção.

O presente trabalho já abordou a questão dos direitos individuais, assim como também tratou do pugilato cibernético sob o prisma do Estado representando a coletividade. Abordar-se-á, no momento, a possibilidade de proteção das empresas enquanto fontes de coesão social e viabilizadoras, de fato, da conquista representada pela centralidade individual.

---

[264] Conceitos trazidos pelo Jurista Carlos Ayres Britto como na matéria: *O centro e a periferia de nós mesmos*. Disponível em: <http://opiniao.estadao.com.br/noticias/geral,o-centro-e-a-periferiade-nos-mesmos,10000002601>. Acesso em: 09 de fevereiro de 2016

### *3.2.1 A defesa das empresas frente ao pugilato cibernético*

Sociedades empresárias bem estruturadas normalmente já possuem investimentos relacionados à segurança de redes informáticas. No entanto, o Estado deve apoiar tais iniciativas de maneira sinérgica. A partir de direitos constitucionais relativos a sociedades empresárias, há aspectos jurídicos que indicam razões para a implementação de políticas públicas que visem à defesa cibernética para as empresas.

Theodoro Júnior discorre que a jurisprudência melhor posicionada acolhe o entendimento de que o nome, o conceito social e a privacidade são bens cabidos e tutelados pela Constituição da Federal de 1988, tanto para pessoa física, quanto para pessoa jurídica. Logo, ambas podem reclamar ressarcimento por prejuízos causados tanto ao nome comercial, conceito na praça, sigilo nos negócios[265]. Ressalte-se que a privacidade da pessoa jurídica também é protegida.

A titularidade de direitos fundamentais por sociedades empresárias é fundamento para qualquer regime constitucional, merecendo a atenção da Ciência do Direito, pois estão vinculados à ideia de Estado democrático de direito[266]. Preliminarmente, pode-se dizer que a Constituição Federal de 1988 não faz distinção quanto à titularidade de direitos fundamentais, e discorre, no caput do art. 5º, sobre o princípio da igualdade de todos perante a lei, sem qualquer distinção. Em poucos casos, a CR/88 faz menção expressa à titularidade de direitos fundamentais por pessoa jurídica, como no caso do art. 5º, XXI (caso das associações para representar seus filiados), ou no caso do art. 8º, III (hipótese de sindicatos defendendo interesses de categorias)[267]. Muitos dos direitos elencados na Constituição são extensíveis às pessoas jurídicas pois, em diversas hipóteses, a proteção última do indivíduo perpassa a proteção oferecida pela norma constitucional às pessoas jurídicas[268]. As pessoas jurídicas com a referida proteção podem ser tanto as brasileiras quanto as estrangeiras que atuem no Brasil[269].

---

[265] THEODORO JÚNIOR, Humberto. *Dano Moral*. 1 ed., São Paulo: Oliveira Mendes, 1988.
[266] TAVARES, André Ramos. *Direito Constitucional da Empresa*. Rio de Janeiro: Forense, 2013. p. 14-18.
[267] Ibidem. p. 23-26.
[268] BASTOS, Celso Ribeiro Bastos. *Curso de direito constitucional*. 21 ed. São Paulo: Saraiva, 2000. p. 282.
[269] CAMPINHO, Sérgio. *O direito de empresa*: à luz do novo Código Civil. 13 ed. Rio de Janeiro: Renovar, 2014.

Outros direitos assegurados pela Constituição, que também são vitais para uma empresa, dizem respeito à segurança jurídica, tais como a previsibilidade e o direito a não surpresa, dentre outros[270].

O STF já se manifestou no sentido de que alguns direitos fundamentais dos contribuintes elencados no art. 15º da CR/88 são aplicáveis às pessoas jurídicas em uma relação tributária, admitindo, ainda que minimamente, a titularidade de direitos fundamentais por pessoas jurídicas[271]. O RE 63.694 / RS ratifica a possibilidade de reconhecer direitos fundamentais de sociedades empresárias.

Quanto à lesão de direitos da pessoa jurídica, existe uma controvérsia acerca da indenização por dano moral. Durante período considerável, houve o entendimento de que a lesão moral seria fenômeno atinente exclusivamente à pessoa natural. Dada a evolução cognitiva, já se admite na doutrina e na jurisprudência tal possibilidade[272].

Cardoso[273] opina no sentido de que a prevenção é o melhor meio para que o ilícito seja evitado, discorrendo que os problemas sociais são resolvidos não por normas, mas por meio de instrumentos de prevenção. Segundo o autor, a prevenção a que se refere reclama uma intervenção dinâmica e positiva que neutralize suas raízes ou causas.

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

O art. 5º, X, da CR/88 afirma que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação". André Ramos Tavares sustenta que a titularidade dos

---

[270] TAVARES, André Ramos. *Direito Constitucional da Empresa*. Rio de Janeiro: Forense, 2013. p. 13-14.
[271] Ibidem. p. 26-27.
[272] SANTINI, José Raffaelli. *Dano Moral*. Campinas: Millennium, 2002. p. 21-26.
[273] CARDOSO, Atinoel Luiz. *Das Pessoas Jurídicas e Seus Aspectos Legais*: Sucessão Comercial, Fundações e Associações, Direito Público e Direito Privado, Capacidade e Vontade Jurídica, Sociedade Anônima e Holding, Instituições e Vontade Social, Extinção da Pessoa Jurídica. São Paulo: AEA Edições Jurídicas, 1999. p. 84-88.

direitos retratados no presente inciso não é restrita a pessoas físicas, mas compreende também pessoas jurídicas; e cita que a conclusão a que chegou encontra guarida no entendimento do STF, citando como argumento a Reclamação 2040-1 / DF, cujo relator foi o Ministro Néri da Silveira.

O referido autor cita ainda o direito à imagem de pessoas jurídicas presentes tipicamente na rede mundial de computadores, oportunidade em que se pode evidenciar a tutela constitucional da imagem das pessoas jurídicas[274]. A imagem certamente deve ser protegida, mas há outros valores que podem ameaçar de forma muito mais significativa a atividade empresária que se utiliza de redes informáticas de maneira direta ou indireta para desempenhar sua função social.

A propriedade constitui outro direito essencial à atividade empresarial. O direito de propriedade deixou de ser absoluto, visto que a propriedade da sociedade empresária, como qualquer outra propriedade no Brasil, deve cumprir sua função social. Se, no século XIX, a propriedade tinha característica essencialmente individualista, hoje deve harmonizar o caráter de direito individual e a função social. Se, por um lado, há um direito subjetivo de exploração de determinado bem da vida, com fulcro no inciso XXII do art. 5º da CR/88, por outro, há o mandamento do inciso XXIII do mesmo artigo, que induz concluir que a propriedade de uma sociedade empresária tem por finalidade também assegurar para a comunidade uma existência com dignidade e justiça social, conforme art. 170, *caput*, da CR/88[275].

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

Por certo, tal preservação também passa por uma segurança cibernética, que deve ser provida pelo Estado. É evidente que o particular pode e deve investir em segurança cibernética a fim de que seus interesses individuais sejam preservados. No

---

[274] TAVARES, André Ramos. *Direito Constitucional da Empresa*. Rio de Janeiro: Forense, 2013. p. 80-87.
[275] Ibidem. p. 62-70.

entanto, a Defesa Cibernética é uma ocupação que o Estado deve tomar também para si a fim de preservar os interesses sociais que ele representa. Modernamente, não se pode imaginar uma proteção adequada sem adentrar no espectro da segurança cibernética.

### *3.2.2 O Direito Digital e a busca pela coesão social*

A preservação de tecnologias que geram desenvolvimento socioeconômico também é de interesse da sociedade, que pode contribuir com as empresas por meio de políticas públicas. Uma das grandes vulnerabilidades dos dados estratégicos das empresas está no risco de vazamento por meio de redes informáticas.

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

As empresas podem ser colocadas como uma das formas de fomento da coesão social, pois compartilham sinergicamente de objetivos relevantes para o bem comum da sociedade em que está inserida, como regra. Reflexos da coesão social que uma empresa pode proporcionar são encontrados em diversos ramos do Direito.

O Direito Digital tem raízes nos princípios fundamentais retratados na Carta Constitucional, mas está presente nas mais diversas áreas do Direito, tais como no Empresarial, Civil, Autoral, Contratual, Econômico, Financeiro, Internacional, dentre outros ramos. O Direito Digital é subsidiado por princípios tradicionais. A norma antiga é, em grande parte, aplicável a hipóteses em que se utilizam novas tecnologias. O que pode acontecer é uma análise mais aprofundada da norma por parte de quem interpreta e de quem aplica as referidas normas. Novas tecnologias agregam ao mundo jurídico peculiaridades e desafios. Tal fato advém de novos comportamentos massificados em razão das novas formas de interagir em sociedade. Trata-se de novos procedimentos que devem ser regulados pelo Direito. Considere-se que a norma possui limitação temporal, como também possui uma atuação limitada em razão do espaço (territorialidade). A

velocidade das transformações se mostra como um desafio à normatização de determinadas condutas[276].

O Direito Digital atende a uma sociedade marcada pela mudança de comportamentos em razão de novas tecnologias. A mudança comportamental é evidente nos negócios e nas relações entre indivíduos. Patrícia Peck Pinheiro cita a adoção cada vez mais frequente de um "Regime de Coopetição" (cooperação adicionado à competição), caracterizado pela necessidade cada vez maior das empresas de buscar a sobrevivência em um ambiente competitivo, globalizado e, principalmente, conectado. Na análise da autora, "empresas isoladas tendem a naufragar"[277]. Assim sendo, aumenta a importância da defesa cibernética. É para o bem da empresa que se deve prover esta segurança, mas é para o bem da comunidade e do Estado que esta proteção seja efetiva. Num mundo onde os bens intangíveis são valiosos para toda a sociedade e muitos deles circulam na rede, a segurança passa a ser requisito para a sobrevivência, principalmente das empresas.

### *3.2.3 O Estado Regulador e sua contribuição para a coesão social*

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

Na hipótese de algum agente deter um poder econômico desproporcional com relação a seus concorrentes, o mercado tende a concentrar poder e gerar desequilíbrio entre concorrentes. Por vezes o fenômeno da concentração econômica é lícito e desejável, quando, *v.g.*, se deseja fortalecer sociedades empresárias por meio de fusão, participação, aquisição[278]. Algumas das hipóteses apresentadas podem ser até

[276] PINHEIRO, Patrícia Peck. *Direito Digital*. 2. ed. São Paulo: Saraiva, 2007. p. 29-35
[277] Ibidem. p. 55-56
[278] TAVARES, André Ramos. *Direito Constitucional da Empresa*. Rio de Janeiro: Forense, 2013. p. 48-51.

fomentadas por um Estado que deseja fortalecer sua indústria, mas definitivamente a espionagem cibernética não coaduna com justiça social.

Nesse aspecto, ressalta-se que o poder econômico pode ser entendido como a detenção dos meios de produção, podendo estar concentrado até mesmo em uma única pessoa[279]. Tais meios, na posse ou propriedade de uma sociedade empresária, são constitucionais e permitidos. O legítimo uso do poder econômico não sofre quaisquer restrições, sendo essencial para o desenvolvimento social[280]. Gera empregos de qualidade, renda e eventualmente nacionaliza ou desenvolve tecnologias, produtos e serviços.

A regulação, neste campo, é naturalmente influenciada pela tecnologia: mais um *steakholder* dessa grande negociação social. Assim como a tecnologia é protagonista na regulação da internet, o mesmo acontece na defesa cibernética. Outra peculiaridade: como é um assunto que grande parte da sociedade ignora, aumenta a responsabilidade de quem influi nesta decisão. A ignorância pode facilitar a manipulação nas políticas públicas, o que não interessa para a comunidade.

Outro aspecto a ser considerado é a regulação nos outros países, pois exercem forte influência no que, de fato, acontece na internet. Como se sabe, o tema merece uma regulação específica, mas regular a guerra tem sido sempre um processo lento e difícil. Não se espera que com a guerra cibernética seja muito diferente. Agências reguladoras de meios de comunicações como a ANATEL no Brasil; e mesmo a legislação, como o Marco Civil da Internet, não consideram o estado de guerra contínua, apesar de ser uma característica da guerra cibernética.

Por mais, *v.g.*, que o Marco Civil privilegie a privacidade, diante de potencial forte ameaça, tal direito poderá dar lugar a outros não menos importantes em determinado contexto. Conforme preceituado no art. 5º da CR/88, a segurança jurídica é um direito relevante quando se trata de atividade empresarial. E essa garantia tem reflexos no pugilato cibernético. A previsibilidade é um dos indícios de segurança

---

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

[280] TAVARES, André Ramos. *Direito Constitucional Econômico*. 3. ed. São Paulo: Método, 2006. v. 1. p. 261-262.

jurídica[281]. A manutenção do Direito em ambiente virtual não depende apenas de normas que amparem relações sociais em uma rede informática.

A desejável supremacia técnica ou a possível superioridade não podem ser obtidas sem investimento sistêmico e esforço social materializado em políticas públicas concretizadas por meio de regulação adequada. Tal fato pode ser constatado por meio de um simples exercício de raciocínio: via de regra, os profissionais que oferecem serviços de Defesa Cibernética, assim como todos os profissionais, desejam saber exatamente o risco inerente do exercício de sua profissão para que possam cumprir suas atribuições de forma segura e na medida que a sociedade deseja. Isto partindo do pressuposto de que a sociedade deve decidir o que é melhor para si.

Ademais, o Estado Administrativo, segundo entendimento de Marcio Iorio Aranha, possui a virtude de tornar convergentes noções de profissionalismo e expertise tradicionalmente aplicadas aos negócios privados, para que sejam aplicadas no contexto da atividade de governar com a conotação de permanência, treinamento, especialização de funções[282]. Trata-se de uma forma de reconhecimento de que as empresas têm muito o que ensinar ao Estado para que ele sirva à sociedade de forma eficaz. O autor afirma ainda que, num contexto de direitos fundamentais objetivados e de Estado Regulador, o adensamento do conteúdo dos direitos fundamentais pode ser auxiliado de forma relevante pela regulação[283]. Pode-se concluir deste entendimento que o Estado que se beneficia dos préstimos de sociedades empresárias pode ainda oferecer um melhor serviço para pessoas físicas e jurídicas por meio de adequada regulação.

O controle essencialmente político das atividades de defesa cibernética poderia deixar a sociedade refém de um governo mal-intencionado que desejasse se utilizar de dados coletados em favor de um controle sobre a população.

Discorrendo acerca das expectativas de uma sociedade democrática frente ao seu governo, Carlos Ayres Britto ressalta que "o judiciário não tem do governo a função, mas tem do governo a força. A força de impedir o desgoverno, que será tanto pior

---

[281] TAVARES, André Ramos. *Direito Constitucional Econômico*. 3. ed. São Paulo: Método, 2006. v. 1. p. 78-79.
[282] ARANHA, Marcio Iorio. *Manual de Direito Regulatório*: Fundamentos de Direito Regulatório. 2. ed. Coleford, UK: Laccademia Publishing, 2014. p. 11-15.
[283] Ibidem. p. 9-11.

quanto resultante do desrespeito à Constituição"[284]**.** Ele sugere que a governabilidade, tornada práxis, corresponderá ao clímax do humanismo e da democracia.

Pode-se concluir que todos devem respeitar os limites ditados pela Constituição para que o Estado seja o que a sociedade deseja. Destarte, por meio de adequada regulação, que passe ao largo do controle político, a sociedade poderá mensurar os investimentos e procedimentos que são úteis para que a comunidade alcance seus objetivos. Mitigando o mau uso de redes informáticas, quer pela educação e pelo Direito quando isso for possível, quer por técnicas de defesa cibernética para fazer valer a norma quando for necessário, o Estado contribuirá com a sociedade no sentido de preservar a paz social e outros valores.

No capítulo 4, sugerem-se outras maneiras de fomentar o desenvolvimento da Defesa Cibernética por meio de políticas públicas, com benefícios para o Estado representando a comunidade e para sociedades empresárias, que tendem a melhorar a qualidade de vida das pessoas.

[284] BRITTO, Carlos Ayres. *O humanismo como categoria constitucional*. Rio de Janeiro: Ed. Forum, 2012. p. 116.

# 4 A MITIGAÇÃO DE RISCOS ORIUNDOS DO PUGILATO CIBERNÉTICO POR MEIO DE POLÍTICAS PÚBLICAS

O êxito do pugilato cibernético depende de investimento em inovação tecnológica relacionada com o setor. Mesmo fora das fronteiras do aludido pugilato, pode-se constatar que a importância do tema inovação tecnológica é inegável. Na percepção do professor Kim, a ciência e a tecnologia parecem ter sido a chave do desenvolvimento dos países avançados[285]. A inovação fomentada pelo Estado moderno pode ser otimizada baseando-se no conceito de tripla hélice, em que há investimento do Estado fomentando a indústria e o meio acadêmico – incluindo no conceito outros institutos de pesquisa e difusão[286].

O fomento à inovação costuma funcionar melhor com políticas públicas bem planejadas e executadas de forma contínua. Nas últimas décadas, principalmente a partir da década de 1960, a Coreia do Sul tem conseguido passar por uma grande transformação: de uma economia baseada em agricultura de subsistência, pode hoje ser considerada uma economia moderna e ágil [287]. Durante muitos anos, a Coreia do Sul apresentou crescimento anual expressivo, e hoje pode ser tida como paradigma de aumento de renda, já sendo uma potência econômica mundial com crescimento notável nas exportações.

O crescimento sul-coreano iniciou-se em razão da industrialização baseada na imitação, e a partir desta imitação iniciou-se um processo de inovação contínua, combinando elementos trazidos de outros países – às vezes importados a partir de transferência tecnológica e de conhecimento – que possibilitaram produção local e inovação a partir da solução de necessidades existentes[288].

Para o caso do pugilato cibernético, pode-se dizer que acessar o código-fonte de *softwares* abertos – principalmente se forem comentados – e aperfeiçoá-los é uma das formas de se desempenhar inovação contínua, combinando os elementos já existentes com novidades que auxiliem em problemas específicos. Outrossim, o acesso ao código-

---

[285] KIM, Linsu. *Da Imitação à Inovação*: a Dinâmica do Aprendizado Tecnológico da Coréia. Campinas: Unicamp, 2005. p. 7.
[286] ETZKOWITZ, H. Reconstrução criativa da Hélice Tripla e Inovação Regional. In: *Revista Inteligência Empresarial*. N. 23. Rio de Janeiro: Editora e-papers, 2005.
[287] KIM, Linsu, op. cit, . p. 13-14.
[288] Ibidem. p. 27-29.

fonte, por si só, pode ser uma forma de se implementar transferência de tecnologia, desde que seja compreendido e seja novidade para quem o acessa. A decisão da Ação ADI 3.059 / RS contribui para que o desenvolvimento brasileiro neste campo seja alcançado.

Para a compreensão da leitura do código-fonte, os institutos difusores de conhecimento devem ter condições de preparar indivíduos para se tornarem profissionais que atuarão no campo da defesa em redes. Cresce ainda de importância uma formação básica bem estruturada, assim como um ensino médio de qualidade, sem o quê a compreensão da tecnologia é manifestamente dificultada.

O Estado tem muitas razões para empreender, e as razões passam pelo fortalecimento da própria sociedade. Será compensador o investimento realizado pelo Estado em favor da inovação que agrega valor a produtos voltados para exportação, como no modelo coreano. No caso da inovação no setor cibernético, a tecnologia adquirida pode agregar valor relevante a produtos e serviços, num ciclo virtuoso que pode realimentar a pesquisa. Independentemente da ação de beligerância do Estado que motivou o desenvolvimento na área cibernética, o investimento tende a ter um resultado de aproveitamento tecnológico dual, aproveitável inclusive para melhorar a qualidade de bens e serviços para a exportação, além de melhor capacitar o país para o pugilato cibernético.

Em tal contexto, a percepção comum é de que investimentos em inovação no campo de redes de computadores e de meios informáticos podem ser especialmente vantajosos para a sociedade. Investir em inovação no setor cibernético propicia ao mesmo tempo qualidade de vida e segurança: qualidade de vida pela fruição, uso e gozo da inovação; e segurança pelo fato de o conhecimento ser útil para a defesa nacional contra possíveis ameaças que trafegam na rede. O ideal é que a inovação seja incentivada pelo Estado, a partir de políticas públicas com objetivos bem definidos.

A seguir, evidenciar-se-á por meio de estudo de casos que esta meta pode ser alcançada mediante uma aplicação mais eficiente de recursos.

## 4.1 A necessidade de aparelhamento do Estado no setor cibernético

A solução para a defesa cibernética passa necessariamente pelo tratamento dos dados de vigilância cibernética, assim como pela celebração de acordos internacionais. A comunidade internacional tem agido de forma cada vez mais colaborativa. Um acordo global diminuiria o risco de beligerância, melhorando as relações[289]. A matéria referente a tratamento de dados tem merecido regulamentação, como ocorre na Itália desde 2003. Este país publicou importante norma relacionada ao tema "tratamento de dados pessoais": o Decreto Legislativo 196, de 30 de junho de 2003[290].

---

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

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

"TITOLO X - COMUNICAZIONI ELETTRONICHE

CAPO I - SERVIZI DI COMUNICAZIONE ELETTRONICA

Art. 121 (Servizi interessati)

1. Le disposizioni del presente titolo si applicano al tratamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni.

Art. 122 (Informazioni raccolte nei riguardi dell'abbonato o dell'utente)

1. Salvo quanto previsto dal comma 2, è vietato l'uso di uma rete di comunicazione elettronica per accedere a informazioniarchiviate nell'a pparecchio terminale di un abbonato o di um utente, per archiviare informazioni o per monitorare le operazioni dell'utente.

2. Il codice di deontologia di cui all'articolo 133 individua i presupposti e i limiti entro i quali l'uso della rete nei modi di cui al comma 1, per determinati scopi legittimi relativi ala memorizzazione tecnica per il tempo strettamente necessário alla trasmissione della comunicazione o a fornire uno specifico servizio richiesto dall'abbonato o dall'utente, è consentito al fornitore del servizio di comunicazione elettronica nei riguardi dell'abbonato e dell'utente che abbiano espresso il consenso sulla base di una previa informativa ai sensi dell'articolo 13 che indichi analiticamente, in modo chiaro e preciso, le finalità e la durata del trattamento.

Art. 123 (Dati relativi al traffico)

1. I dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei commi 2, 3 e 5.

2. Il trattamento dei dati relativi al traffico strettamente necessari a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessária per effetto di una contestazione anche in sede giudiziale.

3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico può trattare i dati di cui al comma 2 nella misura e per la durata necessarie a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, solo se l'abbonato o l'utente cui i dati si riferiscono hanno manifestato il próprio consenso, che è revocabile in ogni momento.

4. Nel fornire l'informativa di cui all'articolo 13 il fornitore del servizio informa l'abbonato o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del medesimo trattamento ai fini di cui ai commi 2 e 3.

5. Il trattamento dei dati personali relativi al traffico è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'articolo 30 sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni e che si occupano della fatturazione o della gestione del traffico, di analisi per conto di clienti, dell'accertamento di frodi, o della commercializzazione dei servizi di comunicazione elettronica o della

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

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

O art. 132 do referido Decreto Legislativo italiano trata sobre coleta de dados e tratamento de dados dentro do respeito às medidas e meios de garantia do interessado[291]. Numa análise sistemática da norma, conclui-se que ela abrange, inclusive, comunicações telefônicas. Deve-se destacar que parte das comunicações telefônicas existentes hoje no Brasil e no mundo acontece tecnicamente na internet, por meio de tecnologias como voz sobre IP (VOIP), ou por outras formas de trânsito de dados. Do exposto, pode-se concluir que também esta forma de comunicação depende da proteção cibernética, até porque, mesmo quando a comunicação não se dá por meio de redes informáticas, estas normalmente são utilizadas no gerenciamento de comunicações telefônicas "tradicionais".

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

---

prestazione dei servizi a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessário per lo svolgimento di tali attività e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata. 6. L'Autorità per le garanzie nelle comunicazioni può ottenere i dati relativi alla fatturazione o al traffico necessari ai fini della risoluzione di controversie attinenti, in particolare, all'interconnessione o alla fatturazione. [...]

[291] Art. 132 (Conservazione di dati di traffico per altre finalità)
1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico sono conservati dal fornitore per trenta mesi, per finalità di accertamento e repressione di reati, secondo le modalità individuate con decreto del Ministro della giustizia, di concerto con i Ministri dell'interno e delle comunicazioni, e su conforme parere del Garante."

Se os instrumentos normativos mencionados fossem tomados como parâmetro, certamente protegeriam também pessoas jurídicas, consoante doutrina e jurisprudência brasileiras apresentadas no capítulo 3. Seria, ao mesmo tempo, um limite das atividades empresariais e uma proteção contra os excessos das mesmas atividades. No contrassenso, a França adotou recentemente uma legislação que permite uma postura bastante intrusiva nos dados que circulam na internet com a finalidade de uma maior proteção contra o terrorismo. O mesmo acontece nos Estados Unidos, mesmo com a substituição do *Patriotc Act*, tema já abordado.

Outro instrumento transnacional que trata do tema são as Linhas Diretrizes da OCDE, altamente ligada ao Direito Empresarial e à realidade brasileira: desde 2013, o governo do Brasil cria formas de implementar tais diretrizes em empreendimentos sob sua jurisdição[292]. É importante frisar que a norma vigente em um país pouco pode influenciar sobre o que de fato acontece no mundo a respeito do pugilato cibernético, e todas as decisões sobre o tema devem considerar esta realidade.

A partir do suposto desentendimento entre empresas – Google, Facebook, Microsoft e Apple – e a polícia federal estadunidense – o FBI –, pôde-se chegar a algumas conclusões. A controvérsia tem início quando a polícia federal estadunidense requisita à Apple que recupere os dados contidos em um telefone da marca, de propriedade de um terrorista islâmico. No entanto, o FBI não solicitou a recuperação apenas de tais dados, solicitou um *backdoor* no IOS, o sistema operacional do iPhone. A Apple teria se negado a atender a requisição do FBI. O departamento de justiça estadunidense considerou a negativa da empresa uma estratégia de marketing. Tim Cook, CEO da Apple, explicou que o que o FBI determinou seria o equivalente, no mundo físico, a uma chave-mestra capaz de abrir centenas de milhões de fechaduras, sendo tal determinação inaceitável, segundo ele. As outras empresas citadas no parágrafo se posicionaram a favor da Apple[293].

O *backdoor* requisitado pode ser entendido como uma ferramenta capaz de entregar para o FBI todos os dados que circulam no *smartphone*. Isso pode ser

---

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

[293] VILICIC, Filipe. A Guerra entre a Apple e o FBI. *Revista Veja*. ed. 2466. São Paulo: Abril, 2016. p. 68-69.

comparado, no que diz respeito à privacidade (e intimidade), a uma porta desconhecida do dono de uma casa – contribuinte do governo e que paga seus impostos – cujas chaves ficam sob a guarda do governo, que pode entrar e sair conforme sua conveniência, sem que o dono tome conhecimento. É algo realmente muito grave. Observa-se que, além do representante do governo poder entrar pela porta – o que já é um absurdo –, ainda causa a vulnerabilidade para o dono da casa, pois, pela tal porta desconhecida, também pode entrar um ladrão para subtrair bens do contribuinte.

Pode-se depreender do caso que a população deve ser protegida dos crimes, de ilegalidades e dos excessos dos agentes públicos. Para isso, o mandamento legal deve evitar a possibilidade de interpretações polêmicas como a apresentada pelo FBI. No entanto, deve-se permitir que o Estado vigie o necessário para que a comunidade permaneça em segurança.

Na hipótese de a suprema corte americana compartilhar o entendimento manifestado pelo FBI, a despeito dos direitos tutelados em outros países, o governo estadunidense terá os meios necessários para invadir o iPhone de quem quer que seja, salvo se algum aparato tecnológico estrangeiro inesperado e operado por alguém com capacitação compatível impedir o objetivo almejado. Lembre-se que o *Patriotic Act* já deu lugar a uma nova lei, supostamente menos intrusiva para os americanos.

Políticas públicas, preferencialmente implementadas a partir de leis, podem auxiliar a sociedade neste processo de maturação, para que o Estado seja cada vez mais eficaz. Meios utilizados no pugilato cibernético podem proteger até mesmo contra o cyber terrorismo, assim como auxiliar muitas investigações estratégicas para uma nação.

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

Mitigando o mau uso de redes informáticas – seja pela educação e pelo Direito, quando isso for possível, seja por técnicas de defesa cibernética para fazer valer a norma, quando for necessário – o Estado contribuirá com a sociedade no sentido de preservar a paz social e outros valores.

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

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

## 4.2 Políticas públicas voltadas para inovação e tecnologia

Os Estados Unidos investiram vultuosos recursos em atividades empreendedoras a fim de estimular a inovação. Nesse contexto, podem-se citar exemplos de êxito como o da Agência de Projetos de Pesquisa Avançada de Defesa (DARPA), o Programa de Pesquisa para a Inovação em Pequenas Empresas (SBIR) e a Iniciativa Nacional de Nanotecnologia. Todos esses projetos representaram uma abordagem proativa do Estado americano com escopo de moldar um mercado que impulsionasse a inovação naquele país.

Implementaram-se políticas públicas com visão estratégica em atividades altamente inovadoras, com pesquisas de risco que o Estado tomou pra si com foco no desenvolvimento socioeconômico[294]. Por certo, o governo norte americano previa utilizar empresas que agregassem valor tecnológico a seus produtos para alcançar seus objetivos estratégicos.

Ainda para ilustrar os casos de êxito para o país quando o poder público assume investimentos e riscos, destaca-se o caso da Apple. Produtos revolucionários como iPhone, iPad e iPod possuem tecnologias básicas incorporadas que são resultantes de décadas de investimento estatal em inovação. Grande parte da tecnologia incorporada a

[294] MAZZUCATO, Mariana. *O Estado Empreendedor*: Desmascarando o Mito do Setor Público vs. Setor Privado. Trad. Elvira Serapicos. São Paulo: Portifolio-Penguin, 2014. p. 109-125.

esses produtos foi desenvolvida por meio de esforços de pesquisa e apoio financeiro do governo e das Forças Armadas estadunidenses[295].

Neste ponto, abrem-se parênteses sobre o suposto desentendimento já citado entre a Apple e o FBI. Caso exista controvérsia entre eles, há forte tendência de superação em razão de serem parceiros há muito tempo, e aparentemente possuem muitos interesses convergentes, sobretudo no que diz respeito à inovação.

O Estado pode e deve, dentro de suas possibilidades, investir em inovação e tecnologia. Tais investimentos auxiliarão o desenvolvimento socioeconômico e, por consequência, o desenvolvimento do Estado. Com o mesmo empenho que o Estado deve agir sinergicamente com o meio acadêmico e as empresas, gerando emprego e renda (modelo da tríplice hélice), deve zelar pela manutenção destas conquistas da sociedade. Uma das formas de fazê-lo é investindo em defesa cibernética e oferecendo tal proteção para a sociedade.

Como já se relatou, ataques cibernéticos podem causar grandes transtornos para empresas, bancos, governos e para a comunidade em geral. Recentemente, foi noticiado que a Bolsa de Valores de Nova Iorque, a companhia aérea *United Airlines* e o jornal estadunidense *Wall Street Journal* teriam sido vítimas de falhas técnicas em suas redes informáticas. A Bolsa de Valores de Nova Iorque, por exemplo, ficou fechada por quase quatro horas no dia 8 de julho de 2015. No mesmo dia, a empresa americana *United Airlines* ficou por duas horas sem operar qualquer voo em todo o mundo; o *Wall Street Journal*, por sua vez, ficou com sua página fora do ar por alguns momentos e instável por período mais longo. Ainda que tenha sido desmentido pelo próprio FBI[296], sites internacionais indicaram um possível ataque *hacker* direcionado para grandes instituições corporativas dos Estados Unidos[297].

A partir dos casos citados, percebe-se uma pequena amostra do potencial de ataques cibernéticos. A despeito de terem causado grande transtorno e prejuízo nas ocasiões mencionadas acima, eles representam muito pouco em face do potencial de

---

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

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

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

ataques cibernéticos. A comunidade, ainda que não tenha consciência plena do perigo, precisa de proteção contra tais ameaças.

Julian Assange, do sítio WikiLeaks, que permaneceu recluso por alguns anos na embaixada do Equador em Londres, opina sobre o prejuízo que a sociedade brasileira, incluindo-se suas empresas, podem ter com uma eventual inércia do governo brasileiro em não se defender de atos de espionagem que podem se dar também por meio de ataques cibernéticos. Afinal, não se pode garantir que a espionagem contra autoridades e empresas brasileiras foi encerrada[298]. Tal assertiva evidencia a possibilidade de prejuízos significativos ao Brasil e seus contribuintes, até que a espionagem contra brasileiros possa, ao menos, ser identificada tecnicamente. Incluem-se ainda nesse risco a possibilidade de sabotagem e outras técnicas prejudiciais em redes informáticas.

O desenvolvimento tecnológico necessário a um bom resultado no campo cibernético é potencializado por um Estado que atue como empreendedor. Por meio de análise schumpeteriana e keynesiana, Mariana Mazzucato mostra que o Estado deve, para o bem da sociedade, cumprir um papel de empreendedorismo, assumindo riscos, criando mercados. A autora destaca a importância do financiamento orientado e dos contratos públicos[299].

Destaca-se o papel do Estado nas incubadoras de inovação e empreendedorismo, como no caso do Vale do Silício. A autora discorre que o Estado pode ser um empreendedor corajoso, tendo sido o grande responsável por inovações como a internet, GPS, telas sensíveis ao toque, comando por voz. Ela questiona se o mercado realizaria tal investimento por iniciativa própria[300]. Nesse ponto, deve-se ressaltar que nenhuma das tecnologias citadas foram desenvolvidas sem que houvesse o interesse do Estado como suporte para tal empreendimento. Este interesse normalmente passa pelo que se conhece por produto de uso dual.

Os investimentos estatais que propiciaram as inovações observadas trouxeram consigo sempre este grande objetivo comum. Observe-se: a internet tem sido responsável por fomentar a pesquisa entre universidades; por outro lado, pode ser uma

---

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

[299] MAZZUCATO, Mariana. *O Estado Empreendedor*: Desmascarando o Mito do Setor Público vs. Setor Privado. Trad. Elvira Serapicos. São Paulo: Portifolio-Penguin, 2014. p. 7-22.

[300] Ibidem, p. 23-26.

poderosa ferramenta de mitigação da privacidade; ela foi estudada como ferramenta para atividades militares desde a sua origem.

O GPS tem também estreita ligação com atividades militares. Nota-se que as tecnologias apresentadas neste tópico possuem utilidade dual: são úteis tanto para a sociedade civil quanto para atividades militares do Estado. Tal constatação se evidencia quando se fala de desconcentrar o comando da internet ou quando se ouve falar de concorrentes ao sistema de GPS. Em ambos os casos, o que se busca é segurança adquirida por meio da independência.

O que se pretendeu destacar é que o investimento estatal normalmente será mais útil se tiver objetivo dual. Esse financiamento deve ser precedido de sério planejamento que anteveja formas de dissuadir a corrupção quando do emprego dos recursos públicos: a espionagem, a venda de dados ou informações e quaisquer outras formas de riscos aos projetos.

Mazzucato evidencia que países periféricos da zona do euro, como Portugal e Itália, se caracterizam por um setor público estagnado e que não foi capaz de realizar investimentos estratégicos como os que países como a Alemanha vem fazendo há décadas. A autora nomeia com clareza que são necessários investimentos em educação, capital humano, pesquisa e desenvolvimento (P&D).

Ante o axioma de que a austeridade traz necessária e suficientemente o crescimento, a autora contra argumenta com o exemplo dos Estados de dívida mais alta que cresceram de forma estável, como Canadá, Austrália e Nova Zelândia[301]. Pode-se analisar de forma semelhante com as pessoas físicas: austeridade não é sinônimo de desenvolvimento; da mesma forma, o endividamento com planejamento, responsabilidade e trabalho pode trazer excelentes oportunidades, principalmente se conseguido com baixos juros.

Investimentos privados são baseados normalmente na percepção de risco, o que faz com que o Estado esteja por trás das grandes revoluções tecnológicas e longos períodos de crescimento. Tal fato acontece pois a inovação costuma trazer consigo um

[301] MAZZUCATO, Mariana. *O Estado Empreendedor*: Desmascarando o Mito do Setor Público vs. Setor Privado. Trad. Elvira Serapicos. São Paulo: Portifolio-Penguin, 2014. p. 43-44.

grande risco em seus estágios iniciais de desenvolvimento, os quais normalmente só são suportados pelo setor público[302].

Como exemplo de sucesso brasileiro financiado pelo Estado em razão do grande risco presente quanto à possibilidade de retorno de investimento em inovação tecnológica, pode-se citar o carro de combate Osório, produzido nos anos 1980 pela ENGESA. Tal empreendimento competiu, em uma concorrência na Arábia Saudita, com o Challenger inglês, o M1 Abrams estadunidense e o AMX-40 da França, tendo sido considerado o melhor carro de combate na ocasião[303]. Em 1988, em Abu Dhabi, competiu ainda com o italiano C-1 Ariete, sendo mais uma vez considerado o melhor[304]. Trata-se de um exemplo bem-sucedido de investimento público, em que pese o fechamento posterior da ENGESA. Outro caso de sucesso é notório: a EMBRAER, que nasceu de investimentos do Estado – em particular da Força Aérea Brasileira – em tecnologias duais.

Deve-se atentar ainda para que os ecossistemas de inovação possuam relações simbióticas e não parasitárias[305], o que pode ser traduzido numa linguagem típica de negociação: a parceria entre o agente público e o privado deve estar centrada no "ganha-ganha". Se uma das partes segue perdendo, não haverá sustentabilidade na relação. O "ganha-ganha" definitivamente não acontece com financeirização[306] do setor privado. Nesta hipótese, perde a sociedade.

Mazzucato usa um conceito interessante importado da Holanda, em que o crédito fiscal para P&D visa empregos, e não o tradicional, que seria receita[307]. Trata-se de uma ideia que pode ser especialmente interessante para a sociedade que financia o Estado empreendedor. A geração de empregos de qualidade alivia a sociedade e realimenta as atividades do Estado com suas políticas de crescimento com vistas a uma

---

[302] MAZZUCATO, Mariana. *O Estado Empreendedor*: Desmascarando o Mito do Setor Público vs. Setor Privado. Trad. Elvira Serapicos. São Paulo: Portifolio-Penguin, 2014. p. 50-51.

[303] FORÇAS TERRESTRES. *Osório*: o MBT brasileiro que bateu o M1 Abrams. Disponível em: <http://www.forte.jor.br/2008/09/21/osorio-o-mbt-brasileiro-que-bateu-o-m1-abrams/>. Acesso em: 18 ago. 2015.

[304] NOTÍCIA MILITAR. EE-T1 *Osório volta a ser fabricado*. Disponível em: <http://noticiamilita.blogspot.com.br/2012/11/ee-t1-osorio-volta-ser-fabricado_16.html>. Acesso em: 18 ago. 2015.

[305] MAZZUCATO, Mariana. op. cit. p. 52.

[306] Exemplo de financeirização acontece com hipóteses, v.g., de recompra das próprias ações com objetivo de valorizar artificialmente uma empresa. Trata-se de um conceito utilizado por Mariana Mazzucato no livro O Estado Empreendedor.

[307] MAZZUCATO. Mariana, op. cit. p. 89.

melhor qualidade de vida aos que o financiam. De toda forma, todo e qualquer investimento estatal deve ser precedido de cautelas para evitar que os frutos dos investimentos sejam perdidos em favor dos que não arcaram com os riscos da pesquisa. Se o BNDES (Banco Nacional do Desenvolvimento) financia pesquisas e desenvolvimento de fármacos, o governo brasileiro deve garantir que as empresas que tiveram êxito em suas pesquisas não sejam vendidas para grupos transnacionais que não tenham compromisso com a geração de impostos, empregos e renda no país que financiou uma pesquisa exitosa.

Quando uma empresa inovadora e com pesquisas financiadas pelo Estado é vendida para um grupo transnacional, as tecnologias por ela desenvolvidas são exportadas para o comprador estrangeiro. Não é incomum que os compradores transnacionais mantenham atividades realmente estratégicas junto a suas matrizes, realizando nos países em que possuem filiais apenas atividades secundárias, menos rentáveis e que não demandam pesquisas.

Nas hipóteses levantadas, ganha o privado mediante grande prejuízo do público que arcou com os riscos da pesquisa. Tal hipótese pode e deve ser evitada por meio da previsão de pesadas multas, que inviabilizem a venda de inovadores financiados pelo Estado para grupos que não sejam nacionais.

Por trás de tecnologias inovadoras como as citadas – internet, comandos por voz, tela sensível ao toque, GPS – tem sido sistemático o investimento estatal, com destaque àqueles que são realizados por meio das Forças Armadas. É o caso de grande parte das tecnologias críticas incorporadas aos produtos Apple, por exemplo[308]. Muitas outras tecnologias poderiam ser citadas, como a própria tecnologia de telefonia digital CDMA: possui relativa segurança e eficiência na propagação, também foi desenvolvida inicialmente com objetivos militares, tendo posteriormente excelente aplicação civil.

Ao que parece, tem valido a pena investir para que as Forças Armadas e outros órgãos de segurança estejam bem aparelhados e, dentro do possível, com tecnologia nacional. Guardadas as particularidades e a cultura beligerante deste país, nos Estados Unidos estes frutos só ficam mais evidentes.

---

[308] MAZZUCATO, Mariana. *O Estado Empreendedor*: Desmascarando o Mito do Setor Público vs. Setor Privado. Trad. Elvira Serapicos. São Paulo: Portifolio-Penguin, 2014. p. 126-133.

Podem ser citados outros exemplos de inovação capitaneada por Forças Armadas: tecnologias ligadas a processamento e armazenamento informatizado de dados, semicondutores, química do estado sólido, telas capacitivas sensíveis ao toque, *click wheel*, tecnologias relacionadas a protocolos de redes, baterias[309].

O conceito de tripé[310] de inovação remete à difusão do conhecimento, no entanto, ele é aplicável mesmo quando se fala em desenvolvimento de tecnologias sigilosas. Conclui-se que projetos dessa natureza podem possuir aspectos pontuais cuja difusão deve ser restrita, sendo-lhes dado tratamento especial.

No Brasil, tecnologias ligadas a radares e sensores eletromagnéticos – tidas como sensíveis e de difícil acesso – vem sendo fomentadas pelo Departamento de Ciência e Tecnologia (DCT) do Exército Brasileiro, podendo trazer bons frutos para a indústria nacional.

A Estratégia Nacional de Defesa e o Livro Branco de Defesa, já abordados no presente estudo, materializam as políticas públicas atinentes à defesa cibernética de forma mais geral. Em sentido estrito, as aludidas políticas públicas são referidas no Livro Verde: segurança cibernética no Brasil.

A END enumera as diretrizes estratégicas atinentes a cada uma das forças armadas, indicando o portfólio desejável a cada uma delas. Conforme visto, lado-a-lado com tais diretrizes, são abordados os papéis decisivos para a defesa nacional, dentre os quais o cibernético. Tal política pretende assegurar a independência nacional, sendo tal independência resguardada pelas forças armadas. Trata de pautas decisivas para a segurança de um país, ditando a estratégia e os meios para que a sociedade participe de tal defesa. A política posiciona a tecnologia no contexto como mais um instrumento de combate, sendo o monitoramento/controle um dos vetores do trinômio, que junto à mobilidade e à presença resulta a capacitação de cada uma das forças armadas. A capacidade de monitorar e controlar é colocada como base para que a sociedade representada nas forças armadas responda rapidamente às ameaças e agressões. A capacitação da indústria para que esta domine tecnologias indispensáveis à defesa

---

[309] MAZZUCATO, Mariana. *O Estado Empreendedor*: Desmascarando o Mito do Setor Público vs. Setor Privado. Trad. Elvira Serapicos. São Paulo: Portifolio-Penguin, 2014. p. 133-157.

[310] O tripé de inovação consiste no investimento sinérgico por parte do Estado, meio acadêmico e indústria, no desenvolvimento de determinada tecnologia, normalmente com o risco assumido pelo Estado. Trata-se de um modelo consagrado e de êxito quando se foca em inovação.

também é sinalizada na END, buscando assegurar, inclusive, recursos financeiros para as empresas estratégicas de defesa. Apesar da sinalização de aporte de recursos, acena também a END com o fomento da rentabilidade da mesma indústria e com capacitação tecnológica independente. O Brasil, conforme a END não pretende ser comprador, mas parceiro de fornecedores estrangeiros quando a importação for a única solução. A inovação, pela Estratégia, também é vetor de desenvolvimento a ser fomentada por todos os meios disponíveis. Frise-se que no contexto de tal política, a relação entre Ciência, Tecnologia e Inovação na defesa entra em sinergia com a Política de Desenvolvimento Produtivo (PDP), de 2008, coordenada pelo Ministério do Desenvolvimento, Indústria e Comércio Exterior[311].

O Livro Branco da Defesa, por sua vez, indica que é dever do Estado prover a segurança necessária para que a sociedade alcance seus objetivos. Indica ainda que o Brasil deve ter uma provisão de defesa compatível com sua estrutura econômica. Informa que a política de defesa e a política externa são complementares e indissociáveis. A criação de produtos de defesa também é alvo da política, e será incentivada dentro do que for possível. O Livro faz referência à defesa cibernética de forma categórica, constatando que o setor cibernético é essencial à segurança nacional pois controla diversos órgãos e sistemas a ela relacionados. Confidencialidade, disponibilidade, integridade e autenticidade dos dados que trafegam em redes informáticas são objetivos a serem alcançados por meio do setor de defesa cibernética, num esforço contínuo e de longo prazo. A proteção contra ataques cibernéticos deve ser perseguida também por meio de indução à inovação e fomento à indústria de defesa, também por meio da promoção de produtos que também sejam de uso civil[312].

As políticas apresentadas convergem para a proposta do presente trabalho de incentivo industrial, acadêmico e em favor da inovação da tecnologia de interesse. Ratificam ainda muitos outros conceitos explorados na presente análise, inclusive se colocando num contexto dentro de políticas públicas maiores. O Livro Verde, também já apresentado, apenas traz pormenores das políticas ora apresentadas.

---

[311] BRASIL. Ministério da Defesa. *Estratégia Nacional de Defesa*: Decreto nº 6.703/2008. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm>. Acesso em: 26 jan. 2016.

[312] BRASIL. Ministério da Defesa. *Livro Branco da Defesa Nacional*. Brasil, 2012.

Chame-se a atenção para o fomento ao monitoramento e controle da política ora apresentada, mas que deve ser realizado para que a sociedade responda prontamente às eventuais agressões, portanto não se trata de um monitoramento sem propósito. Além do que, todas as necessidades sociais aqui colocadas devem ser interpretadas de forma sistêmica.

O Livro Verde do Gabinete de Segurança Institucional da Presidência da República chama a atenção para alguns fenômenos modernos como a sistemática convergência tecnológica; interconexão e interdependência das redes de informação cada vez mais presentes; popularização da internet; avanço tecnológico de equipamentos ligados em rede, aumento das ameaças e vulnerabilidades ligadas às redes informáticas; realidade de ambientes complexos, com diversidade de interesses e contínuas mudanças; a transversalidade da segurança cibernética. Indica que muitos são os desafios e ameaças neste campo sinalizando potenciais diretrizes estratégicas para esta área de atuação. Coloca como tendência para 2020 uma revolução da infraestrutura, maior compartilhamento de dados confidenciais na rede, maior conectividade, aumento do uso de serviços bancários pela rede como também do comercio eletrônico, normas mais severas, internets múltiplas, novos modelos de relacionamento e confiança. A partir deste ambiente, são citadas diretrizes para a política nacional de segurança cibernética, abrangendo aspectos político-estratégicos, econômicos, socioambiental educacional, marco legal para a cibernética, cooperação internacional, segurança de infraestruturas críticas[313].

A partir da realidade posta, é necessário o fomento da proteção social em um campo cada vez mais complexo e dependente da tecnologia e de seu bom funcionamento. O uso racional de recursos e o bom senso na aplicação das ferramentas disponíveis para a segurança cibernética passam a ser norteadores de condutas em uma realidade jamais vivida antes pela comunidade. O estudo de caso apresentado *infra* pretende ser um exemplo de fomento que pode oferecer significativos ganhos de segurança para a sociedade e para o Estado, por meio da utilização inteligente de recursos públicos em benefício de todos os que investem no país por meio de tributos.

[313]BRASIL Presidência da República. *Livro verde*: segurança cibernética no Brasil. Brasília: GSIPR/SE/DSIC, 2010.

## 4.3 Estudo de caso: o antivírus brasileiro e sua utilidade no contexto do pugilato cibernético

Como visto, ameaças cibernéticas são uma realidade que afrontam a defesa nacional de qualquer Estado nos dias de hoje, mesmo em tempo de paz. A fim de se precaver contra ameaças virtuais, o Exército Brasileiro, por meio de seu Departamento de Ciência e Tecnologia, tem implementado projetos voltados à inovação e de cunho dual, como é o caso do projeto do antivírus brasileiro (Defesa BR) e do simulador de operações cibernéticas (SIMOC).

O SIMOC foi implementado pela empresa brasileira Decatron, tendo consumido uma quantidade maior de recursos do que o projeto do antivírus, cerca de 5,1 milhões de reais[314]. Trata-se de um projeto inovador no Brasil, que fornece tecnologia de ponta para treinamentos em guerra cibernética, podendo ser apontado como um projeto que viabilizou relevantes frutos de inovação dual.

O alcance dos projetos transcende o simples fato de existir uma proteção contra ameaças virtuais corriqueiras. Por vezes, vírus de computadores são analisados por programadores de antivírus a partir de arquivos infectados enviados pelo usuário. Quando existem informações estratégicas contaminadas por ameaças virtuais, a análise deve ser realizada por equipes da confiança do proprietário da informação. O projeto de desenvolvimento do antivírus permite que toda a análise de dados seja realizada em local conhecido e por pessoas identificáveis, com as quais se pode trocar informações com maior facilidade e segurança.

Em outros momentos, as informações estratégicas dizem respeito aos processos e sistemas informáticos em uso. Compartilhar tais informações – que podem dizer respeito à segurança de um país – com empresas estrangeiras pode potencializar riscos que seriam evitáveis caso fossem realizados no Brasil. As ferramentas de proteção informáticas não protegem apenas dados e arquivos, mas sistemas inteiros e processos lógicos.

Foi contratada a montagem de um laboratório de segurança virtual nas dependências do Exército com a finalidade de que respostas contra ameaças virtuais

[314] REDAÇÃO LINHA DEFENSIVA. *Exército brasileiro investe R$ 6 milhões em segurança e guerra digital*. Disponível em: <http://www.linhadefensiva.org/2012/01/exercio-brasileiro-investe-r-6-milhoes-em-seguranca-e-guerra-digital/>. Acesso em: 02 ago. 2015.

sejam otimizadas em razão da estrutura implementada, com a vantagem de fomentar o desenvolvimento de tecnologias nacionais de interesse da defesa cibernética brasileira. A empresa contratada para o desenvolvimento do antivírus nacional foi a BluePex Controle e Segurança, escolhida mediante processo competitivo licitatório. O gasto no projeto foi estimado em R$720,000.00 (setecentos e vinte mil reais), no decorrer de dois anos, com prestação de suporte técnico personalizado[315].

Antes do projeto, os arquivos infectados eram enviados para análise em laboratórios de empresas transnacionais, o que levou o General Antonino Santos Guerra a manifestar-se no sentido de que não tinha certeza para que região era enviado o arquivo infectado. Em virtude da contratação, o tratamento pôde ser realizado em território nacional e interagindo com técnicos que falam português[316].

Sobre o projeto do antivírus brasileiro, o Centro de Tecnologia da Informação Renato Archer (CTI)[317] declarou que o produto tem um potencial animador na ótica do Ministério da Ciência, Tecnologia e Inovação (MDIC), necessitando de escalabilidade para que o projeto seja viabilizado. A expectativa do Exército Brasileiro é de que ele seja testado ao menos no âmbito da Administração Pública Federal[318].

Projetos como os citados têm merecido recursos do Exército Brasileiro independente do fomento à inovação promovido pelo Ministério da Ciência Tecnologia e Inovação (MCTI)[319]. O CCOMGEX tem sido o órgão do Exército que coordena o projeto do antivírus nacional, por meio de um contrato de prestação de serviços tendo como objeto o desenvolvimento do produto. O produto tem sido utilizado desde a sua criação em cerca de sessenta mil terminais, dispensando a aquisição de novas licenças anuais[320]. Tal fato, além de gerar uma economia considerável, evita que sejam gastos recursos em antivírus de empresas no exterior, aumentando a geração de empregos de qualidade e renda no Brasil.

---

[315] FERRER, Rafael. *Exército usará antivírus brasileiro*. Disponível em: <http://info.abril.com.br/noticias/ti/exercito-usara-antivirus-brasileiro-01022012-8.shl>. Acesso em: 02 ago. 2015.
[316] Ibidem.
[317] CTI é uma unidade de pesquisa do MCTI.
[318] CONVERGÊNCIA DIGITAL. *Governo garante propriedade intelectual de antivirus nacional.* Disponível em: <http://tvuol.uol.com.br/video/governo-garante-propriedade-intelectual-de-antivirus-nacional-0402CC193162D4B94326/>. Acesso em: 02 ago. 2015.
[319] Ibidem.
[320] FERRER, Rafael. op.cit.

Para que se tenha ideia da otimização do gasto público proporcionada por esse projeto, a antiga fornecedora de antivírus para o Exército Brasileiro forneceu quase trinta e oito mil licenças de antivírus com validade de dois anos por aproximadamente R$ 300.000,00 (trezentos mil reais)[321], o que permite concluir que cada licença de dois anos teve um custo médio de quase oito reais. Se fossem compradas sessenta mil licenças (número inicial de máquinas em que se instalou o antivírus brasileiro) pelo mesmo valor unitário, o investimento seria de quase R$ 500.000,00 (meio milhão de reais), evidenciando assim a grande vantagem do projeto, que não chegou a oitocentos mil reais, mas que garantiu ao Exército os direitos de propriedade intelectual do programa, podendo oferecer licença de uso a quem lhe aprouver.

Apenas para evidenciar os gastos governamentais com *software* antivírus, a Receita Federal adquiriu, por meio do pregão eletrônico 17/2014 válido até dezembro de 2015, doze mil licenças do antivírus *Symantec* ao preço unitário de R$199,00 (cento e noventa e nove reais), perfazendo um total de R$2.388.000,00 (dois milhões trezentos e oitenta e oito mil reais) de investimento. O objeto do pregão foi um registro de preços para a complementação de uma solução pré-existente integrada de segurança composta dos pacotes *Symantec Protection Suite Enterprise Edition for Endpoints 4.0* mais *Symantec Antivírus For Network Attached Storage 5.2*, ou a última versão disponível à época da contratação, com implantação, suporte e treinamento de duas turmas de onze pessoas[322].

Naturalmente, a Receita Federal não pode se arriscar nas suas relevantes atividades cotidianas, levando-se em conta que o volume de ameaças sofridas diariamente pode causar enorme prejuízo à arrecadação da União. No entanto, parcerias poderiam ser viabilizadas para o desenvolvimento de um antivírus eficaz, totalmente nacional, de forma paralela à contratação citada. A seguir, são elencadas outras compras públicas recentes que também tiveram objeto a proteção de sistemas informáticos, evidenciando o alto volume de recursos públicos empregados e a possibilidade de se conseguir resultados mais relevantes para a inovação brasileira mediante atuação sinérgica de órgãos estatais.

---

[321] REDAÇÃO LINHA DEFENSIVA. op. cit.

[322] PREGÃO ELETRÔNICO DA RECEITA FEDERAL (RFB/COPOL) nº 17/2014 e seu respectivo Edital. Pregão disponível mediante busca em: <www.comprasnet.gov.br>. Acesso em: 10 ago. 2015.

A Prefeitura de Osasco (SP) planejava a aquisição de licenças de uso de *softwares* antivírus, filtragem de acesso web, treinamento e suporte. A licitação 21 de 2014 foi orçada em R$ 999.990,00 (novecentos e noventa e nove mil, novecentos e noventa reais). Está embutido no custo um suporte técnico 5x8 (dias úteis no horário de expediente da prefeitura), implementação e treinamento para administração da plataforma, inclusive desinstalando soluções antigas[323].

A Secretaria de Administração do Ministério Público Federal prevê a contratação de empresa para fornecimento de até sete mil novas licenças do *software* antivírus *TrendMicro Enterprise Security for EndPoints Advanced* e do *software TrendMicro Mobile Security* em suas versões mais recentes, com prestação de suporte técnico continuado e garantia de atualização de versão de até quase dezenove mil licenças já adquiridas. Para tanto prevê um gasto de R$ 623.000,00 (seiscentos e vinte e três mil reais)[324].

A Universidade Tecnológica Federal do Paraná previa a aquisição de solução de *software* para proteção completa corporativa contra vírus e códigos maliciosos por doze meses com um detalhe interessante: contemplando o controle de dispositivos e aplicações, controle de acesso, além de apoio na instalação e transferência de tecnologia. Trata-se de uma previsão de compra de oito mil licenças por R$ 287.920,00 (duzentos e oitenta e sete mil novecentos e vinte reais) a um custo unitário de R$ 35,99 (trinta e cinco reais e noventa e nove centavos)[325]. Numa leitura mais atenta do edital, percebe-se que o que a ementa chama de Transferência de Tecnologia é, na verdade, mera transferência de conhecimento operacional, pois aborda tópicos relativos a treinamento de uso e operação de funcionalidades básicas do *software*, a ser ministrado por profissional com certificação máxima junto ao respectivo fabricante da solução e com distribuição de material didático.

Por sua vez, o Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina (IFSC) está em fase de aquisição de licenças (perpétuas) de solução de

[323] PREGÃO ELETRÔNICO nº 021/2014 da Secretaria de Administração da Prefeitura do Município de Osasco e seu respectivo Edital. Pregão disponível mediante busca em: <www.comprasnet.gov.br>. Acesso em: 10 ago. 2015.

[324] PREGÃO ELETRÔNICO DA PROCURADORIA GERAL DA REPÚBLICA nº 161/2014 e seu respectivo Edital. Pregão disponível mediante busca em: <www.comprasnet.gov.br>. Acesso em: 10 ago. 2015.

[325] PREGÃO ELETRÔNICO DA UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ (SRP) nº 22/2014 e seu respectivo Edital. Pregão disponível mediante busca em: <www.comprasnet.gov.br>. Acesso em: 10 ago. 2015.

segurança corporativa (antivírus) para seus *campi* e reitoria, com validade de licenciamento e atualização pelo período de 36 (trinta e seis) meses. No edital está incluso um suporte remoto 8x5, mas com visita pessoal em hipóteses em que o IFSC entender necessário, com atendimento em até oito horas úteis nos casos prioritários com serviço indisponível em razão de problemas com a solução instalada[326]. Uma licença perpétua, se mantida estagnada, tende a contribuir pouco com a inovação, em um mundo globalizado, de constantes transformações tecnológicas.

Se a solução anterior não for compatível com a proposta, a tendência é que a empresa vencedora instale uma nova e cobre por ela. Ao que parece, esta solução não fomenta a competição entre diferentes fabricantes e, a depender da evolução tecnológica, pode ser economicamente inócua na compra de atualizações. Muito diverso seria um desenvolvimento próprio em contínua evolução.

### *4.3.1 Tecnologias desejáveis ao êxito no pugilato cibernético*

O contrato firmado entre o Exército Brasileiro e a Empresa Bluepex Controle e Segurança, mencionado supra, tinha a finalidade de desenvolver um programa contra códigos maliciosos, um *software anti-malware*[327]. *Malware* deriva do termo *malicious software*, um programa que tem por finalidade se infiltrar em um sistema de computador alheio com a intenção de causar efeitos, tais como: perda de confidencialidade, integridade, utilidade, disponibilidade, autenticidade e posse de dados[328]. A decisão apoiou-se em diversos argumentos, dentre os quais, se pode destacar que a entidade contratante é uma Instituição Científica e Tecnológica (ICT) do Exército Brasileiro. A Lei no 10.973, de 2 de dezembro de 2004, que dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo, prevê em seu art. 2º, V, que uma ICT é um órgão ou entidade da administração pública que tenha a finalidade institucional de executar atividades de pesquisa básica ou aplicada de caráter científico ou tecnológico.

---

[326] PREGÃO ELETRÔNICO POR REGISTRO DE PREÇOS nº 134/2014 do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina e seu respectivo Edital. Pregão disponível mediante busca em: <www.comprasnet.gov.br>. Acesso em: 10 ago. 2015.

[327] PREGÃO ELETRÔNICO SPR Nº 31/2011 – Base Administrativa do CCOMGEX .

[328] Informações presentes na estratégia de contratação do *software*, referente ao Pregão Eletrônico SPR Nº 31/2011 – Base Administrativa do CCOMGEX.

Outro forte argumento decorre da inexistência, à época, de um *software* nacional de código-fonte aberto e gratuito que atendesse à demanda da Força Terrestre brasileira. Nesse sentido, a END sinaliza com a necessidade de desenvolvimento de tecnologia genuinamente nacional, e que fomente a Indústria Nacional de Defesa. Além do desenvolvimento natural da indústria nacional a partir da aquisição, de acordo com a norma em vigor, existe uma natural transferência de tecnologia para o EB, capacitando recursos humanos no Brasil em sentido amplo, e em sentido estrito na empresa contratada e no Exército Brasileiro. Trata-se do desenvolvimento de atitudes, conhecimentos e habilidades para prover uma solução integrada contra uma potencial ameaça. Tudo foi realizado com a dotação orçamentária do Departamento de Ciência e Tecnologia do Exército[329]. Trata-se de transferência com conhecimentos implícitos e explícitos que agregam valor a inovações decorrentes de necessidades localmente identificadas.

Até então, os *softwares* eram tradicionalmente adquiridos de empresas transnacionais que possuíam código-fonte proprietário. Acresce-se a isso o fato de não se poder garantir a maneira como as informações são tratadas ou utilizadas pelos fornecedores dos *softwares*. Isto acontece porque, às vezes, as soluções são invasivas, possuindo acesso integral a dados que trafegam nas redes protegidas por elas[330].

Uma solução própria permite auditar o código-fonte do *software*, e como forma de garantir o sigilo das informações e dados que trafegam por esta solução. Além disso, desenvolve a indústria nacional de defesa, a tecnologia nacional, gera empregos de qualidade e renda decorrente de uma melhor qualificação pessoal.

Previamente ao processo licitatório, verificou-se a viabilidade da contratação, o plano de sustentação do projeto, análise de risco. Foram enumerados requisitos a serem atendidos, dos quais se pode destacar a obrigatoriedade de transferência de tecnologia para o Exército Brasileiro. Frise-se que, na hipótese em estudo, segundo o modelo adotado, a norma prevê que a propriedade intelectual e todos os direitos decorrentes são reservados ao EB, no entanto a expertise permanece com os técnicos e empreendedores que trabalharam no projeto.

---

[329] Argumentos extraídos da Memória para a Decisão referente a aquisição, referente ao Pregão Eletrônico SPR Nº 31/2011 – Base Administrativa do CCOMGEX.

[330] Argumentos retratados na oficialização da demanda do *software* analisado (DOD), referente ao Pregão Eletrônico SPR Nº 31/2011 – Base Administrativa do CCOMGEX.

O Exército, por sua vez, pode aproveitar a propriedade intelectual adquirida para melhorar seus processos, como também contribuir com outros órgãos públicos e demais necessidades da sociedade que demandam a tecnologia adquirida

A contratação previa ainda que a desenvolvedora da solução fosse sediada no Brasil, obrigando-se a empresa contratada a garantir que a solução fosse desenvolvida e mantida a sua tecnologia no Brasil. Militares designados pelo Exército Brasileiro tiveram acesso irrestrito a todos os processos durante todo o período de vigência do contrato[331].

Para o Exército, a contratação permitiu maior confiança no trato das informações, por meio do uso de uma solução de código aberto e completamente conhecida, que funciona de forma integrada ou isolada. Outra segurança foi colocada no edital: a empresa precisou demonstrar, por meio de atestados, a capacidade técnica para cumprir a tarefa a ele confiada, como condição da homologação da vitória no certame, além de sujeição a termo de confidencialidade com relação à tecnologia desenvolvida para a Força Terrestre. A empresa se sujeitou a fiscalização compatível com a natureza da contratação, sujeitou-se a penalidades por eventuais inadimplementos, e ainda ministrou curso de capacitação para análise de *malware*, com fornecimento de manuais técnicos em português e carga horária mínima definida. Também foram exigidos: plano de trabalho, plano de projeto executivo, plano de mobilização, cronograma macro com atividades detalhadas desde seu planejamento e com controle de mudanças[332].

Tanto o caso de fomento do antivírus brasileiro como o caso do simulador de guerra cibernética foram eficientes para os objetivos pensados de fomento e proteção. Em que pese o risco assumido pelo Estado, nos modelos em análise, as empresas contratadas assumiram parte do risco, pois se obrigaram a entregar um produto, tanto em um caso como em outro.

### *4.3.2 Oportunidades decorrentes do investimento realizado*

Quanto ao legado do projeto de desenvolvimento do antivírus brasileiro, alguns pontos merecem ser destacados para análise. O projeto deu condições à empresa que o

[331] Informações retiradas da Estratégia de Contratação do software, referente ao Pregão Eletrônico SPR Nº 31/2011 – Base Administrativa do CCOMGEX.
[332] Conforme Documento de Relacionamento atinente ao projeto, referente ao Pregão Eletrônico SPR Nº 31/2011 – Base Administrativa do CCOMGEX.

executou de contratar profissionais com formação técnica ou superior. Se já eram funcionários da empresa previamente, o projeto preservou seus empregos, aumentou sua experiência e o conhecimento técnico dos envolvidos. Muito provavelmente os profissionais continuarão utilizando seus talentos no Estado onde se encontram. A presença de novos profissionais na empresa, caso tenha havido contratações em decorrência do projeto, tem o potencial de instigar o empreendedor a continuar investindo nas pessoas contratadas, as quais podem contribuir em outros empreendimentos. Provavelmente funcionários considerados estratégicos pela empresa continuarão empregados, senão nesta, em outra empresa local. Ao fim e ao cabo, projetos desta espécie oferecem geração de conhecimento e tecnologia para a empresa e para o Brasil.

Conclui-se que o clássico tripé da inovação é útil para fomentar a pesquisa que dá lucro à empresa a partir do investimento do Estado. Assumindo algum risco, como por meio de uma compra pública, o Estado pode favorecer a sociedade com investimentos na empresa que inova e no meio acadêmico, ainda que de forma indireta. Nesse caso, às universidades coube o papel apenas de fornecer mão de obra qualificada, compatível com as necessidades do empreendimento.

A depender das necessidades do empreendedor, haverá, por vezes, necessidade de investimento por parte da empresa, com a finalidade de aprimorar o capital intelectual de seus funcionários. As dificuldades típicas de um país em desenvolvimento podem ser comparadas às situações de crise; por consequência, há a necessidade de se reagir à situação de crise (econômica, energética, ambiental, tecnológica), que podem funcionar como verdadeira locomotiva da inovação[333].

### *4.3.3 Do fomento à inovação na defesa*

Para entender o custeio do projeto de forma mais clara, convém retomar alguns conceitos. A licitação é um procedimento administrativo utilizado pelas pessoas indicadas pela lei com o objetivo de selecionar a proposta mais adequada para a celebração de um contrato, por meio de critérios objetivos e impessoais. O procedimento, segundo o art. 3º da Lei nº 8.666, de 21 de junho de 1993 – Lei de

[333] MARZANO, Stefano; ARGANTE, Enzo. *Domare La Tecnologia*. Roma: Salerno Editrice, 2009. p. 19.

Licitações e Contratos –, observando o princípio da isonomia, visa a selecionar a proposta mais vantajosa para a Administração. Outro objetivo é promover o desenvolvimento nacional sustentável, conforme o Decreto 7.746/12[334].

A competitividade, a isonomia, a vinculação ao instrumento convocatório, o procedimento formal e o julgamento objetivo são princípios que regem a licitação[335]. No contexto de produtos de defesa e inovação voltada para a defesa, não se pode olvidar dos conceitos e princípios preconizados pela Lei nº 12.598, de 21 de março de 2012, a qual estabelece normas especiais para as compras, as contratações e o desenvolvimento de produtos e de sistemas de defesa. A referida lei dispõe também sobre regras de incentivo à área estratégica de defesa.

A Lei nº 12.598, de 21 de março de 2012, dá destaque a conceitos de produto de defesa (PRODE), produto estratégico de defesa (PED), empresa estratégica de defesa (EED), previstos no seu art. 2º[336]. Nota-se que investir em EED é muito diferente de

---

[334] OLIVEIRA, Carvalho Rezende Oliveira. *Licitações e Contratos Administrativos*: teoria e prática. 3ª ed. Rio de Janeiro: Forense; São Paulo: Método, 2014. p. 25.

[335] Ibidem, p. 28-34.

[336] Art. 2º Para os efeitos desta Lei, são considerados:
I - Produto de Defesa - PRODE - todo bem, serviço, obra ou informação, inclusive armamentos, munições, meios de transporte e de comunicações, fardamentos e materiais de uso individual e coletivo utilizados nas atividades finalísticas de defesa, com exceção daqueles de uso administrativo;
II - Produto Estratégico de Defesa - PED - todo PRODE que, pelo conteúdo tecnológico, pela dificuldade de obtenção ou pela imprescindibilidade, seja de interesse estratégico para a defesa nacional, tais como:
a) recursos bélicos navais, terrestres e aeroespaciais;
b) serviços técnicos especializados na área de projetos, pesquisas e desenvolvimento científico e tecnológico;
c) equipamentos e serviços técnicos especializados para as áreas de informação e de inteligência;
III - Sistema de Defesa - SD - conjunto inter-relacionado ou interativo de PRODE que atenda a uma finalidade específica;
IV - Empresa Estratégica de Defesa - EED - toda pessoa jurídica credenciada pelo Ministério da Defesa mediante o atendimento cumulativo das seguintes condições:
a) ter como finalidade, em seu objeto social, a realização ou condução de atividades de pesquisa, projeto, desenvolvimento, industrialização, prestação dos serviços referidos no art. 10, produção, reparo, conservação, revisão, conversão, modernização ou manutenção de PED no País, incluídas a venda e a revenda somente quando integradas às atividades industriais supracitadas;
b) ter no País a sede, a sua administração e o estabelecimento industrial, equiparado a industrial ou prestador de serviço;
c) dispor, no País, de comprovado conhecimento científico ou tecnológico próprio ou complementado por acordos de parceria com Instituição Científica e Tecnológica para realização de atividades conjuntas de pesquisa científica e tecnológica e desenvolvimento de tecnologia, produto ou processo, relacionado à atividade desenvolvida, observado o disposto no inciso X do caput;
d) assegurar, em seus atos constitutivos ou nos atos de seu controlador direto ou indireto, que o conjunto de sócios ou acionistas e grupos de sócios ou acionistas estrangeiros não possam exercer em cada assembleia geral número de votos superior a 2/3 (dois terços) do total de votos que puderem ser exercidos pelos acionistas brasileiros presentes; e
e) assegurar a continuidade produtiva no País; [...]
XI - Sócios ou Acionistas Brasileiros:

investir em indústria nacional, conforme se verifica a partir da leitura da norma. Destaque-se que para receber o título de Empresa Estratégica de Defesa é necessário, cumulativamente, dentre outras coisas: ter sede, administração e estabelecimento no Brasil; dispor de conhecimento científico ou tecnológico próprio ou complementado por acordos de parceria, tudo no Brasil; controladores majoritariamente brasileiros. Tal realidade faz muita diferença quando se trata de empresa estratégica para a segurança do país.

A prestação de serviços, bem como a execução de obras, pressupõe a elaboração de um projeto básico e de um projeto executivo (art. 6º, IX e X, Lei nº 8.666, de 21 de junho de 1993), que devem estabelecer de forma clara e precisa todos os aspectos econômicos e técnicos do objeto a ser contratado. As principais exigências estão elencadas no art. 7º, parágrafo 2º da Lei de Licitações e Contratos; no entanto, a depender do projeto, podem existir outras exigências, como um estudo de impacto ambiental.

A regra da contratação pública é a licitação, mas nas hipóteses elencadas no art. 25 da Lei nº 8.666, de 21 de junho de 1993, a licitação é inexigível. A inexigibilidade de licitação pressupõe inviabilidade de competição. Jorge Ulisses Jacoby Fernandes[337], quanto à possibilidade de contratação direta (sem licitação), discorre sobre a dispensa de licitação na hipótese de incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo. Lei nº 10.973, de 2 de dezembro de 2004

Conforme disposto no art. 3º da Lei nº 10.973, de 2 de dezembro de 2004, o Estado pode estimular e apoiar ações estratégicas que apoiem a inovação de produtos e de processos, sendo-lhe também facultado, em alguns casos, fomentar a inovação por

---

a) pessoas naturais brasileiras, natas ou naturalizadas, residentes no Brasil ou no exterior;
b) pessoas jurídicas de direito privado organizadas em conformidade com a lei brasileira que tenham no País a sede e a administração, que não tenham estrangeiros como acionista controlador nem como sociedade controladora e sejam controladas, direta ou indiretamente, por uma ou mais pessoas naturais de que trata a alínea a; e
c) os fundos ou clubes de investimentos, organizados em conformidade com a lei brasileira, com sede e administração no País e cujos administradores ou condôminos, detentores da maioria de suas quotas, sejam pessoas que atendam ao disposto nas alíneas a e b;
XII - Sócios ou Acionistas Estrangeiros - as pessoas, naturais ou jurídicas, os fundos ou clubes de investimento e quaisquer outras entidades não compreendidas no inciso XI do caput.
Parágrafo único. As EED serão submetidas à avaliação das condições previstas no inciso IV do caput na forma disciplinada pelo Ministério da Defesa.

[337] FERNANDES, Jorge Ulisses Jacoby. *Contratação direta sem licitação*. 9 ed. Belo Horizonte: Fórum, 2012. p. 517.

meio de compra de produtos, tal como nos casos apresentados de fomento à inovação cibernética.

A norma legal pode ser, neste contexto, mais um instrumento de fomento de políticas públicas de inovação, pois pode induzir e facilitar as pesquisas de inovação. A regulamentação da compra pública pode, *v.g.*, materializar tal possibilidade: pela possibilidade de contratação direta sem licitação para a hipótese de incentivos à inovação no ambiente produtivo; por meio do estímulo e apoio a ações estratégicas que fomentem a inovação; através do fomento decorrente da seleção da proposta mais vantajosa. A ideia trazida pela norma é interessante e pode ser bem utilizada.

Na experiência cibernética apresentada, ganha a academia – pois o país tem acesso a novas tecnologias –, ganha a indústria – pelo suporte a produtos e serviços inovadores que podem ser aperfeiçoados e vendidos inclusive em outros mercados –, ganha a sociedade – que além das benesses para a indústria e para a academia, tem acesso a uma prestação de serviços estatais aperfeiçoados. Hoje, no Brasil, a segurança cibernética propiciada com tecnologia nacional é cada vez maior.

Percebe-se que o fomento poderia ser maior, com lucros proporcionais para sociedade, cada vez mais evidentes. O capítulo cita alguns poucos exemplos de órgãos públicos investindo em segurança cibernética com compras de soluções desenvolvidas em outros países, e foram citadas algumas vulnerabilidades deste processo que pode ser aperfeiçoado. Por outro lado, a compra pública, se utilizada para fomentar desenvolvimento tecnológico e estímulo à inovação, pode gerar resultados de médio prazo. No exemplo do antivírus brasileiro, o projeto consumiu – para o desenvolvimento de um *software* nacional – o que equivaleria à compra de licenças de programas por apenas três anos, considerando os custos do investimento em períodos anteriores. Se se empregassem recursos de outros setores da Administração Pública, o retorno em inovação poderia ser muito mais significativo.

# CONCLUSÃO

O presente trabalho retrata de forma exemplificativa riscos inerentes ao uso de redes de computadores no atual contexto social, e se pode concluir que os riscos em potencial podem impactar de forma substancial a sociedade e a forma em que se vive atualmente. Tais riscos podem ameaçar o Estado entendido como órgão formado pela comunidade como instrumento para o aperfeiçoamento da convivência social; como também podem ameaçar cada indivíduo pela privação de serviços públicos ou pela limitação ou mesmo impedimento do exercício de direitos fundamentais.

Os impactos potenciais dos riscos não estão limitados às pessoas físicas e às instituições de Estado. Podem impingir de forma bastante expressiva pessoas jurídicas de direito público ou privado. Quando instituições de Estado ou mesmo Empresas públicas ou privadas são injustamente ameaçadas, perde também a sociedade que delas se aproveita, aumentando a importância de não se olvidar da necessidade da defesa cibernética.

Quando se enfrenta soluções que dependem da segurança cibernética, o remédio indicado deve ser bem dosado, a fim de que sejam evitadas reações adversas. Restringir as reações indesejadas é consequência da dosagem e da forma como é utilizado o remédio existente. O fato é que a defesa cibernética impõe necessidade de vigilância, e tal vigilância contínua pode impactar inclusive na privacidade dos indivíduos que se aproveitam das benesses de uma eficaz segurança cibernética, sejam eles quem forem: pessoas físicas ou jurídicas. Trata-se ainda de um remédio que deve ser manipulado e utilizado com redobrada cautela em hipóteses em que o Estado pode eventualmente estar excessivamente aparelhado por forças de governo. Espera-se que o pugilato cibernético haja em favor da sociedade e do Estado que a serve. Não em favor de qualquer governo.

Almeja-se que a cada pessoa sob a égide constitucional seja dado o direito de viver, e que se possa viver vida em abundância. O *caput* do artigo 5º da Constituição da República de 1988 assegura o direito à vida. No inciso X do mesmo artigo, decorrendo, pois, do *caput*, é assegurado o direito à intimidade, a vida privada.

O direito à privacidade é uma conquista civilizatória, e não se questiona a necessidade de que um direito de tal magnitude deva ser preservado em qualquer Estado

democrático de direito. No entanto, por vezes, tal direito deve ser sobrepesado com a necessidade de que sejam protegidos outros direitos não menos importantes, como por exemplo, se pode citar o direito à vida. Em outras palavras, não faria sentido preservar a privacidade se para tal se colocasse em risco premente o direito à vida.

Em algumas circunstâncias, será razoável e proporcional, abdicar em algum grau da privacidade em favor da segurança cibernética. Enumerar tais circunstâncias proporcionará aos profissionais que labutam com o pugilato cibernético segurança jurídica necessária para que seja oferecido para a sociedade exatamente o produto que ela deseja, considerando o risco que esta mesma comunidade resolveu correr, conhecendo todo o contexto e elementos envolvidos.

Ao que se pode aduzir da redação constitucional, o pugilato cibernético deve defender a vida em detrimento até mesmo do direito à privacidade. Ademais, deve-se considerar que a escolha da medida da preservação da privacidade deve considerar a realidade fática da vigilância permitida e, efetivamente, realizada em decorrência da legislação dos outros países do mundo; haja vista que a internet não respeita fronteiras.

O ambiente cibernético possui dimensão transnacional, e iniciativas como o *Freedom Act* e o *Patriotic Act* norte americanos podem refletir em todas as nações. É importante a consciência de que o Brasil se encontra em um estágio de insipiência das discussões e conhecimento do tema. Trata-se de algo presente na vida de todos hoje em dia, e os problemas precisam ser enfrentados.

Pesquisadores da agência estadunidense CIA trabalharam por quase dez anos no intuito de quebrar a segurança dos eletrônicos da Apple, por meio de *backdoors* em programas distribuídos pela Apple Store[338]. Atualmente, como já citado, há um suposto desentendimento entre o FBI e a Apple em virtude da intenção do FBI em inserir um *backdoor* no sistema operacional dos aparelhos iPhone.

Ao que parece, os agentes de segurança dos Estados Unidos optam por mitigar a privacidade em prol da segurança e do bem comum, algo factível se respeitados os limites da democracia e do debate social prévio. Há de haver razoabilidade e

[338] REUTERS. *CIA tentou hackear iPhones desde os primeiros dias do aparelho, diz site*. Disponível em: <http://www.msn.com/pt-br/noticias/ciencia-e-tecnologia/cia-tentou-hackear-iphones-desde-os-primeiros-dias-do-aparelho-diz-site/ar-AA9B5V1?ocid=mailsignoutmd#fullstory>. Acesso em: 10/3/2015.

proporcionalidade. A decisão de lá reflete aqui, e somente com preparação que depende de investimentos o Brasil poderá opinar como detentor de criticidade necessária sobre o limite mais adequado para impor em território nacional e como fazer para que a lei não se torne letra morta.

Os representantes do Estado aptos a realizar defesa cibernética em favor dos cidadãos tendem a não invadir a privacidade alheia até que haja normas que o determinem. Se a escolha da sociedade privilegiar a segurança informática, admitindo-se mitigar a privacidade para combater aberrações como o terrorismo, essa vontade deve se manifestar por meio da regulação da conduta do agente público, sujeito ao princípio da legalidade estrita.

Ratifica-se que decisões similares de todos os países do globo refletem aqui. A tecnologia aumenta a velocidade com que as mudanças no ambiente comunitário impactem os sistemas normativos domésticos. Em razão disso, pode ser difícil que uma norma seja realmente adequada às condutas que se esperam do agente público. Contudo, a sociedade pode eleger preceitos de política pública setorial, direcionando a produção de regramentos viáveis[339].

Quando os escândalos de vazamento das práticas do serviço secreto de informações dos EUA vieram a público, foi minada a confiança das pessoas sobre o respeito à privacidade, inclusive de países aliados[340]. Some-se a isso a possibilidade de terrorismo real com conduta iniciada no mundo virtual. A partir daqueles episódios, o pugilato cibernético passou a revestir-se de grande importância social. Sendo um importante instrumento técnico a serviço do Estado para dar efetividade à Lei, a esta deve se sujeitar.

A regulação do pugilato cibernético, quando dá margem a diferentes interpretações, acaba por inviabilizar, na prática, a adequada condução das atividades de defesa cibernética pelos profissionais especializados, visto que o profissional que milita na área almeja que seu trabalho esteja inquestionavelmente dentro da legalidade. Sendo assim, uma regulação adequada fará valer a vontade da sociedade também pela

---

[339] ARANHA, Marcio Iorio. *Manual de Direito Regulatório*: Fundamentos de Direito Regulatório. 2 ed. Coleford, UK: Laccademia Publishing, 2014. p. 41-42.
[340] Ibidem, p. 162.

promoção de segurança jurídica junto a atividade de um profissional que atua em área tão sensível.

A defesa cibernética pode trazer benefícios, em especial para a sociedade brasileira, visto que o país é considerado, por especialistas no setor, relativamente vulnerável a ataques cibernéticos. O desenvolvimento econômico, naturalmente, tem estimulado certa dependência dos meios informáticos ligados em rede. Por consequência, a proteção de redes de computadores acaba por resguardar interesses econômicos e os interesses sociais a eles ligados.

A sensação de segurança na vida em sociedade está intrinsecamente ligada à prestação de serviços pelo Estado, haja vista que este possui, de regra, o monopólio do uso da força. Existe uma preocupação – a qual diminui com o amadurecimento de uma democracia – de como as forças políticas que governam o Estado usarão os dados e instrumentos de controle disponíveis. Com o desenvolvimento democrático do Estado de Direito, as forças de segurança atuarão sempre em sinergia com a ordem legal, que representa, em última análise, a vontade social.

O direito à privacidade e outras conquistas civilizatórias, como os direitos fundamentais, devem ser preservados. A defesa cibernética pode se apresentar como uma ferramenta de preservação da privacidade em sentido amplo, pela efetividade que pode conferir à ordem jurídica em ambiente hostil em redes informáticas. Neste ponto pode-se evidenciar um paradoxo: a contradição consiste no fato de que a mesma defesa cibernética que pode proteger a privacidade pode relativizá-la para que seja eficaz.

A privacidade de cidadãos, empresas e agentes públicos brasileiros já vem sendo mitigada, como já foi evidenciado. A população parece ignorar ou admitir riscos contra sua privacidade em troca de segurança ou mesmo ao aceitar as facilidades oferecidas pelos modernos equipamentos informáticos ligados em rede e serviços nele disponibilizados, a despeito dos riscos que tais hábitos podem acarretar para a privacidade e para outras conquistas, mesmo que por ignorância.

De forma pragmática, a comunidade deve considerar que a defesa cibernética traz riscos e segurança concomitantemente. O segredo está no equilíbrio. Os riscos que a defesa cibernética oferece, aparentemente já foram assumidos pela maior parte da sociedade, sem que, no entanto, o tenham feito de forma expressa ou mesmo consciente.

Em outras palavras, quase todo o risco intrínseco a uma defesa cibernética eficaz já faz parte da vida das pessoas, para que sejam cumpridos outros objetivos, que vão desde o bem-estar e comodidade na rede, até a facilidade das empresas anunciarem o produto certo para potenciais compradores. Além desses, outros tantos propósitos citados neste trabalho já serviram à mitigação da privacidade na rede.

Ainda no que tange à privacidade, a Comissão Europeia aconselhou seus cidadãos a deixarem de usar o Facebook em virtude de preocupação com dados pessoais postados na internet[341]. A Comissão Europeia conclui de forma a corroborar com o que se argumentou: a legislação local não tem como garantir a proteção dos dados vinculados a um serviço estrangeiro, a despeito de existir uma norma europeia que proíbe o envio de dados de usuários para os Estados Unidos. Além disso, destaca-se que há representações contra a Apple, Facebook, Microsoft, Skype e Yahoo junto ao Tribunal Europeu de Justiça, em Luxemburgo, por motivos atinentes a violação de privacidade.

Por certo, a sociedade deve debater se o aprimoramento da segurança cibernética mitigará a privacidade das pessoas mais do que já está mitigada. Em caso afirmativo, é imprescindível oferecer segurança jurídica aos profissionais que atuam nesta área. O importante é que trabalhem em proveito da sociedade, consoante os limites legais estabelecidos de forma consciente a partir de debate social, considerando os riscos envolvidos.

O debate social deve ressaltar que até mesmo riscos políticos devem ser considerados, pelo simples fato de que o combate a riscos que implicam em ampla vigilância pode impor novas vulnerabilidades, caso as informações coletadas sejam utilizadas de forma irresponsável por autoridades públicas.

É lamentável que muitos dados que poderiam ser utilizados para segurança já tenham sido coletados para fins comerciais. Para agravar mais o quadro, destaca-se que esses dados também têm sido coletados por outros Estados com foco na segurança cibernética.

---

[341] INFOMONEY. *Comissão Europeia aconselha cidadãos a deixarem o Facebook.* Disponível em: <http://www.msn.com/pt-br/noticias/ciencia-e-tecnologia/comiss%C3%A3o-europeia-aconselha-cidad%C3%A3os-a-deixarem-o-facebook/ar-AAa71kh?ocid=mailsignoutmd>. Acesso em: 28 mar. 2015.

Ao se analisarem ameaças de vigilância contra empresas nacionais, deve-se tomar em conta a necessidade de outros Estados e suas empresas (na hipótese de vigilância estrangeira) de proteger seus próprios investimentos e a possibilidade de espionagem industrial que, ao menos potencialmente, empobrece o Brasil e deteriora a economia doméstica.

Também é de grande relevância o combate ao terrorismo e a possibilidade de uso racional das modernas tecnologias. Porém, a privacidade deve ser preservada em alguma medida, pois trata-se de uma das conquistas civilizatórias. Não parece justo ou ético que governos condicionem seus cidadãos a abrir mão desta conquista, devendo haver um equilíbrio entre a necessidade e o direito que ela relativiza.

Faz-se mister a consciência de que não existe prestação de serviço gratuito: paga-se por ele de uma forma ou de outra, tanto no mundo físico quanto no virtual. A segurança também tem um preço: a norma e sua interpretação devem materializar a vontade social, no limite da razoabilidade, proporcionalidade e outros valores jurídicos e democráticos consagrados.

Ratificando a afirmação de Popper[342], não existe liberdade que não seja garantida pelo Estado. Assim sendo, o Estado precisa se valer do pugilato cibernético em pontos primordiais para garantir a existência da sociedade, visto que esta pode se ver ameaçada concretamente em razão de um ataque virtual. Para tanto, deve-se investir em tecnologias, capacitação técnica de pessoal e regulação jurídica do ambiente cibernético.

A cooperação entre atores internacionais é importante, mas, uma vez que a expressão militar é indispensável, deve-se considerar uma preparação adequada para um instituto necessário em situações de adversidade e crise. Frise-se que uma ameaça virtual relevante pode partir de pessoas comuns com conhecimentos adequados de rede de computadores, não necessariamente de Estados oponentes. Esta característica faz crescer a importância do pugilato cibernético e sua regulação jurídica.

No que tange à regulação, os agentes públicos que labutam com o pugilato cibernético terão um resultado potencializado se souberem claramente seus limites de atuação. Quando os limites não são claros, é natural que os profissionais optem por

---

[342] POPPER, Karl. *As Aventuras da Racionalidade*. (Org.) PEREIRA, Julio Cesar R. Porto Alegre: EDIPUCRS, 1995. p. 140 e 141.

evitar riscos para si, evitando adentrar no que pode lhes ser defeso fazer. A despeito da importância da regulação, ressalta-se que, mediante investimentos adequados, a defesa cibernética pode oferecer para a sociedade algo que nem mesmo a norma conseguiria atualmente, em razão dos limites físicos da atuação do judiciário, inexistentes em ambiente virtual: a tutela a bens caros à sociedade e ao Estado brasileiro. Destarte a democracia será reforçada e realimentada.

Leis como a nº 12.737, de 30 de novembro de 2012 – que tipifica delitos informáticos – e a Lei nº 12.964, de 8 de abril de 2014 – que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil – indicam a regulamentação do tema. Nesse contexto, ganham importância para debates futuros sobre a regulação os legados do Livro Verde e do Livro Branco de Defesa Nacional. Porém, nas oportunidades em que a norma, por qualquer motivo, não conseguir produzir, por si só, os efeitos esperados, as técnicas de pugilato cibernético poderão assegurar a tutela de bens jurídicos.

O pugilato cibernético eficiente depende de investimentos em capacitação e tecnologia. Existem em países centrais investimentos expressivos que têm foco no processamento de dados de interceptação para análise, como o projeto Echelon e outros citados por Snowden ou pelo site Wikileaks. A "filosofia da interceptação" retratada pelos italianos Boatti e Tavaroli é bastante presente, e a eficácia da defesa depende de inovação contínua.

O presente trabalho tratou de possibilidades de fomento à inovação a partir de conceitos já experimentados. Pretendeu-se destacar o modelo da tripla hélice, o qual evidencia o papel do Estado fomentando inovação por meio da convergência de recursos em projetos que integrem o ramo industrial e o meio acadêmico.

Na esteira da inovação, o meio acadêmico possui a função de formação de pessoal, de difusão do conhecimento, de pesquisa, de aperfeiçoamento dos talentos humanos. Apoiada na academia, a indústria poderá inovar a partir de seu *know-how*, agregando valor a produtos que foram pesquisados com escopo inicial de atender necessidades da comunidade, mas que acaba beneficiando a própria indústria que lucrará com a inovação e o meio acadêmico, num processo de auto aperfeiçoamento. Esses resultados são potencializados quando, a partir da inovação, são gerados produtos com competitividade e aceitação no comércio internacional. Mediante aceitação no

mercado internacional, a inovação rende frutos para a sociedade que a desenvolveu, melhorando as receitas do Estado.

Constata-se que a inovação tecnológica agrega valor não somente aos produtos, mas também ao trabalho daqueles que laboram em setores inovadores. A inovação fomenta, por meio do desenvolvimento cognitivo e tecnológico, a exportação, o emprego, a capacitação e a economia.

O processo da inovação não é abrupto. Ele possui fases bem definidas que devem ser vencidas com perspicácia e estratégia. A Coréia do Sul começou a implementar a sua estratégia a partir dos anos 1960, e somente em 1972 passou a fomentar a exportação de produtos com tecnologia agregada. Logo, vê-se que são necessárias políticas de Estado – e não de governo – para que se efetivem as mudanças necessárias.

Investimentos estatais em inovação tecnológica têm propiciado, em sentido mais amplo, qualidade de vida para a sociedade, e em sentido mais estrito, ganhos relevantes para a sociedade que nela investe com objetivo e programas bem definidos, bem como para os demais atores diretamente envolvidos; quase sempre num contexto de tripla hélice. A Internet, o GPS, telas sensíveis ao toque, comandos por voz podem ser tidos como exemplos de inovação que podem ser enquadrados dentro do aqui exposto. Da argumentação ora apresentada, decorre que é desejável investir em defesa cibernética de forma sistemática, a partir de um planejamento realizado em razão de políticas públicas anteriormente delineadas.

A partir de um planejamento de inovação conduzido pela Força Aérea Brasileira – que também fomenta a P&D em escolas como o Instituto Tecnológico de Aeronáutica – chegou-se a um exemplo evidente de inovação: a EMBRAER, uma das empresas brasileiras que mais agrega valor tecnológico à sua produção e que tem lugar significativo nas exportações brasileiras. Por sua vez, o Exército Brasileiro – que também financia escolas de destaque no cenário nacional, como o Instituto Militar de Engenharia – destaca-se no fomento ao desenvolvimento de produtos como o Carro de Combate Osório, radares nacionais e sensores eletromagnéticos.

No que tange ao setor cibernético, o Exército Brasileiro vem fomentando pesquisa e desenvolvimento, por meio de seu Departamento de Ciência e Tecnologia. O

antivírus brasileiro e o simulador de guerra cibernética podem ser citados como inovação fomentada pelo Estado e que contribui com a sociedade de maneira geral. Além da produção de segurança, hoje o país detém tecnologias que podem ser utilizadas na prestação de outros serviços em redes informáticas, melhorando a qualidade dos empregos, dos produtos e estimulando novas fontes de receitas para o Estado. Esses dois exemplos revelam que diversos podem ser os benefícios dessa sinergia.

A norma legal pode ser, neste contexto, importante instrumento de políticas públicas de inovação, pois pode induzir e facilitar as pesquisas de inovação. Além da pesquisa e desenvolvimento, as políticas de inovação podem se efetivar por meio de compras públicas. Nesse aspecto, já existe a possibilidade de contratação direta (sem licitação) em hipóteses de incentivos à inovação no ambiente produtivo; pelo estímulo e apoio a ações estratégicas que fomentem a inovação; pelo estímulo pela seleção da proposta mais vantajosa. Pode-se concluir que a compra pública, conforme modelo apresentado, pode revelar-se eficiente para desenvolvimento tecnológico e estímulo à inovação.

Quando a ameaça cibernética bate à porta, o ideal é que se tenha tecnologia própria ou confiar em produtos desenvolvidos por aliados. Por isso, vale a pena investir em pesquisa e desenvolvimento. As normas, que materializam políticas públicas, podem ser aperfeiçoadas e fomentar ainda mais investimentos estatais em inovação em projetos dual. Um caminho para tanto pode ser o investimento em inovação a partir da indústria de defesa, fazendo uso dos conceitos de empresa estratégica de defesa e de produto de defesa, consoante a Lei nº 12.598, de 21 de março de 2012.

Todo o contexto apresentado tem se refletido na doutrina, na jurisprudência, na evolução das normas e na interpretação destas. De fato a privacidade tem sido mitigada na modernidade em função das necessidades sociais típicas da era da internet, mediante riscos muitas vezes assumidos voluntariamente pelas pessoas. E decisões legislativas materializadas em leis como a nº 12.964, de 8 de abril de 2014; decisões judiciais como a retratada na ADI 3.059MC / RS; e atos do executivo como os materializados no Livro Verde - Segurança Cibernética no Brasil e no Livro Branco de Defesa Nacional convergem para o objetivo da sociedade brasileira em construir um Brasil cada vez mais autônomo e seguro também em ambiente cibernético.

Assim sendo, a comunidade caminha entre a centralidade individual – quando não abre mão de conquistas civilizatórias, como o direito à privacidade, senão na medida necessária – e a coesão social, o que acontece naturalmente pelo equilíbrio das forças na busca pelo bem comum.

# REFERÊNCIAS

AGÊNCIA BRASIL. *Especialistas ouvidos por CPI alertam para baixa segurança da informação.* Brasília, 2013. Disponível em: <http://www.correiobraziliense.com.br/app/noticia /politica/2013/10/22/interna_politica,394706/especialistas-ouvidos-por-cpi-alertam-para-baixa seguranca-da-informacao.shtml>. Acesso em: 18 nov. 2013.

AGENCIA BRASIL. *Marco entre a ditadura e a democracia, constituição de 1988 completa 25 anos.* Disponível em: <http://memoria.ebc.com.br/agenciabrasil/noticia/2013-10-04/marco-entre-ditadura-e-democracia-constituicao-de-1988-completa-25-anos>. Acesso em: 30 jun. 2014.

AGENCIA LUSA. *China emprega 2 milhões de pessoas para controlar a internet.* Disponível em: <http://memoria.ebc.com.br/agenciabrasil/noticia/2013-10-05/china-emprega-2-milhoes-de-pessoas-para-controlar-internet/>. Acesso em: 09 ago. 2014.

AGRELA, Lucas. *Boss é o primeiro smartphone com a criptografia da rede tor.* Disponível em: <http://info.abril.com.br/noticias/tecnologia-pessoal/2015/01/boss-e-o-primeiro-smartphone-com-a-criptografia-da-rede-tor.shtml>. Acesso em: 14 fev. 2015.

AGUILHAR, L. *A espionagem ultrapassou limites.* São Paulo, Disponível em: <http://blogs.estadao.com.br/link/a-espionagem-ultrapassou-limites/>. Acesso em 18 nov. 2013.

AGUILLAR, F. H. *Controle social de serviços públicos.* São Paulo: Max Limonad, 1999.

ALEXY, Robert. *Teoria dos direitos fundamentais*. Trad. Virgilio Afonso da Silva. 2 Ed. São Paulo: Malheiros Editores, 2008.

ÁLVARES, João Gabriel. *Territorialidade e guerra cibernética*: novo paradigma fronteiriço. In: Segurança e Defesa Cibernética: da fronteira física aos muros virtuais. Recife: UFPE, 2014.

ALVES JR., Sergio. *Políticas Nacionais de Segurança Cibernética*. Disponível em: <http://www.anatel.gov.br/Portal/documentos/sala_imprensa/13-12-2012--11h28min17s-Seguran%C3%A7a%20Cibern%C3%A9tica%20-%20S%C3%A9rgio%20Alves%20Jr%20-%20AIN-Anatel.pdf>. Acesso em: 26 jun. 2014.

IV SIMPÓSIO DE PÓS-GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS DO PROGRAMA "SAN TIAGO DANTAS" (UNESP, UNICAMP E PUC/SP). *Anais*. Disponível em: <http://www.santiagodantassp.locaweb.com.br/novo/images/simposio/artigos2013/gabriela_sandroni.pdf>. Acesso em: 14 jan. 2016.

ANATEL. *Nono Dígito*. Brasília, 2012. Disponível em: <http://www.anatel.gov.br/Portal/exibirPortalNivelDois.do?codItemCanal=1746&nomeVisao=Cidad%E3o&nomeCanal=Nono%20D%EDgito&nomeItemCanal=Nono%20D%EDgito>. Acesso em: 19 fev. 2014.

ANISTIA INTERNACIONAL. *Pesquisa inédita indica preocupação dos internautas brasileiros com vigilância e privacidade na internet.* Disponível em: <https://anistia.org.br/noticias/pesquisa-inedita-indica-preocupacao-dos-internautas-brasileiros-com-vigilancia-e-privacidade-na-internet/>. Acesso em 14 fev. 2016.

APF. *Primeiro-ministro canadense deixa de seguir Homer Simpson no Twitter.* Disponível em: <http://noticias.br.msn.com/primeiro-ministro-canadense-deixa-de-seguir-homer-simpson-no-twitter-1>, consultado em 26 jun.14.

ARANHA, Marcio Iorio. *Manual de Direito Regulatório*: Fundamentos de Direito Regulatório. 2 ed. Coleford, UK: Laccademia Publishing, 2014.

ARANHA, M.I.; WIMMER, M.; PIERANTI, O.P. *Direito regulatório*. Brasília: Universidade de Brasília, 2009.

BARROSO, Luís Roberto. *Curso de direito constitucional contemporâneo*: os conceitos fundamentais e a construção do novo modelo. 3 ed. São Paulo: Saraiva, 2011.

BASTOS, Celso Ribeiro Bastos. *Curso de direito constitucional*. 21 ed. São Paulo: Saraiva, 2000.

BAUMAN, Zygmunt. *Após Snowden*: Repensando o Impacto da Vigilância. Disponível em: <https://revistas.ufrj.br/index.php/eco_pos/article/view/2660/2225>. Acesso em: 14 jan. 2016.

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

BECK, Ulrich. *Sobre el terrorismo y la guerra*. Barcelona: Paidós, 2003.

BERCITO, Diogo. *França reforça segurança contra terrorismo*. Portal Folha. Disponível em: <http://www1.folha.uol.com.br/mundo/2015/01/1573518-franca-reforca-seguranca-contra-terrorismo.shtml>. Acesso em: 08 fev. 2015.

BEZERRA, Arthur C.; WALTZ, Igor. *Privacidade, neutralidade e inimputabilidade da internet no Brasil*. Revista Eptic Online, p.161-175, maio/ago, 2014. v.16, n.2

BITTAR, Carlos Alberto. *Os direitos da personalidade*. 7 ed. Rio de Janeiro: Forense, 2008.

BOATTI, Giorgio; TAVAROLI, Giuliano. *SPIE*: *I servizi segreti delle multinazionali*: dossier, intercettazioni, guerre informatiche. Milano: Mondadori. 2008.

BOBBIO. Norberto. *O tempo da memória*. In: BOBBIO. Norberto. A Era dos Direitos. Rio de Janeiro: Elsevier, 2004.

BOM DIA BRASIL. *Petrobras foi espionada pelos Estados Unidos, apontam documentos.* Disponível em: <http://globotv.globo.com/rede-globo/bom-dia-brasil/v/petrobras-foi-espionada-pelos-estados-unidos-apontam-documentos/2811481/>. Acesso em: 08 jun.14.

BONIN, R. O Livro Bomba. *Revista Veja*. São Paulo: Abril, edição 2351, 2013.

BRASIL. *C 34-1*: O Emprego da Guerra Eletrônica. Brasília: EGGCF, 2008.

BRASIL. Constituição (1998) *Constituição da República Federativa do Brasil de 1988*. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>. Acesso em: 26 jan. 2016.

BRASIL. *Decreto nº 6.703, de 18 de dezembro de 2008*. Estratégia Nacional de Defesa. 2 ed. Brasília: Ministério da Defesa. 2008.

BRASIL. *Decreto nº 6.703, de 18 de dezembro de 2008*. Estratégia Nacional de Defesa. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm>. Acesso em: 26 jan. 2016.

BRASIL. *Lei nº 7.170, de 14 de dezembro de 1983*. Regula crimes contra a segurança nacional. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L7170.htm>. Acesso em: 26 jan. 2016.

BRASIL. *Lei nº 9.296, de 24 de julho de 1996*. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: <http://www.planalto.gov.br/CCivil_03/LEIS/L9296.htm>. Acesso em: 26 jan. 2016.

BRASIL. *Lei no 10.406, de 10 de janeiro de 2002*. Código Civil de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 26 jan. 2016.

BRASIL. *Lei nº 12.527, de 18 de novembro de 2011*. Regula o acesso a informações. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 26 jan. 2016.

BRASIL. *Lei nº 12.737, de 30 de novembro de 2012.* Tipificação criminal de delitos informáticos. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 26 jan. 2016.

BRASIL. *Lei 12.965, de 23 de abril de 2014.* Princípios, garantias, direitos e deveres para o uso da internet no Brasil: Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 26 jan. 2016.

BRASIL. *Lei nº 13.260, de 16 de março de 2016*. Regulamenta o disposto no inciso XLIII do art. 5o da Constituição Federal. Lei 13.260/16. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13260.htm>. Acesso em: 26 jan. 2016.

BRASIL. *Livro Branco da Defesa Nacional*. Brasil, 2012.

BRASIL. *Livro verde*: segurança cibernética no Brasil. Brasília: GSIPR/SE/DSIC, 2010.

BRASIL. *Portaria Normativa nº 196/EMD/MD, de 22 de fevereiro de 2007*. MD35-G-01. 2007.

BRITTO, Carlos Ayres. Banca de qualificação de mestrado em Direito em 10 de novembro de 2015 no Centro Universitário de Brasília.

BRITTO, Carlos Ayres. *O humanismo como categoria constitucional*. Rio de Janeiro: Ed. Forum, 2012.

BRITTO, Carlos Ayres. *O centro e a periferia de nós mesmos*. Disponível em: <http://opiniao.estadao.com.br/noticias/geral,o-centro-e-a-periferiade-nos-mesmos,10000002601>. Acesso em: 09 fev. 2016.

BRITTO, Carlos Ayres. *Teoria da Constituição*. Rio de Janeiro: Forense, 2003.

BUCCI, Maria Paula Dallari. O Conceito de Política Pública em Direito. In: BUCCI, Maria Paula Dallari (Org.). *Políticas públicas*: reflexões sobre o conceito jurídico. São Paulo: Saraiva, 2006.

CAMPINHO, Sérgio. *O direito de empresa*: à luz do novo Código Civil. 13 ed. Rio de Janeiro: Renovar, 2014.

CANALTECH . *Governo britânico considera Ubuntu o sistema operacional mais seguro*. Disponível em: <http://canaltech.com.br/noticia/linux/Governo-britanico-considera-Ubuntu-o-sistema-operacional-mais-seguro/>. Acesso em: 09 ago. 2014.

CANOTILHO, J. J. Gomes, et al. *Comentários à Constituição do Brasil*. São Paulo: Saraiva/Almedina, 2013.

CANOTILHO, José Joaquim Gomes. *Direito Constitucional e Teoria da Constituição*. 7 ed. Coimbra: Almedina, 2007.

CANOTILHO, J. J. Gomes; MOREIRA, Vital. *Fundamentos da Constituição*. Coimbra: Coimbra Editora, 1991.

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

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

CARVALHO, Kildare Gonçalves Carvalho. *Direito Constitucional*. 13. ed. Belo Horizonte: Del Rey, 2007.

CASTELLS, Manuel. *A sociedade em rede*. Trad: Roneide Venâncio Majer. 8 ed. São Paulo: Paz e Terra, 2005. v.1.

CASTELLS, Manuel. *Redes de Indignação e Esperança*: Movimentos Sociais na era da Internet. Trad: Carlos Alberto Medeiros. São Paulo: Zahar, 2013.

CAVALIERI FILHO, Sergio. *Programa de responsabilidade civil*. 8 ed. São Paulo: Atlas, 2008.

CHANDER, Anupam; LE, Uyen P. *Breaking the Web:* Data Localization vs. the Global Internet. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858>. Acesso em: 09 fev. 2016.

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

CLARKE, Richard A. *Cyberwar*: The Next Threat to National Security and What to do About It. New York: Ed. Ecco, 2012.

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

CONGRESSO INTERNACIONAL SOFTWARE LIVRE E GOVERNO ELETRÔNICO (V Congresso). *A favor de uma defesa ativa contra ataques cibernéticos*: Belém do Pará. Disponível em: <https://gestao.consegi.serpro.gov.br/cobertura/noticias/a-favor-de-uma-defesa-ativa-contra-ataques-ciberneticos>. Acesso em: 16 fev. 2014.

CONVERGÊNCIA DIGITAL. *Governo garante propriedade intelectual de antivirus nacional*. Disponível em: <http://tvuol.uol.com.br/video/governo-garante-propriedade-intelectual-de-antivirus-nacional-0402CC193162D4B94326/>. Acesso em: 02 ago. 2015.

CORDEIRO, Antônio Menezes. *Tratado de Direito Civil Português*: Parte Geral – Pessoas. Lisboa: Almedina, 2004. v. 1, tomo III.

CRESPO, M.X.F. *Crimes digitais*. São Paulo: Saraiva, 2011.

CRUISE, Sinead. *HSBC says internet banking services down after cyber attack*. Disponível em: < http://www.reuters.com/article/us-hsbc-cyber-idUSKCN0V71BO>. Acesso em: 07/02/2016.

CRUZ JÚNIOR, Samuel César da. *Tecnologias e riscos*: armas cibernéticas. Brasília: IPEA, 2013.

DELEGADOS DA CONVENÇÃO DE FILADÉLFIA. *Constitution of the United States.* Disponível em: <http://www.senate.gov/civics/constitution_item/constitution.htm>. Acesso em: 07 fev. 2015.

DAMÉ, Luiza. *Dilma assina decreto de Garantia da Lei e da Ordem para o Rio*. Portal O Globo. Disponível em: <http://oglobo.globo.com/brasil/dilma-assina-decreto-de-garantia-da-lei-da-ordem-para-rio-12022760>. Acesso em: 26 jun. 2014.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006.

DÓRIA, P.; RODRIGUES L. *Segurança não justifica espionagem econômica*. Disponível em <http://oglobo.globo.com/pais/exercito-monitorou-lideres-de-atos-pelas-redes-sociais-9063915>. Acesso em: 09 dez. 2013.

DAILYTASK. *Tails: O sistema operacional mais protegido contra a NSA*. Disponível em: <http://dailytask.com.br/slide/tails-o-sistema-operacional-mais-protegido-contra-a-nsa/>. Acesso em: 09 ago. 2014.

ÉPOCA. *Julian Assange pode deixar embaixada do Equador nesta sexta*. Disponível em: <http://epoca.globo.com/tempo/filtro/noticia/2016/02/fundador-do-wikileaks-assange-pode-deixar-embaixada-do-equador-nesta-sexta-feira.html>. Acesso em: 06 fev. 2016.

ETZKOWITZ, H. *Reconstrução criativa da Hélice Tripla e Inovação Regional*. In: Revista Inteligência Empresarial, número 23. Rio de Janeiro: Editora e-papers, 2005.

EZEKIEL, Alan W. *Hackers, spies, and stolen secrets: protecting law firms from data theft*. In: Harvard Journal of Law & Technology Volume 26, Number 2 Spring 2013. Disponível em: <http://jolt.law.harvard.edu/articles/pdf/v26/26HarvJLTech649.pdf>. Acesso em: 14 jan. 2016.

FERNANDES, Jorge Ulisses Jacoby. *Contratação direta sem licitação*. 9 ed. Belo Horizonte: Fórum, 2012.

FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados*: o direito à privacidade e os limites à função fiscalizadora do Estado, Cadernos de Direito Constitucional e Ciência Política. São Paulo: Revista dos Tribunais, 1992.

FERRER, Rafael. *Exército usará antivírus brasileiro*. Disponível em: <http://info.abril.com.br/noticias/ti/exercito-usara-antivirus-brasileiro-01022012-8.shl>. Acesso em: 02 ago. 2015.

FOLHA DE SÃO PAULO. *China é acusada de hackear reunião do G20*. Disponível em: <http://www1.folha.uol.com.br/fsp/mundo/143297-china-e-acusada-de-hackear-reuniao-do-g20.shtml>. Acesso em: 12 dez.13.

FOLHA DE SÃO PAULO. *Dilma foi espionada pelos EUA, diz TV*. Disponível em: <http://www1.folha.uol.com.br/mundo/2013/09/1335522-dilma-foi-espionada-pelos-eua-diz-tv.shtml>. Acesso em: 07 fev. 2015.

FOLHA VITÓRIA. *Planalto decide ignorar denúncia de que Dilma continua sendo espionada*. Disponível em: <http://www.folhavitoria.com.br/politica/noticia/2015/02/planalto-decide-ignorar-denuncia-de-que-dilma-continua-sendo-espionada.html>. Acesso em: 07 fev. 2015.

FORÇAS TERRESTRES. *Osório*: o MBT brasileiro que bateu o M1 Abrams. Disponível em: <http://www.forte.jor.br/2008/09/21/osorio-o-mbt-brasileiro-que-bateu-o-m1-abrams/>. Acesso em: 18 ago. 2015.

FUCHS, Christian. *Web 2.0, Prosumption, and Surveillance. In: Surveillance & Society*. vol. 8, no 3., 2011, Queen's University, Canada. Disponível em: <http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/4165/4167>. Acesso em: 06 fev. 2016.

GARATTONI, Bruno; BADÔ, Fernando. *Vírus de computador se espalha pelo ar*. Disponível em: <http://super.abril.com.br/tecnologia/virus-computador-se-espalha-pelo-ar-787622.shtml>, consultado em: 09 ago. 2014.

GARCIA, Gabriel. *França quer fortalecer privacidade na rede para ´equilibrar forças´*. Disponível em: <http://info.abril.com.br/noticias/internet/2014/12/franca-quer-fortalecer-privacidade-na-rede-para-equilibrar-forcas.shtml>. Acesso em: 10 maio 2015.

GDDC. *Comentários Gerais do Comité dos Direitos do Homem*. Disponível em: <http://direitoshumanos.gddc.pt/2_1/IIPAG2_1_2_1_2.htm>. Acesso em: 26 jan. 2016.

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

GOBERT, Muller. In: VAZ., L.G.D. *Políticas públicas. Revista nova Atenas de educação e tecnologia*. São Luiz do Maranhão: CEFET. 2007. v. 10. nº. 01, jan./jun.

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

GUERRA, Sidney Cesar Silva. *A liberdade de imprensa e o direito à imagem*. 2. ed. Rio de Janeiro: Renovar, 2004.

GREENWALD, Glenn. *Sem Lugar para se esconder*. Trad. Fernanda Abreu. Rio de Janeiro: Sextante, 2014.

GROSSMANN, L.O. *Espionagem dos EUA já cancela projetos de computação em nuvem*. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=34377#.UoqGqxrrzQs>. Acesso em: 18 nov. 2013.

HABERMAS, Jürgem. *Verdade e Justificação*: Ensaios Filosóficos. São Paulo: Edições Loyola, 2004.

HARDING, Luke. *Os Arquivos de Snowden*. Trad. Bruno Correia e Alice Klesck. Rio de Janeiro: LeYa, 2014.

HARRIS, Shon. *CISSP*. Sixth Edition. USA: Mc Graw Hill, 2013.

HERMAN, SUSAN N. *Os desafios do crime cibernético*. Disponível em: <http://www.seer.ufrgs.br/index.php/redppc/article/view/46105/28721>. Acesso em: 08 jan. 2016.

HOBBES, Thomas. *Leviatã ou matéria, Forma e poder de um Estado eclesiástico e civil*. Trad: MONTEIRO. João Paulo e NIZZA. Maria Beatriz da Silva. São Paulo: Abril Cultural, 1984.

HOLLIS. Duncan B. *Why States Need an International Law for Information Operations.* Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1083889>. Acesso em: 10 fev. 2016.

IDC. *Os números do Facebook, dez anos após sua criação*. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/os-numeros-do-facebook-dez-anos-apos-sua-criacao#5>. Acesso em: 26 jun. 2014.

IDOETA, Paula Adamo. *Como a Petrobras virou 'dor de cabeça' para governo e investidores.* Disponível em: <http://www.bbc.co.uk/portuguese/noticias/2014/03/140320_petrobras_governo_pai>. Acesso em: 07 fev. 2015.

INFOMONEY. *Comissão Europeia aconselha cidadãos a deixarem o Facebook*. Disponível em: <http://www.msn.com/pt-br/noticias/ciencia-e-tecnologia/comiss%C3%A3o-europeia-aconselha-cidad%C3%A3os-a-deixarem-o-facebook/ar-AAa71kh?ocid=mailsignoutmd>. Acesso em: 28 mar. 2015.

INTERPOL. *A Global Presence*. Disponível em: <http://www.interpol.int/Member-countries/World>. Acesso em: 19 nov. 2013.

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

JORNALWEBDIGITAL. *Pesquisa Avast no Brasil e mais 10 países*: usuário prefere perder privacidade do que dados financeiros. Disponível em: <http://jornalwebdigital.blogspot.com.br/2015/12/pesquisa-avast-no-brasil-e-mais-10.html>, Acesso em: 14 jan. 2016.

KERN, Soeren. *O Parlamento Francês Aprova Lei Abrangente de Espionagem de Dados*. 6 de Maio de 2015. Trad.: Joseph Skilnik. Disponível em: <http://pt.gatestoneinstitute.org/5715/franca-lei-espionagem>. Acesso em 07 mai. 2015.

KESAN Jay P; HAYES Carol M. *Mitigative counterstriking*: self-defense and deterrence in cyberspace. In: Harvard Journal of Law & Technology Volume 25, Number 2 Spring 2012. Disponível em: <http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech429.pdf>. Acesso em: 14 jan. 2016.

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

LAWNER, Kevin J. *Post-Sept. 11th international surveillance activity*: a failure of intelligence: the echelon interception system & (and) the fundamental right to privacy in Europe. Disponível em:

<http://heinonline.org/HOL/LandingPage?handle=hein.journals/pacinlwr14&div=22&id=&page=>. Acesso em: 07 fev. 2016.

LEMOS, Ronaldo, et al. *Estudio I*: Privacidade na Internet. Globonews. Exibido em: 30 maio 2012.

LYON, David. *As apostas de Snowden:* desafios para entendimento de vigilância hoje. Disponível em: <http://www.seer.ufrgs.br/index.php/redppc/article/view/52029/32055>. Acesso em: 08 jan. 2016.

MACHADO, H. B. *Curso de Direito Tributário*. São Paulo: Malheiros Editores, 2008.

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

MALAWER. Stuart S. *Cyber Warfare*: Law and Policy Proposals for U.S. and Global Governance. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1437002&download=yes>. Acesso em: 10 fev. 2016.

MANDARINO JUNIOR, Raphael; CANONGIA, Claudia. *Segurança cibernética*: o desafio da nova sociedade da informação. Disponível em: <http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/349/342>. Acesso em: 14 jan. 2016.

MARTINS, Elaine. *É hora de descobrir os segredos da computação quântica*. Disponível em: <http://www.tecmundo.com.br/computacao-quantica/2666-e-hora-de-descobrir-os-segredos-da-computacao-quantica.htm>. Acesso em: 13 fev. 2015.

MARZANO, Stefano; ARGANTE, Enzo. *Domare La Tecnologia*. Roma: Salerno Editrice, 2009.

MATSURA, Sérgio. *Brasil terá Escola Nacional de Defesa Cibernética*. Disponível em: <http://oglobo.globo.com/sociedade/tecnologia/brasil-tera-escola-nacional-de-defesa-cibernetica-15914957>. Acesso em: 06 fev. 2016.

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

MENDES, Gilmar Ferreira; BRANCO, Gustavo Gonet. *Curso de direito constitucional*. 9 ed. São Paulo: Saraiva, 2014.

MENEZES, Dyelle. *Ação para defesa cibernética recebeu apenas 31% do previsto ano passado*. Disponível em: <http://www.contasabertas.com.br/website/arquivos/530/>. Acesso em: 08 jun.14.

MENEZES, Rafael da Silva; ASSUNÇÃO, Linara Oeiras. *Os contornos jurídicos da proteção à privacidade no marco civil da internet.* In: Governança das Redes e o Marco Civil da Internet: Liberdades, Privacidade e Democracia. Organizadores: Fabrício Bertini Pasquot Polido e Mônica Steffen Guise Rosina. Belo Horizonte: UFMG, 2015.

MIRANDA, Francisco Cavalcante Pontes de. *Tratados de Direito Privado*, 4 ed. São Paulo: Ed. Revista dos Tribunais, 1983. Tomo VII.

MORAES, Alexandre de. *Constituição do Brasil interpretada e legislação constitucional*. 5 ed. São Paulo: Atlas, 2005.

MORAES, Alexandre de. *Direitos Humanos Fundamentais*: Teoria Geral. Comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil. 9 ed. São Paulo: Atlas, 2011.

MOTTA, S. *CDCIBER: na guerra cibernética, Brasil adota estratégia do contra-ataque*. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/1632/cdciber---na-guerra-cibernetica--brasil-adota-estrategia-do-contra-ataque>. Acesso em: 16 fev.14.

MÜLLER, Friedrich. In: ALEXY, Robert. *Teoría de los Derechos Fundamentales*. Madrid: CEPC, 2001.

NASCIMENTO, Aline Tiduco Hossaka Molette. *Direito à vida privada e à intimidade do portador do HIV e sua proteção no ambiente de trabalho*. Curitiba: UFPR, 2009. Disponível em: <http://dspace.c3sl.ufpr.br/dspace/handle/1884/31089?show=full>. Acesso em: 26 jun. 2014.

NOTÍCIA MILITAR. EE-T1 *Osório volta a ser Fabricado*. Disponível em: <http://noticiamilita.blogspot.com.br/2012/11/ee-t1-osorio-volta-ser-fabricado_16.html>. Acesso em: 18 ago. 2015.

OCDE. *Síntese Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais*. Disponível em: <http://www.oecd.org/sti/ieconomy/15590254.pdf>. Acesso em: 15 fev. 2015.

OLHAR DIGITAL. *Google quer entrar no corpo das pessoas usando a nanotecnologia*. Disponível em: <http://olhardigital.uol.com.br/noticia/google-quer-entrar-no-corpo-das-pessoas-usando-nanotecnologia/44909>. Acesso em: 14 fev. 2015.

OLIVEIRA, Carvalho Rezende Oliveira. *Licitações e Contratos Administrativos*: teoria e prática. 3ª ed. Rio de Janeiro: Forense; São Paulo: Método, 2014.

OLIVEIRA, Eduardo Levi Chaves Barbosa de; SANTOS, Saulo Alex Santana; ROCHA, Fábio Gomes. *Software livre na auditoria e segurança da informação*: desenvolvimento de sistema operacional para perícia, auditoria, teste e gestão de segurança da informação. In: Anais 2014 da 16a Semana de pesquisa da Universidade Tiradentes: ciência e tecnologia para um Brasil sem fronteiras. Disponível em: <https://eventos.set.edu.br/index.php/sempesq/article/view/334>. Acesso em: 14 jan. 2016.

OLIVEIRA, James Eduardo. *Código Civil anotado e comentado*: doutrina e jurisprudência. Rio de Janeiro: Forense, 2009.

ONU. *Declaração Universal dos Direitos do Homem de 1948*. Disponível em: <http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf>. Acesso em: 07 fev. 2016.

Pacto Internacional sobre os Direitos Civis e Políticos, de 1966. Disponível em: <https://www.oas.org/dil/port/1966%20Pacto%20Internacional%20sobre%20Direitos%20Civis%20e%20Pol%C3%ADticos.pdf>. Acesso em: 14 fev. 2015.

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

PINHEIRO, Patrícia Peck. *Direito Digital*. 2 ed. São Paulo: Saraiva, 2007.

PELAJO, Christiane. *Governo da França anuncia medidas de combate ao terrorismo no país*. Jornal da Globo. Edição do dia 21 jan. 2015. Disponível em: <http://g1.globo.com/jornal-da-globo/noticia/2015/01/governo-da-franca-anuncia-medidas-de-combate-ao-terrorismo-no-pais.html>. Acesso em 07 fev. 2015.

PEROSA, Teresa. *O Brasil na era do terror*. In: Revista Época nº 920. São Paulo: Ed. Globo, 2016.

PIN, Sun Tzu Sun. *A Arte da Guerra*. Trad. COTRIN, Ana Aguiar. São Paulo: Ed. Martins Fontes, 2002.

PMI. *Um guia do conhecimento em gerenciamento de projetos*: Guia PMBOK - Project Management Body of Knowledge, 5a edição. São Paulo: Ed. Saraiva, 2014.

POPPER, Karl. *As Aventuras da Racionalidade*. (Org.) PEREIRA, Julio Cesar R. Porto Alegre: EDIPUCRS, 1995.

PORTAL G1. *Aprovação de lei contra terrorismo gera polêmica na França*. Disponível em: <http://g1.globo.com/jornal-nacional/noticia/2015/05/aprovacao-de-lei-contra-terrorismo-gera-polemica-na-franca.html>. Acesso em: 10 mai. 2015.

PORTAL G1. *Canal de TV de oposição é retirado do ar na Venezuela*. Disponível em: <http://g1.globo.com/Noticias/Mundo/0,,MUL1460686-5602,00-CANAL+DE+TV+DE+OPOSICAO+E+RETIRADO+DO+AR+NA+VENEZUELA.html>. Acesso em: 30 jun. 2014.

PORTAL G1. *EUA vão interromper espionagem de líderes aliados, promete Obama*. Disponível em: <http://g1.globo.com/mundo/noticia/2014/01/obama-anuncia-reducao-do-poder-da-agencia-de-espionagem-dos-eua.html>. Acesso em: 09 ago.14.

PORTAL G1. *Petrobras foi espionada pelos EUA, apontam documentos da NSA*. Fantástico. Edição do dia 08/09/2013. Disponível em: <http://g1.globo.com/fantastico/noticia/2013/09/petrobras-foi-espionada-pelos-eua-apontam-documentos-da-nsa.html>. Acesso em 07 fev. 2015.

PORTAL G1. *Governo diz que já tem autorização para usar Exército nas ruas, na BA*. Disponível em: <http://g1.globo.com/bahia/noticia/2014/04/dilma-assina-decreto-de-garantia-da-lei-e-da-ordem-para-ba-diz-governo.html>. Acesso em: 30 jun. 2014.

Portal G1. *Entenda o ataque à rede on-line do PlayStation 3, a PSN*. Tecnologia e Games. Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/05/entenda-o-ataque-rede-line-do-playstation-3-psn.html>. Acesso em: 14 fev. 2015.

PORTAL O GLOBO. *Câmara francesa aprova lei de inteligência que libera espionagem ilimitada nas comunicações*: ed. de 05/05/2015. Disponível em: <http://oglobo.globo.com/mundo/camara-francesa-aprova-lei-de-inteligencia-que-libera-espionagem-ilimitada-nas-comunicacoes-16062176>. Acesso em: 07 maio 2015.

PORTAL DA HISTÓRIA. *Discurso de Abraham Lincoln*. Disponível em: <http://www.arqnet.pt/portal/discursos/novembro01.html>. Acesso em: 26 jun. 2014.

POZZOBON, Tanise; POZOBON, Rejane de Oliveira. *O que o Google sabe sobre você?* Primeiras observações sobre direcionamento de informações. In: Revista do programa de pós-graduação da Universidade Federal Fluminense no 32. Rio de Janeiro, UFF, 2015.

PREGÃO ELETRÔNICO DA PROCURADORIA GERAL DA REPÚBLICA nº 161/2014 e seu respectivo Edital. Pregão disponível mediante busca em: <www.comprasnet.gov.br>. Acesso em: 10 ago. 2015.

PREGÃO ELETRÔNICO DA RECEITA FEDERAL (RFB/COPOL) nº 17/2014 e seu respectivo Edital. Pregão disponível mediante busca em: <www.comprasnet.gov.br>. Acesso em: 10 ago. 2015.

PREGÃO ELETRÔNICO DA UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ (SRP) nº 22/2014 e seu respectivo Edital. Pregão disponível mediante busca em: <www.comprasnet.gov.br>. Acesso em: 10 ago. 2015.

PREGÃO ELETRÔNICO nº 021/2014 da Secretaria de Administração da Prefeitura do Município de Osasco e seu respectivo Edital. Pregão disponível mediante busca em: <www.comprasnet.gov.br>. Acesso em: 10 ago. 2015.

PREGÃO ELETRÔNICO POR REGISTRO DE PREÇOS nº 134/2014 do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina e seu respectivo Edital. Pregão disponível mediante busca em: <www.comprasnet.gov.br>. Acesso em: 10 ago. 2015.

PREGÃO ELETRÔNICO SPR Nº 31/2011 – Base Administrativa do CCOMGEX.

RAMÍREZ, Sergio García. *Considerações sobre terrorismo*. In: OLLOQUI, José Juan de (Coord.). Problemas jurídicos e políticos del terrorismo. México: Universidad Nacional Autónoma de México, 2004.

REDAÇÃO ÉPOCA. *Medo de espionagem aumenta venda de máquinas de escrever na Alemanha*. Disponível em: <http://epoca.globo.com/vida/noticia/2014/07/medo-bespionagemb-aumenta-venda-de-maquinas-de-escrever-na-alemanha.html/>. Acesso em: 09 ago. 2014.

REDAÇÃO G1. *Entenda o caso de Edward Snowden, que revelou espiongem dos EUA*. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 16 fev. 2014.

REDAÇÃO INFO. *Microsoft abre centro para combater crimes cibernéticos*. Disponível em: <http://info.abril.com.br/noticias/internet/2013/11/microsoft-abre-centro-para-combater-crimes-ciberneticos.shtml>. Acesso em: 08 dez. 2013.

REDAÇÃO LINHA DEFENSIVA. *Exército brasileiro investe R$ 6 milhões em segurança e guerra digital*. Disponível em: <http://www.linhadefensiva.org/2012/01/exercio-brasileiro-investe-r-6-milhoes-em-seguranca-e-guerra-digital/>. Acesso em: 02 ago. 2015.

REIS, Solange, et al. *Entre Aspas*: Privacidade na rede. GLOBONEWS. Exibido em: 11 jun. 2013.

REUTERS. *CIA tentou hackear iPhones desde os primeiros dias do aparelho, diz site*. Disponível em: <http://www.msn.com/pt-br/noticias/ciencia-e-tecnologia/cia-tentou-hackear-iphones-desde-os-primeiros-dias-do-aparelho-diz-site/ar-AA9B5V1?ocid=mailsignoutmd#fullstory>. Acesso em: 10/3/2015.

RIBEIRO, Gustavo. *A França e o direito de espionar*. Disponível em: <http://jota.info/a-franca-e-o-direito-de-espionar>. Acesso em: 09 mai. 2015.

RIO GRANDE DO SUL. *Lei nº 11.871, de 19 de dezembro de 2002*. Utilização de programas de computador no Estado do Rio Grande do Sul. Lei 11871/02. Disponível em: <http://www.al.rs.gov.br/legis/M010/M0100099.ASP?Hid_Tipo=TEXTO&Hid_TodasNormas=264&hTexto=&Hid_IDNorma=264>. Acesso em: 26 jan. 2016.

RODOTÀ, Stefano. *A Vida na Sociedade da Vigilância*: A Privacidade Hoje, Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda; Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

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

SAMPAIO, José Adércio Leite. *Direito à intimidade e à vida privada*: uma visão jurídica da sexualidade da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998.

SÁNCHEZ-OCAÑA, Alejandro Suárez. A Verdade por Trás do Google. Trad. Sandra Martha Dolinsky. São Paulo: Planeta, 2013.

SANTINI, José Raffaelli. *Dano Moral*. Campinas: Millennium, 2002.

SARAVIA, Enrique. *Política pública, política cultural, indústrias culturais e indústrias criativas.* In: Plano da Secretaria da Economia Criativa: políticas, diretrizes e ações, 2011 – 2014. Brasília: Ministério da Cultura, 2011.

SARLET, Ingo Wolfgang. *Dignidade da Pessoa Humana e Direitos Fundamentais na Constituição Federal de 1988*. 6. ed. Porto Alegre: Livraria do Advogado, 2008.

SASSINE. V. *Exército monitorou líderes de atos pelas redes sociais*. Disponível em: <http://oglobo.globo.com/pais/exercito-monitorou-lideres-de-atos-pelas-redes-sociais-9063915>. Acesso em: 08 dez. 2013.

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

SCHELL, Bernadette H. *Internet censorship*: a reference handbook. Oxford: ABC-CLIO, 2014.

SEMITSU. Junichi P. *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance.* Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1782267>. Acesso em: 14 fev. 2016.

SENADO FEDERAL. *Inimigos invisíveis*: a guerra cibernética. Disponível em: <http://www.senado.gov.br/noticias/Jornal/emdiscussao/defesa-nacional/razoes-para-a-implementaao-da-estrategia-nacional-de-defesa/inimigos-invisiveis-a-guerra-cibernetica.aspx>. Acesso em: 06 fev. 2016.

SEVERIANO, Alan. *Obama faz vídeo para incentivar cadastramento no programa de saúde.* Jornal Hoje. Disponível em: <http://glo.bo/1F63APa> Acesso em: 13 fev. 2015.

SILVA, José Afonso da. *Curso de direito constitucional positivo*. 37 ed. São Paulo: Malheiros. 2014.

SOGHOIAN, Christopher; PELL, Stephanie K. *Your secret stingray's no secret anymore: the vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy*. In: Harvard Journal of Law & Technology Volume 28, Number 1 Fall 2014. Disponível em: <http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech1.pdf>. Acesso em: 14 jan. 2016.

SOTO, Cesar. *O mundo contra os Hackers*. In: Revista ISTOÉ. ed. 21 Jan 2015, nº2355. São Paulo: Três, 2015.

SOUZA, Beatriz. *Dilma continua sendo espionada pelos EUA, diz NY Times*. Disponível em: <http://exame.abril.com.br/brasil/noticias/dilma-continua-sendo-espionada-pelos-eua-diz-ny-times>. Acesso em 07 fev. 2015.

SNOWDEN, Edward. *Milênio*: Sonia Bridi entrevista Edward Snowden. Disponível em: <http://globotv.globo.com/globo-news/milenio/v/milenio-sonia-bridi-entrevista-edward-snowden/3389933/>. Acesso em: 08 jun. 2014.

SUNDFELD, C. A.; Vieira, O. V. *Direito global*. São Paulo: Max Limonad, 1999.

TAVARES, André Ramos. *Direito Constitucional Econômico*. 3 ed. São Paulo: Método, 2006. v. 1.

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

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

THE US-CHINA ECONOMIC AND SECURITY REVIEW COMISSION. *Capability of the people's Republico f China to conduct cyber warfare and computer network exploitation*. McLean: Northrop Grumman Co., 2009.

TERRA TECNOLOGIA. *Saiba como funciona o controle da internet na China*. Disponível em: <http://tecnologia.terra.com.br/saiba-como-funciona-o-controle-da-internet-na-china,57182d8e6545b310VgnCLD200000bbcceb0aRCRD.html/>. Acesso em: 09 ago. 2014.
VALOR ECONÔMICO. *FBI não encontra Indício de Ataque Cibernético em Falha na Bolsa de NY*. Disponível em: <http://www.valor.com.br/financas/4127214/fbi-nao-encontra-indicio-de-ataque-cibernetico-em-falha-na-bolsa-de-ny>. Acesso em: 09 jul. 2015.

VERVAELE, JOHN A. E. *A legislação anti-terrorista nos estados unidos: um direito penal do inimigo?* Disponível em: <http://www.seer.ufrgs.br/index.php/redppc/article/view/52029/32055>. Acesso em: 08 jan. 2016.

VILICIC, Filipe. A Guerra entre a Apple e o FBI. *Revista Veja*. ed. 2466. São Paulo: Abril, 2016.

VILICIC, F. Por uma Web Sem Censura. *Revista Veja*. ed. 2351. São Paulo: Abril, 2013.

WATERS, Richard. *Google acata decisão da União Europeia sobre privacidade*. Disponível em: <http://www1.folha.uol.com.br/mundo/2014/05/1462454-google-acata-decisao-da-uniao-europeia-sobre-privacidade.shtml>. Acesso em: 06 set. 2014.

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

wikileaks.org

WU, Tim. *Impérios da comunicação*: do telefone à internet, da AT&T ao Google. Trad. Cláudio Carina. Rio de Janeiro: Zahar, 2012.

YANG, Steven; CHEN, Lulu Yilun. *Governo da China não quer mais os MacBooks e iPads da Apple*. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/governo-da-china-nao-quer-mais-os-macbooks-e-ipads-da-apple/>. Acesso em: 09 ago. 2014.

ZIMMERMANN, Phil. *Por que você precisa do PGP?* Disponível em: <http://www.pgpi.org/doc/whypgp/br/>. Acesso em: 09 ago. 2014.